INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO SUL
CAMPUS CAXIAS DO SUL

INTRODUÇÃO À TEORIA DE GALOIS

TRABALHO DE CONCLUSÃO DE CURSO
LICENCIATURA EM MATEMÁTICA

BRUNA FAVERO

CAXIAS DO SUL
2019

BRUNA FAVERO

INTRODUÇÃO À TEORIA DE GALOIS

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do grau de Licenciado em Matemática, pelo Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul – *Campus* Caxias do Sul.

Área de Concentração: Matemática

Orientadores:
Orientador: Prof. Me. Nícolas Moro Müller – IFRS – *Campus* Caxias do Sul
Coorientador: Prof. Dr. Rafael Cavalheiro – FURG

CAXIAS DO SUL

2019

Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul, *Campus* Caxias do Sul

51 Favero, Bruna
F273i Introdução a teoria de Galois. [manuscrito] / Bruna Favero ; orientador, Nícolas Moro Müller ; coorientador, Rafael Cavalheiro -- Caxias do Sul, RS, 2019.
67 f.

TCC (Licenciatura em Matemática) - Instituto Federal de Educação, Ciência e Tecnologia do RS (IFRS), Caxias do Sul, 2019.

1. Licenciatura em matemática. 2. Teoria de Galois. 3.Extensão de corpos (Matemática) I. Müller, Nícolas Moro. II. Cavalheiro, Rafael. III. Título.
CDU 51

Ficha catalográfica elaborada pela bibliotecária Jaçanã Eggres Pando - CRB 10/1936

BRUNA FAVERO

INTRODUÇÃO À TEORIA DE GALOIS

A banca examinadora, abaixo listada, aprova o Trabalho de Conclusão de Curso Introdução à Teoria de Galois elaborado por Bruna Favero como requisito parcial para obtenção do grau de Licenciado em Matemática, pelo Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul – *Campus* Caxias do Sul.

Me. Félix Afonso de Afonso – PPGMat - UFRGS

Me. Eduardo Henrique Philippsen – PPGMat - UFRGS

Me. Leonardo Duarte Silva – PPGMat - UFRGS

Caxias do Sul, 2019.

AGRADECIMENTOS

Primeiramente gostaria de agradecer a Deus.

Agradeço à minha família por todo apoio ao longo desses quatro anos, em especial à minha mãe, Adriana, por estar ao meu lado em cada passo dessa trajetória.

Agradeço ao meu orientador professor Nícolas Moro Müller e ao coorientador professor Rafael Cavalheiro por aceitarem conduzir o meu trabalho de pesquisa. Aos demais professores por todos os ensinamentos e inspirações.

Agradeço também as minhas colegas, Letícia, Virgínia e Munique, por todo o apoio, por todas as tardes de estudos e pelas inúmeras risadas.

E por fim, agradeço também ao Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul - *Campus* Caxias do Sul, pela oportunidade de concluir esta graduação.

RESUMO

O presente trabalho apresenta conteúdos introdutórios para a Teoria de Galois, a fim de tornar possível a compreensão desta. A Teoria de Galois tem grande importância na caracterização de polinômios acerca da sua solubilidade por meio de radicais, utilizando propriedades de grupos de automorfismos de um corpo. A metodologia utilizada para a realização do trabalho foi a pesquisa bibliográfica, que possibilitou o estudo dos tópicos em material já consolidado. No decorrer do trabalho é feita a apresentação de conteúdos que são pré-requisitos, além de conceitos e definições como extensões algébricas e extensões Galoisianas que precedem a Correspondência de Galois e a solubilidade por meio de radicais, viabilizando o objetivo do trabalho.

Palavras-chave: Grupos, Extensão de corpos, Teoria de Galois.

ABSTRACT

This work presents introductory contents for the Galois theory, in order to be possible understand it. The methodology applied for the work accomplishment was the bibliographical research, which made possible the study of topics in already consolidated material. During the work, is made the contents presentation that are prerequisites, as well as concepts, definitions such as algebraic extensions, and galoisian extensions that precede Galois correspondence and solvability by radicals, enabling the work purpose. The Galois theory has a great importance in the characterization of polynomials about their solvability by radicals, using properties of automorphism groups of a fields.

Keywords: Groups, Field extensions, Galois theory.

SUMÁRIO

1 INTRODUÇÃO

Originalmente a álgebra restringia-se ao estudo das equações e métodos para resolvê-las, sejam estes, métodos geométricos, utilizados pelos gregos, ou métodos mais sofisticados, com a utilização de simbologia de representação e manipulação desenvolvida a partir da Idade Média. No entanto, ao invés de procurar métodos numéricos para resolver equações, Galois passou a investigar a estrutura dos corpos e grupos e estabeleceu uma conexão entre eles que hoje chamamos de Teoria de Galois (BAUMGART, 1992).

Objetivamos com este trabalho estudar tais estruturas, partindo do estudo inicial da Álgebra Abstrata realizado durante a graduação, com a finalidade de formar conhecimentos necessários para o estudo da Teoria de Galois e de sua aplicabilidade na determinação da solubilidade de equações de grau maior ou igual a cinco por meio de radicais.

O trabalho está dividido em seis capítulos, sendo esta introdução o primeiro. Abordamos no segundo capítulo a metodologia utilizada para o desenvolvimento do trabalho. Uma vez que este baseia-se em estudos de teorias e conceitos já elaborados, a metodologia se dá de forma bibliográfica. No capítulo três, faz-se uma breve abordagem histórica da evolução do estudo das equações polinomiais e da solubilidade por meio de radicais.

Os conceitos preliminares estão dispostos no quarto capítulo, onde são abordados conceitos e definições de anéis, ideais e homomorfismos, noções de álgebra linear, extensões algébricas dos racionais, grau de uma extensão algébrica, grupos, subgrupos, classes laterais, grupos quocientes e homomorfismo de grupos.

O quinto capítulo traz definições e propriedades de extensões galoisianas e extensões normais, tópicos fundamentais para a posterior compreensão da Teoria de Galois e a solubilidade por meio de radicais. As conclusões sobre o estudo realizado encontram-se no capítulo seis.

2 METODOLOGIA

A metodologia escolhida para a realização deste trabalho foi a pesquisa bibliográfica, uma vez que o campo de pesquisa estabelecido encontra-se bem desenvolvido em livros, artigos, dissertações, entre outros. Por meio desta, buscaremos apropriação necessária do tema a fim de estabelecer-se caminhos para a resposta do problema.

Segundo Gil (2010, p.45) as etapas de uma pesquisa bibliográfica são as seguintes:

a) escolha do tema;
b) levantamento bibliográfico preliminar;
c) formulação do problema;
d) elaboração do plano provisório de assunto;
e) busca das fontes;
f) leitura do material;
g) fichamento;
h) organização lógica do assunto;
i) redação do texto.

Partindo da definição do tema foi realizado um levantamento bibliográfico, fundamentado em livros, a fim de identificar as referências mais adequadas ao nosso propósito. Desse modo, foi selecionado Gonçalves (2015) como principal referência tanto para a conceituação dos pré-requisitos, conceitos e definições necessários à compreensão do tema, como anéis, ideais, homomorfismos, extensões algébricas e grupos, quanto para a introdução à Teoria de Galois, e como referências complementares Domingues e Iezzi (2003), Martin (2010) e Bueno (2006). Para levantamento histórico utilizou-se Domingues e Iezzi (2003), Eves (2004) e Katz (2010).

3 EMBASAMENTO HISTÓRICO

Problemas envolvendo o produto de duas incógnitas ou o quadrado de uma, originaram equações conhecidas hoje em dia por equações quadráticas. Antes do século $VI\,d.C.$, os babilônicos resolveram equações quadráticas através de uma regra que pode ser traduzida na fórmula moderna para resolver $x^2 + bx = c$,

$$x = \sqrt{\left(\frac{b}{2}\right)^2 + c} - \frac{b}{2}.$$

No entanto, os babilônicos não consideravam soluções negativas, porque estas não tem significado geométrico, nem duas soluções positivas distintas, pois consideravam que uma equação não poderia ter dois valores diferentes para a mesma incógnita. (KATZ, 2010)

Em cerca de $825\,d.C.$, o matemático e astrônomo islâmico al-Khwarizmi, baseado nas ideias babilônicas para a resolução da equação $x^2+bx = c$, passou a considerar soluções diferentes para uma mesma incógnita e o emprego de adição ou subtração para obter a solução do problema, dado pela equação

$$x = -\frac{b}{2} \pm \sqrt{\left(\frac{b}{2}\right)^2 + c},$$

que foi sendo adaptada, através do tempo, até chegar na atual fórmula resolutiva para equação quadrática.

Entre 1500 e 1515, o matemático italiano Scipione del Ferro desenvolveu um procedimento para resolver a equação cúbica $x^3+px = q$ $(p, q > 0)$, que pode ser traduzido pela fórmula

$$\sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} - \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}.$$

Com isso ele mostrou que é possível expressar as raízes da equação cúbica considerada em termos dos seus coeficientes utilizando apenas adições, multiplicações e radiciações.

No século $XVI d.C.$, o matemático francês François Viète determinou uma solução para a equação quártica, considerando $x^4+ax^2+bx = c$, cuja forma pode se reduzir toda quártica completa. Somando $x^2y^2 + \dfrac{y^4}{4}$ a ambos os membros de $x^4 = c - ax^2 - bx$ obtém-se

$$\left(x^2 + \frac{y^2}{2}\right)^2 = (y^2 - a) \cdot x^2 - bx + \left(\frac{y^4}{4} + c\right).$$

Escolhe-se então y de modo que o segundo membro seja um quadrado perfeito, sendo possível extrair raízes quadradas, concluindo o problema (EVES, 2004).

Partindo da solução de Del Ferro sobre a resolubilidade de equações algébricas, o matemático e astrônomo italiano Joseph-Louis Lagrange começou a desvendar o caminho a ser seguido para abordar o problema, observou que permutações envolvendo as raízes da equação era de grande importância para a resolução desta. Em 1824, o matemático norueguês Niels Henrik Abel mostrou que não há nenhuma fórmula geral por radicais para resolver as equações de grau ≥ 5, conclusão de que Lagrange já suspeitava (DOMINGUES E IEZZI, 2003).

Ainda, partindo da ideia da resolubilidade das equações algébricas através de radicais, introduzidas por Del Ferro, foi posteriormente generalizada pelo matemático francês Evariste Galois, que segundo Katz (2010)

> [$\cdots$] começa por classificar a ideia de racionalidade, uma vez que, uma equação tem coeficientes num certo domínio, por exemplo, o conjunto dos números racionais comuns, dizer que uma equação é resolúvel através de radicais significa que é possível exprimir suas raízes, utilizando as quatro operações aritméticas básicas e a operação de extração de raiz, aplicadas aos elementos deste domínio original.

Além disso, a fim de caracterizar quais equações de grau ≥ 5 seriam solúveis por meio de radicais e quais não seriam, Galois analisou a noção de permutação e emprega a palavra "grupo", por vezes utilizado para referir-se a um conjunto de permutações que é fechado para a composição e outras vezes para referir apenas um conjunto de arranjos de letras, obtido através da aplicação de certas permutações.

A noção de grupo foi um instrumento de muita importância para a organização e o estudo de muitos ramos da matemática, em álgebra, foi um fator de grande importância para o desenvolvimento da álgebra abstrata no século XX. A ideia de Galois para responder esta questão foi associar a cada equação um grupo formado pelas permutações de suas raízes e condicionar a resolubilidade por radicais a uma propriedade desse grupo.

4 TEORIA PRELIMINAR

Este capítulo tem como objetivo apresentar a fundamentação teórica necessária para a compreensão da pesquisa. O mesmo será dividido em três seções: Anéis, Ideais e Homomorfismos, Extensões Algébricas dos Racionais e Grupos. As definições, os exemplos e os resultados aqui apresentados foram extraídos e/ou adaptados de Gonçalves (2015).

4.1 ANÉIS, IDEAIS E HOMOMORFISMOS

Nesta seção, iremos conceituar pré-requisitos necessários para a compreensão dos tópicos básicos de extensões algébricas, que são fundamentais para o estudo da Teoria de Galois. São eles: anel, corpo, ideal, homomorfismo e anéis de polinômios. A seguir definiremos anéis e corpos, subanéis e subcorpos.

4.1.1 Anéis

Seja A um conjunto não vazio onde estejam definidas duas operações binárias, as quais chamaremos de adição e multiplicação em A e denotaremos (como em $\mathbb{Z}$) por $+$ e $\cdot$.

Assim,

$$\begin{array}{ccc} + : A \times A \to A & \text{e} & \cdot : A \times A \to A \\ (a,b) \mapsto a+b & & (a,b) \mapsto a \cdot b \end{array}.$$

Dizemos que $(A, +, \cdot)$ é um *anel* se as seguintes propriedades, as quais chamaremos de axiomas, são verificadas quaisquer que sejam a, b, $c \in A$.

i) Associatividade da adição:
$(a+b)+c = a+(b+c)$;

ii) Existência do elemento neutro para a adição:
Existe $0_A \in A$ tal que $a + 0_A = 0_A + a = a$;

iii) Existência do elemento simétrico em relação à adição:
Dado $a \in A$ existe um único $b \in A$, denotado por $b = -a$, tal que
$a + b = b + a = 0_A$;

iv) Comutatividade da adição:
$a + b = b + a$;

v) Associatividade da multiplicação:
$(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

vi) Distributividade da multiplicação em relação à adição:
$a \cdot (b + c) = a \cdot b + a \cdot c$ e $(a + b) \cdot c = a \cdot c + b \cdot c$.

Desta forma, temos que os axiomas de i) a vi) são os axiomas que definem um anel.

Se além das propriedades acima $(A, +, \cdot)$ satisfaz:

vii) Existência do elemento neutro para a multiplicação:
Existe $1_A \in A, 0_A \neq 1_A$ tal que $x \cdot 1_A = 1_A \cdot x = x$, $\forall\, x \in A$.
Dizemos que $(A, +, \cdot)$ é um *anel com unidade* 1_A ou *anel unitário*.

viii) Comutatividade da multiplicação:
$a \cdot b = b \cdot a$.
Dizemos que $(A, +, \cdot)$ é um *anel comutativo* ou *abeliano*.

Neste trabalho todos os anéis considerados serão comutativos e com unidade e, para simplificar a notação denotaremos o anel $(A, +, \cdot)$ simplesmente por A. Além disso, por vezes escrevemos simplesmente ab para representar $a \cdot b$, onde $a, b \in A$.

Um elemento não nulo a do anel $(A, +, \cdot)$ é chamado ıdivisor de zero se existe $0_A \neq b \in A$ tal que $a \cdot b = 0_A$. Assim, um anel $(A, +, \cdot)$ é sem divisores de zero se é um anel em que $a \cdot b = 0_A \Rightarrow a = 0_A$ ou $b = 0_A$.

Definição 4.1.1. *Um domínio de integridade, ou simplesmente domínio, é um anel sem divisores de zero.*

Sejam A um anel e $a, b \in A$. Dizemos que b é o *inverso* de a e, denotamos por $b = a^{-1}$, quando $a \cdot b = b \cdot a = 1_A$.

Exemplo 4.1.2. *Seja $(\mathbb{Z}, +, \cdot)$, onde $+$ e $\cdot$ são as operações usuais. Temos que $\mathbb{Z}$ é um domínio.*

Vamos verificar os axiomas de anel. Para todo x, y e $z \in \mathbb{Z}$, temos

i) Associatividade da adição: $(x + y) + z = x + (y + z)$;

ii) Existência do elemento neutro: existe $0 \in \mathbb{Z}$ tal que $x + 0 = 0 + x = x$;

iii) Existência do elemento simétrico em relação à adição: existe $-x \in \mathbb{Z}$ tal que $x + (-x) = (-x) + x = 0$;

iv) Comutatividade da adição: $x + y = y + x$;

v) Associatividade da multiplicação: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;

vi) Distributividade da multiplicação em relação à adição: $x \cdot (y + z) = x \cdot y + x \cdot z$;

vii) Existência do elemento neutro para a multiplicação: existe $1 \in \mathbb{Z}$ tal que $x \cdot 1 = 1 \cdot x = x$;

viii) Comutatividade da multiplicação: $x \cdot y = y \cdot x$;

ix) $\mathbb{Z}$ não possui divisires de zero: $x \cdot y = 0 \Rightarrow x = 0$ ou $y = 0$.

Portanto, $\mathbb{Z}$ é um anel sem divisores de zero, ou seja, um domínio.

Definição 4.1.3. *Seja K um anel. Dizemos que K é um corpo quando todos os elementos não nulos de K possuem inverso.*

Exemplo 4.1.4. *Seja $\mathbb{C}$ conjunto de todos os pares ordenados (a, b) em que $a, b \in \mathbb{R}$:*

$$\mathbb{C} = \{(a, b); a, b \in \mathbb{R}\}.$$

Com as operações de $+$ e $\cdot$ definidas por $(a, b) + (c, d) = (a + c, b + d)$ e $(a, b) \cdot (c, d) = (ac + bd, ad + bc)$, respectivamente. E com as seguintes propriedades:

a) $(0,0)+(a,b)=(a,b)+(0,0)=(a,b)$;

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

Vamos verificar que $\mathbb{C}$ *é um corpo.*

De fato, para quaisquer x, y e $z \in \mathbb{C}$, temos

i) Associatividade da adição: $x+(y+z)=(x+y)+z$;

ii) Comutatividade da adição: $x+y=y+x$;

iii) Existência do elemento neutro: $0+x=x$;

iv) Existência do elemento simétrico em relação à adição: dado $x=(a,b)\in\mathbb{C}$, existe $-x=(-a,-b)\in\mathbb{C}$ tal que $x+(-x)=0$;

v) Associatividade da multiplicação: $x\cdot(y\cdot z)=(x\cdot y)\cdot z$;

vi) Comutatividade da multiplicação: $x\cdot y=y\cdot x$;

vii) Existência do elemento neutro para a multiplicação: $1\cdot x=x$;

viii) Distribuitividade da multiplicação com relação à adição: $x\cdot(y+z)=xy+xz$;

iv) $\mathbb{C}$ não possui divisores de zero: $x\cdot y=0\Rightarrow x=(0,0)$ ou $y=(0,0)$;

x) Existência do elemento inverso: se $x=(a,b)\neq 0$, então existe $x^{-1}=\left(\dfrac{a}{a^2+b^2},\dfrac{-b}{a^2+b^2}\right)\in\mathbb{C}$ tal que $x\cdot x^{-1}=1$.

Portanto, $\mathbb{C}$ é corpo.

Proposição 4.1.5. *Todo corpo, em particular, é um domínio de integridade.*

Demonstração. Sejam K um corpo e $a, b \in K$ tais que $a\cdot b=0_K$.

Se $a=0_K$, temos o que se pede.

Suponhamos $a\neq 0_K$. Da definição de corpo, temos que existe $a^{-1}\in K$ tal que $a^{-1}\cdot a=1_K$, onde a^{-1} é o inverso de a. Assim, temos que

$$a\cdot b=0_K\Rightarrow a^{-1}\cdot(a\cdot b)=a^{-1}\cdot 0_K\Rightarrow(a^{-1}\cdot a)\cdot b=0_K\Rightarrow 1_K\cdot b=0_K\Rightarrow b=0_K.$$

Logo, quando $a \cdot b = 0_K$, devemos ter $a = 0_K$ ou $b = 0_K$. Portanto, temos que K é um domínio. □

Definição 4.1.6. *Seja* $(A, +, \cdot)$ *um anel. Um subconjunto não vazio* $B \subset A$ *é subanel de* A *quando*

i) $x + y \in B$ *e* $x \cdot y \in B$, $\forall\, x, y \in B$;

ii) $1_A \in B$;

iii) $(B, +, \cdot)$ *é um anel.*

Se um subanel $(B, +, \cdot)$ de um corpo $(K, +, \cdot)$ é também um corpo, dizemos que B é um *subcorpo* de K. Se K é um domínio, dizemos que B é subdomínio de K. Por exemplo, seja $\mathbb{R}$ o corpo dos números reais, para cada p primo, temos que $\mathbb{Q}[\sqrt{p}] = \left\{a + b\sqrt{p}; a, b \in \mathbb{Q}\right\}$ é um subcorpo de $\mathbb{R}$.

4.1.2 Ideais e Homomorfismos de anéis

Nesta subseção trataremos da definição e propriedades dos ideais e dos homomorfismos de anéis.

Definição 4.1.7. *Sejam* A *um anel e* $\varnothing \neq I \subseteq A$. *Dizemos que* I *é um ideal de* A *se* $x - y \in I$ *e* $x \cdot a \in I$, *para todo* $a \in A$ *e* $x, y \in I$.

Os ideais $\{0_A\}$ e A são chamados de *ideais triviais de* A.

Exemplo 4.1.8. *Sejam* $I = (2\mathbb{Z}, +, \cdot)$ *e* $A = (\mathbb{Z}, +, \cdot)$, *com adição usual de inteiros e multiplicação definida por* $x \cdot y = 0$ *para quaisquer* $x, y \in \mathbb{Z}$. *Vamos verificar que* I *é ideal de* A.

Sejam $x, y \in \mathbb{Z}$, temos

i) $2x - 2y = 2(x - y) \in I$;

ii) $2x \cdot y = 2(x \cdot y) = 2 \cdot 0 \in I$.

Logo, I é ideal de A.

Definição 4.1.9. *Sejam A um anel e M um ideal de A. Dizemos que M é ideal maximal de A quando $M \neq A$ e se I é um ideal de A com $M \subseteq I \subseteq A$ então, $I = M$ ou $I = A$.*

Teorema 4.1.10. *Seja $(K, +, \cdot)$ um anel. Então, as seguintes condições são equivalentes:*

a) K é um corpo;

b) $\{0_K\}$ é um ideal maximal de K;

c) Os únicos ideais de K são os triviais.

A demonstração desse teorema pode ser encontrada em GONÇALVES (2015, p. 49).

Definição 4.1.11. *Sejam A um anel I um ideal de A. Vamos definir a seguinte relação em A: dados $x, x' \in A$, $x \equiv x' \,(mod\, I)$ se, e somente se, $x - x' \in I$.*

Seja I um ideal de A. Denomina-se *classe de equivalência* de um elemento $x \in A$ o conjunto de todos os elementos $x' \in A$ tais que $x' \equiv x(mod\, I)$ e denotamos esse conjunto por $\overline{x} = x + I$. O conjunto das classes de equivalência geradas por I em A será denotado por

$$A/I = \{\overline{x} = x + I; x \in A\}.$$

Podemos definir uma adição e multiplicação em A/I, por $\overline{a} + \overline{b} = \overline{a + b}$ e $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$, respectivamente.

As operações de adição e multiplicação em A/I estão bem definidas, isto é, dados $\overline{a}, \overline{b}, \overline{x}, \overline{y} \in A/I$ com $(\overline{a}, \overline{b}) = (\overline{x}, \overline{y})$, temos que

$$\overline{a} + \overline{b} = \overline{x} + \overline{y} \quad \text{e} \quad \overline{a} \cdot \overline{b} = \overline{x} \cdot \overline{y}.$$

Ainda, sendo I um ideal do anel A então, $(A/I, +, \cdot)$ é um anel, chamado de *anel quociente* de A por I. A demonstração do que foi citado acima pode ser encontrada em DOMINGUES E IEZZI (2003, p. 265).

Teorema 4.1.12. *Sejam A um anel e I um ideal de A. Então, I é ideal maximal de A se, e somente se, A/I é um corpo.*

A demonstração desse teorema pode ser encontrada em GONÇALVES (2015, p.52).

Definição 4.1.13. *Sejam A e B anéis. Uma função $f : A \to B$ diz-se um homomorfismo de anéis se satisfaz as seguintes condições:*

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

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

iii) $f(1_A) = 1_B$.

Observação 4.1.14. *Se $f : A \to B$ for um homomorfismo de anéis bijetor dizemos que f é um isomorfismo de anéis de A em B. Neste caso escrevemos $A \simeq B$. Ainda, os isomorfismos de A sobre si mesmo, ou seja, $f : A \to A$, são chamados de automorfismos de A. O conjunto dos automorfismos de A é denotado por $Aut\,(A)$.*

Exemplo 4.1.15. *Denotamos por $\mathbb{Z}_n = \left\{\overline{a}; a \in \mathbb{Z}\right\}$ o conjunto de todas as classes de equivalência módulo n, para $n \in \mathbb{N}$ e $\overline{a} = \left\{b \in \mathbb{Z}; a \equiv b \ mod\ n\right\}$. Agora, seja $f : \mathbb{Z} \to \mathbb{Z}_n$, $f(x) = \overline{x}$, é homomorfismo de anéis.*

De fato, tomando $x, y \in \mathbb{Z}$, temos

i) $f(\overline{x+y}) = \overline{x+y} = \overline{x} + \overline{y} = f(\overline{x}) + f(\overline{y})$;

ii) $f(\overline{x \cdot y}) = \overline{x \cdot y} = \overline{x} \cdot \overline{y} = f(\overline{x}) \cdot f(\overline{y})$;

iii) $f(1) = \overline{1}$.

Definição 4.1.16. *Seja $f : A \to B$ um homomorfismo de anéis. Chamamos de núcleo de f e representamos por $Ker(f)$, o conjunto formado pelos elementos de A cuja imagem por f é $0_B \in B$, isto é,*

$$Ker(f) = \{a \in A; f(a) = 0_B\}.$$

Além disso, definimos a imagem de f por

$$Im(f) = \{y \in B; \exists\, a \in A \ tal\ que\ f(a) = y\}.$$

4.2 NOÇÕES DE ÁLGEBRA LINEAR

Nesta subseção trataremos de alguns conceitos de álgebra linear necessários para descrição de alguns resultados sobre extensões algébricas.

Definição 4.2.1. *Sejam K um corpo e V um conjunto não vazio, onde estão definidas as seguintes operações:*

$$+ : V \times V \to V \qquad e \quad \cdot : K \times V \to V.$$
$$(u, v) \mapsto u + v \qquad\qquad (\lambda, v) \mapsto \lambda v$$

Dizemos que V munido dessas operações é um espaço vetorial sobre o corpo K se as propriedades a seguir são verificadas para quaisquer $u, v, w \in V$ e $\lambda, \mu \in K$.

i) $u + (v + w) = (u + v) + w$;

ii) existe $0_K \in V$ *tal que* $u + 0_K = 0_K + u = u$;

iii) dado $x \in V$ *existe* $y \in V$ *tal que* $x + y = y + x = 0_K$;

iv) $u + v = v + u$;

v) $1_K v = v$, *onde* 1_K *é a unidade do corpo* K;

vi) $\lambda(u + v) = \lambda u + \lambda v$ *e* $(\mu + \lambda)u = \mu u + \lambda u$;

vii) $\lambda(\mu v) = \mu(\lambda v) = (\lambda\mu)v$.

Observação 4.2.2. *Chamamos $+$ de adição e $\cdot$ de multiplicação por escalar. Os elementos de V são chamados vetores.*

Definição 4.2.3. *Sejam K um corpo e V um espaço vetorial sobre K e $\varnothing \neq W \subseteq V$. Dizemos que W é um subespaço vetorial de V se:*

i) $w_1, w_2 \in W \Rightarrow w_1 + w_2 \in W$;

ii) $\lambda \in K, w \in W \Rightarrow \lambda w \in W$.

Sejam $v_1, \cdots, v_n \in V$. Dizemos que $\{v_1, \cdots, v_n\}$ é *linearmente independente (L.I)* se a equação vetorial $\sum_{i=1}^{n} \alpha_i v_i = 0, \alpha_i \in K$, para cada $i \in \{1, 2, \cdots, n\}$ é satisfeita apenas para os escalares $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$. Caso contrário, dizemos que $\{v_1, \cdots, v_n\}$ é *linearmente dependente (L.D)*.

Definição 4.2.4. *Se* $u_1, u_2, \cdots, u_r \in V$ *então,*

$$W = \left\{ \sum_{i=1}^{r} \alpha_i u_i ; \alpha_i \in K, i \in \{1, \cdots, r\} \right\}$$

é um subespaço vetorial de V*. De fato, sejam* $w, w_1, w_2 \in W$ *e* $\lambda \in K$*, temos*

i) Se $w_1 = \sum_{i=1}^{r} \alpha_i u_i$ *e* $w_2 = \sum_{i=1}^{r} \beta_i u_i$*, então* $w_1 + w_2 = \sum_{i=1}^{r} (\alpha_i + \beta_i) u_i \in W$*;*

ii) Se $w = \sum_{i=1}^{r} \alpha_i u_i$*, então* $\lambda w = \lambda \cdot \left(\sum_{i=1}^{r} \alpha_i u_i \right) = \sum_{i=1}^{r} \lambda(\alpha_i u_i) =$ $= \sum_{i=1}^{r} (\lambda \alpha_i) u_i \in W$*, pois* $\lambda \alpha_i \in K, \forall\, 1 \leq i \leq r$*.*

Chamaremos W *de subespaço gerado por* $u_1, \cdots, u_r$ *e denotaremos esse espaço por* $W = \langle u_1, \cdots, u_r \rangle$*.*

Ainda, se um conjunto (ordenado) $\{v_1, \cdots, v_n\} \subset V$ for L.I. e tal que $\langle v_1, \cdots, v_n \rangle = V$, dizemos que $\{v_1, \cdots, v_n\}$ é uma base de V.

Teorema 4.2.5. *Todo subconjunto linearmente independente* $S = \{y_1, \cdots, y_j\}$ *de um espaço vetorial* V *de dimensão* $n \geq 1$ *pode ser completado para formar uma base de* V*.*

A demonstração desse teorema pode ser encontrada em BUENO (2006. p. 5).

Teorema 4.2.6.

a) Todo espaço vetorial V *sobre um corpo* K *possui uma base.*

b) Se um espaço vetorial V *sobre um corpo* K *possui uma base com* n *elementos então, toda base de* V *possui* n *elementos.*

Demonstração. (a) Como $V \neq \{\vec{0}\}$, podemos considerar $\vec{0} \neq \vec{v} \in V$.

Note que $\vec{v}$ é L.I, então pelo Teorema 4.2.5 este conjunto pode ser estendido a uma base de V.

(b) Sejam $\beta = \{\vec{v_1}, \cdots, \vec{v_m}\}$ e $\gamma = \{\vec{u_1}, \cdots, \vec{u_n}\}$ bases de V. Mostraremos que $m = n$.

Como β gera V e γ é L.I, implica que $n \leq m$ e como γ gera V e β é L.I, imploca que $m \leq n$. Portanto, $m = n$. □

Definição 4.2.7. *Sejam V um espaço vetorial sobre o corpo K e $\{v_1, \cdots, v_n\}$ uma base de V com n elementos, chamamos ao número n de dimensão de V sobre K e denotamos $[V : K] = n$.*

Diz-se que um espaço vetorial V tem *dimensão finita* quando admite uma base com um número finito de elementos.

4.3 GRUPOS

Nesta seção abordaremos outro ponto chave para a Teoria de Galois, a Teoria de Grupos.

4.3.1 Definições, Propriedades e Exemplos

Seja G um conjunto não vazio onde está definida uma operação entre pares de G, denotada por

$$\begin{aligned} * : G \times G &\to G. \\ (x, y) &\mapsto x * y \end{aligned}$$

Dizemos que o par $(G, *)$ é um grupo se são válidas as seguintes propriedades:

i) Associatividade:

$a * (b * c) = (a * b) * c$, $\forall\, a, b, c \in G$;

ii) Elemento Neutro:

Existe $e \in G$ tal que $a * e = e * a$, $\forall\, a \in G$;

iii) Elemento Simétrico:

Para cada $a \in G$, existe $b \in G$ tal que $a * b = b * a = e$.

Um elemento e satisfazendo o item *ii*) é chamado *elemento neutro* de G e, o elemento b que satisfaz o item *iii*) é dito *simétrico* de a em G, que denotaremos por a^{-1}.

Dizemos que o grupo $(G, *)$ é um grupo *abeliano*, se satisfaz a seguinte propriedade:

iv) Comutatividade:

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

A fim de simplificar notações, usaremos G em vez de $(G, *)$ para denotar um grupo. Usaremos ab, em vez de $a * b$, para representar o resultado de a operado com b. Ainda, usaremos a notação aditiva $a * b = a + b$ apenas para grupos abelianos e, nesse caso, o simétrico de a é denotado por $-a$ e $b + (-a)$ é denotado simplesmente por $b - a$, e o elemento neutro será representado por 0.

Exemplo 4.3.1.

a) $(\mathbb{Z}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ *são grupos abelianos;*

b) $(\mathbb{Z}_n, +)$ *é grupo abeliano finito com n elementos;*

c) Seja $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$. $(\mathbb{R}^*, \cdot)$ *é grupo abeliano;*

d) $(\mathbb{N}, +), (\mathbb{N}^*, \cdot)$ *e* $(\mathbb{Z}^*, \cdot)$ *não são grupos.*

De fato, em $(\mathbb{N}, +)$ o elemento neutro é zero, mas para $1 \in \mathbb{N}$ não existe $x \in \mathbb{N}$ tal que $1 + x = 0$. Em $(\mathbb{N}^*, \cdot)$ e $(\mathbb{Z}^*, \cdot)$, o elemento neutro é 1, mas para $2 \in \mathbb{N}^* \subset \mathbb{Z}^*$, não existe $x \in \mathbb{Z}^*$ tal que $2 \cdot x = 1$.

Proposição 4.3.2. *Seja G um grupo. Então*

a) Existe um único elemento neutro em G;

b) Para cada $a \in G$*, existe um único simétrico de a em G;*

c) Se $a \in G$ *e* $a^{-1} \in G$ *é o simétrico de a, então o simétrico de* a^{-1} *é a, ou seja,* $\left(a^{-1}\right)^{-1} = a$*;*

d) Se $a, b \in G$ *e* $a^{-1}, b^{-1} \in G$ *são seus simétricos, então o simétrico de ab é* $b^{-1}a^{-1}$.

Demonstração. (a) Supondo que e e $\hat{e}$ sejam elementos neutros de G, temos $e\hat{e} = \hat{e}$ e $e\hat{e} = e$, donde $e = \hat{e}$.

(b) Sejam a' e $\hat{a}$ os simétricos de a em G. Desse modo, $aa' = e = \hat{a}a$, donde segue que

$$\hat{a} = \hat{a}e = \hat{a}(aa') = (\hat{a}a)a' = ea' = a'.$$

(c) De fato, de a^{-1} ser o simétrico de a, temos

$$a^{-1}a = aa^{-1} = e,$$

o que, por definição, significa que $\left(a^{-1}\right)^{-1} = a$.

(d) Basta notar que

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$$

e

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

Logo, $(ab)^{-1} = b^{-1}a^{-1}$. □

Exemplo 4.3.3. *Seja S um conjunto não vazio e considere*

$$G = \{f : S \to S; f \text{ bijetiva}\}.$$

Se $\circ$ é a operação "composição de funções", isto é

$$\begin{aligned} \circ : G \times G &\to G, \\ (g, f) &\mapsto g \circ f \end{aligned}$$

então G é um grupo tendo a função identidade

$$\begin{aligned} id_S : S &\to S \\ x &\mapsto x \end{aligned}$$

como elemento neutro.

Esse grupo é chamado de *Grupo das Permutações do Conjunto S* e chamamos de permutação um elemento $f \in G$. No caso em que $S = \{1, 2, \cdots, n\}$, denotaremos esse grupo por S_n, e temos que o número de elementos de S_n é exatamente $n!$.

Agora, vamos mostrar que os grupos S_n, $n \geq 3$, são exemplos de grupos não abelianos. De fato, sejam $f, g \in S_n$ definidas como segue

- $f : \{1, 2, 3, \cdots, n\} \to \{1, 2, 3, \cdots, n\}$, dada por $f(1) = 2, f(2) = 1$, $f(x) = x$, para cada $3 \leq x \leq n$;
- $g : \{1, 2, 3, \cdots, n\} \to \{1, 2, 3, \cdots, n\}$ dada por $g(1) = 2, g(2) = 3, g(3) = 1$ e se $n \geq 4$, $g(x) = x$, para cada $4 \leq x \leq n$.

Note que

$$(g \circ f)(1) = g\big(f(1)\big) = g(2) = 3 \text{ e } (f \circ g)(1) = f\big(g(1)\big) = f(2) = 1.$$

Assim, temos que $g \circ f \neq f \circ g$.

Em particular, S_3 é um exemplo de um grupo não abeliano com exatamente seis elementos.

É usual denotar um elemento f do grupo S_n por,

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix}.$$

Assim, o grupo S_3 é composto dos seguintes seis elementos:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f_1^{-1},$$
$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f_2^{-1}, \qquad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_3^{-1},$$
$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_5^{-1}, \qquad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_4^{-1}.$$

Observação 4.3.4. *Uma permutação $\alpha \in S_n$ é denominada um p-ciclo, $p \leq n$, se existem elementos distintos $a_1, \cdots, a_p \in \{1, \cdots, n\}$ tais que*

$$\alpha(a_1) = a_2, \alpha(a_2) = a_3, \cdots, \alpha(a_{p-1}) = a_p, \alpha(a_p) = a_1,$$

e

$$a(j) = j, \forall\, j \in \{1, \cdots, n\} \backslash \{a_1, \cdots, a_p\}.$$

Tal $p-$ ciclo será denotado por $(a_1 \cdots a_p)$ e o número p é chamado o comprimento do ciclo.

Os $2-ciclos$ são também chamados de transposições. Chamamos de permutação par uma permutação que pode ser expressa como o produto de um número par de transposições, e denotamos o grupo de permutações pares de S_n por A_n.

A demonstração do que foi citado acima, pode ser encontrada em MARTIN (2010, p. 172).

Exemplo 4.3.5. *Seja* $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}$ *um elemento do grupo* S_5.

Escrevendo f na notação de ciclos, obtemos $f = (1\,4)(2\,5) \in S_5$. Note que, f pode ser escrita como o produto de duas transposições, assim, f é dita uma permutação par.

Definição 4.3.6. *Sejam G um grupo e $x \in G$. Se $n \in \mathbb{Z}$ definimos x^n como segue:*

$$x^n = \begin{cases} e, & se\ n = 0; \\ x^{n-1} \cdot x, & se\ n > 0; \\ (x^{-n})^{-1}, & se\ n < 0. \end{cases}$$

Se $m, n \in \mathbb{Z}$ pode-se provar, usando indução, as seguintes propriedades:

i) $x^m \cdot x^n = x^{m+n}$;

ii) $(x^m)^n = x^{mn}$.

Se denotarmos $\langle x \rangle = \{x^m; m \in \mathbb{Z}\} \subset G$, como $x^0 = e$, $(x^m)^{-1} = x^{-m}$ e $x^m \cdot x^n = x^{m+n}$, segue que $\langle x \rangle$ é um exemplo de subgrupo abeliano. O subgrupo $\langle x \rangle$ de G é chamado *subgrupo gerado* por x. Ainda, o grupo $\langle x \rangle$ é chamado *grupo cíclico* gerado pelo elemento $x \in G$. Observe que, todo grupo cíclico é abeliano.

Lema 4.3.7. *Os ciclos* $(1\,2)$ *e* $(1\,2\cdots n)$ *geram o grupo* S_n.

A demonstração desse lema pode ser encontrada em GONÇALVES (2015, p. 164).

4.4 SUBGRUPOS E CLASSES LATERAIS

Nesta seção definiremos conceitos e traremos alguns resultados importantes, dentre eles o Teorema de Lagrange.

Definição 4.4.1. *Seja $(G, *)$ um grupo e consideremos $H \subset G$, sendo $H \neq \varnothing$. Dizemos que H é subgrupo de G quando:*

i) $e \in H$;

ii) $\forall\, a, b \in H \Rightarrow ab \in H$;

iii) $(H, *)$ *é um grupo.*

Quando H é subgrupo de G, denotamos $H \leq G$.

A seguir, veremos algumas proposições e exemplos sobre subgrupos.

Proposição 4.4.2. *Seja G um grupo e H um subconjunto de G. As seguintes condições são equivalentes:*

a) $H \leq G$;

b) Valem:

i) $e \in H$;

ii) $\forall\, a \in H$ *tem-se* $a^{-1} \in H$;

iii) $\forall\, a, b \in H$ *tem-se* $ab \in H$.

c) $H \neq \varnothing$ *e* $\forall\, a, b \in H$ *tem-se* $ab^{-1} \in H$.

Demonstração. (a) $\Rightarrow$ (b) Seja $H \leq G$. Precisamos verificar os itens $i), ii)$ e $iii)$. Da Definição 4.4.1, temos que $e \in H$ e $(H, *)$ é um grupo. Em particular, temos o item $i)$. Pelo fato de $(H, *)$ ser grupo, temos que para cada $a \in H$, existe $a^{-1} \in H$, logo temos $ii)$. E por fim, note que a operação $*$ é fechada em H, isto é $* : H \times H \to H$, e portanto para cada $a, b \in H$, temos $ab \in H$, ou seja, vale $iii)$.

(b) $\Rightarrow$ (c) Primeiro, note que $H \leq \varnothing$ pois pelo item i), temos que $e \in H$. Dados $a, b \in H$, pelo item ii) temos que $b^{-1} \in H$. Assim, $a, b^{-1} \in H$ e pelo item iii) temos que $ab^{-1} \in H$.

(c) $\Rightarrow$ (a) Precisamos verificar os três itens da Definição 4.4.1. Como $H \neq \varnothing$, existe $c \in H$. Por hipótese, $cc^{-1} \in H$. Logo, vale o item i) (da definição), ou seja, H possui o neutro da operação. Agora, dado $b \in H$, temos $e, b \in H$, donde $b^{-1} = eb^{-1} \in H$, por hipótese. Ou seja, para cada elemento de H, temos que o seu simétrico também está em H.

Sejam $a, b \in H$. Sabemos que $b^{-1} \in H$. Utilizando a hipótese, e a Proposição 4.5.1 obtemos

$$ab = a\big(b^{-1}\big)^{-1} \in H,$$

ou seja, a operação fechada em H.

Por fim, a associatividade de H é herdada de G e portanto $(H, *)$ é um grupo, com a operação de G, de modo que está provado que $H \leq G$. □

Exemplo 4.4.3. *Seja* $H = \{x \in \mathbb{R}^*; x > 0\}$. *Mostraremos que* $(H, \cdot) \leq (\mathbb{R}^*, \cdot)$.

Note que $H \neq 0$, pois $1 > 0$. Portanto, $1 \in H$. Ainda, para todo $b \in H$ temos que $b > 0$. Assim, $b^{-1} = \dfrac{1}{b} > 0$ e

$$\forall\, a, b \in H \Rightarrow a > 0 \text{ e } b^{-1} > 0 \Rightarrow ab^{-1} > 0 \Rightarrow ab^{-1} \in H.$$

Logo, pela Proposição 4.4.2, item c) segue que $(H, \cdot) \leq (\mathbb{R}^*, \cdot)$.

Proposição 4.4.4. *Sejam* $x, y \in G$ *e* $H \leq G$. *Então* $x \equiv y (mod\, H) \Leftrightarrow xy^{-1} \in H$ *define uma relação de equivalência no conjunto* G.

Demonstração. Para mostrar que $x \equiv y (mod\, H) \Leftrightarrow xy^{-1} \in H$ é relação de equivalência, devemos mostrar que esta é reflexiva, simétrica e transitiva.

(i) Reflexiva: $x \equiv x\, (mod\, H)$, para cada $x \in G$, pois $x \cdot x^{-1} = e \in H$;

(ii) Simétrica: $x \equiv y\, (mod\, H) \Rightarrow y \equiv x\, (mod\, H)$. De fato, se $xy^{-1} \in H$ então, $yx^{-1} = (xy^{-1})^{-1} \in H$.

(iii) Transitiva: $x \equiv y\,(mod\,H)$ e $y \equiv z\,(mod\,H) \Rightarrow x \equiv z\,(mod\,H)$. De fato, se

$$xy^{-1} \in H \text{ e } yz^{-1} \in H \Rightarrow xz^{-1} = (xy^{-1})(yz^{-1}) \in H.$$

Por $(i), (ii)$ e (iii), temos o que se pede. □

Consideremos agora $H \leq G$ e $x \in G$. Temos então a classe de equivalência de x, dada por

$$\bar{x} = \{y \in G; y \equiv x\,(mod\,H)\}.$$

Assim,

$$y \in \bar{x} \Leftrightarrow y \equiv x\,(mod\,H) \Leftrightarrow yx^{-1} = h, \text{ para algum } h \in H \Leftrightarrow y = hx,$$

para algum $h \in H$.

Se denotarmos $Hx = \{hx; h \in H\}$ então, temos que $\bar{x} = Hx$ que é chamada *classe lateral (à direita) de x, de H em G*. De maneira análoga, teremos que $xH = \{xh; h \in H\}$, chamada *classe lateral (à esquerda) de x de H em G*, será dada pela classe de equivalência do elemento $x \in G$ na relação de equivalência dada por $x \cong y \Leftrightarrow x^{-1}y \in H$.

Com a representação de classes laterais (à direita), denotaremos o conjunto quociente $\{\bar{x}; x \in G\}$ por G/H, ou seja, $G/H = \{Hx; x \in G\} = \{hx; h \in H\}; x \in G$ é o conjunto de todas as classes laterais (à direita) de H em G.

Exemplo 4.4.5. *Seja $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$. Vamos determinar as classes laterais à esquerda e à direita de $H = \{\bar{0}, \bar{2}\}$ em $(\mathbb{Z}_4, +)$ para cada elemento de $\mathbb{Z}_4$.*

Como $\mathbb{Z}_4$ é grupo aditivo, temos que

$$x + H = \{x + h; h \in H\} \text{ e } H + x = \{h + x; h \in H\}.$$

Assim,

- $\bar{0} + H = H + \bar{0} = \{\bar{0}, \bar{2}\}$;
- $\bar{2} + H = H + \bar{2} = \{\bar{0}, \bar{2}\}$;
- $\bar{1} + H = H + \bar{1} = \{\bar{1}, \bar{3}\}$;
- $\bar{3} + H = H + \bar{3} = \{\bar{1}, \bar{3}\}$.

Note que, $\bar{0} + H = \bar{2} + H$ e $\bar{1} + H = \bar{3} + H$. Daí, segue que

$$(\bar{0} + H) \cap (\bar{1} + H) = \varnothing \text{ e } \mathbb{Z}_4 = (\bar{0} + H) \cup (\bar{1} + H).$$

Definição 4.4.6. *Seja A um conjunto não vazio. Define-se como partição de A, qualquer subconjunto P de $P(A)$, onde $P(A)$ é o conjunto das partes de A, que satisfaz as seguintes condições, onde $P(A) = \{A_1, A_2, \cdots, A_n\}$:*

i) $A_i \neq \varnothing$, *para* $i = 1, 2, \cdots, n$;

ii) $A_i \subset A$, *para* $i = 1, 2, \cdots, n$;

iii) $A = A_1 \cup A_2 \cup \cdots \cup A_n$;

iv) $A_i \cap A_j = \varnothing$, *para* $i \neq j$, *com* $i, j = 1, 2, \cdots, n$.

Exemplo 4.4.7. *Se* $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$, *então* $X = \{\{1, 3\}, \{2, 4, 7\}, \{5\}, \{6, 8\}\}$ *é uma partição de A, com quatro elementos.*

Suponhamos agora que G/H possui exatamente n classes laterais (à direita) distintas, ou seja, $G/H = \{Hx_1, Hx_2, \cdots, Hx_n\}$ onde $x_1, x_2, \cdots, x_n \in G$. Como $\{Hx_1, \cdots, Hx_n\}$ é uma partição de G temos que $Hx_i \cap Hx_j = \varnothing$ se $i \neq j$, isto é, duas classes laterais à direita são iguais ou disjuntas e mais ainda, $G = Hx_1 \cup \cdots \cup Hx_n$. Assim, a união das classes laterais à direita disjuntas é G.

Se G é um grupo finito, definimos a *ordem de G* como sendo o número de elementos de G, e denotamos por $|G|$. Além disso, para $a \in G$, definimos a ordem de a como sendo $\big|\langle a \rangle\big|$, e denotamos simplesmente por $|a|$.

Teorema 4.4.8. *(Teorema de Lagrange) Se G é um grupo finito e $H \leq G$, então $|H|$ é um divisor de $|G|$ (isto é, a ordem de H é um divisor da ordem de G).*

Demonstração. Suponhamos que G seja um grupo finito e $H \leq G$. Assim, temos que o conjunto G/H das classes laterais distintas (à direita) de G é finito e $|G/H| = n$, para algum $n \in \mathbb{N}$.

Seja $G/H = \{Hx_1, \cdots, Hx_n\}$ o conjunto das classes laterais à direita. Desta forma, temos que $G = Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n$ e $Hx_i \cap Hx_j = \varnothing$ para $i \neq j$.

Agora, para cada $1 \leq i \leq n$, considere a função

$$\begin{aligned} \psi_i : H &\to Hx_i \\ h &\mapsto hx_i. \end{aligned}$$

Temos que ψ_i é sobrejetiva, e ainda, se $\psi(h) = \psi(h')$ obtém-se $hx_i = h'x_i$ e então $h = h'$, ou seja, ψ_i é bijetiva. Portanto, $|Hx_i| = |H|$, para cada $i \in \{1, 2, \cdots, n\}$. Logo,

$$|G| = |Hx_1| + |Hx_2| + \cdots + |Hx_n| = |H| + |H| + \cdots + |H| = n \cdot |H|.$$

E, portanto, $|H| \Big| |G|$. □

Corolário 4.4.9. *Todo grupo finito de ordem prima é cíclico (em particular é abeliano).*

Demonstração. Seja G um grupo tal que $|G| = p$, onde p é um número primo. Se $x \in G$, $x \neq e$, então $\langle x \rangle$ é um subgrupo de G contendo o conjunto $\{e, x\}$. Assim, pelo Teorema de Lagrange, temos que $\big|\langle x \rangle\big|$ é um divisor de $|G| = p$ e $\big|\langle x \rangle\big| > 1$.

Portanto, $\big|\langle x \rangle\big| = p$ e isso nos diz que $G = \langle x \rangle$. □

Corolário 4.4.10. *Se G é um grupo tal que $|G| \leq 5$ então G é abeliano.*

Demonstração. Se $|G| = 1$ então, $G = \{e\}$, que é abeliano.

Se $|G| = 2, |G| = 3$ e $|G| = 5$, pelo Corolário 4.4.9 segue que G é abeliano.

Para $|G| = 4$, temos a seguinte solução. Se existe $x \neq e, x \in G$, tal que $\langle x \rangle = G$, então G é cíclico e, portanto, abeliano.

Suponhamos então que para qualquer $x \in G$, com $x \neq e$, temos $\langle x \rangle \neq G$. Daí, pelo Teorema de Lagrange segue que $\big|\langle x \rangle\big| = 2$. Assim,

$$x^2 = e \Rightarrow x^{-1} = x, \forall\, x \in G.$$

Portanto, se $x, y \in G$ tem-se $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$, ou seja, G é abeliano. □

4.5 GRUPOS QUOCIENTES E HOMOMORFISMOS DE GRUPOS

Sejam G um grupo e $H \leq G$. Para $g \in G$, definimos a função ψ_g (conjugação pelo elemento $g \in G$) por,

$$\begin{aligned} \psi_g : G &\to G \\ x &\mapsto \psi_g(x) = x^g = g^{-1}xg. \end{aligned}$$

Observe que $\psi_g(H) = \{\psi_g(h); h \in H\} = \{h^g = g^{-1}hg; h \in H\}$, que denotaremos por H^g ou $g^{-1}Hg$, também é um subgrupo de G, pois:

i) $e = g^{-1}eg = e^g \in H^g$, onde "$e$" é o elemento neutro de G;

ii) $h_1^g, h_2^g \in H^g \Rightarrow h_1^g h_2^g = (g^{-1}h_1g)(g^{-1}h_2g) = g^{-1}h_1(gg^{-1})h_2g = g^{-1}h_1eh_2g = = g^{-1}h_1h_2g = (h_1h_2)^g \in H^g$;

iii) $h^g \in H^g \Rightarrow (h^g)^{-1} = (g^{-1}hg)^{-1} = g^{-1}h^{-1}g = (h^{-1})^g \in H^g$.

Assim, a função conjugação transforma subgrupos de G em subgrupos de G.

Dizemos que um subgrupo $H \leq G$ é *normal* (ou *invariante* em G) se $\psi_g(H) = H^g \subseteq H$, para cada $g \in G$.

Note que $H^g \subseteq H \Rightarrow g^{-1}Hg \subseteq H$ e $H^{g^{-1}} \subseteq H$. Daí, $(g^{-1})^{-1} H (g^{-1}) \subseteq H$ e portanto $gHg^{-1} \subseteq H$. Daí, $H \subseteq g^{-1}Hg \subseteq H$, ou seja, $H \subseteq H^g \subseteq H$, e portanto $H = H^g$.

Se H é um subgrupo normal de G, então denotaremos por $H \triangleleft G$. Note que, $\{e\}$ e G são sempre subgrupos normais de G. Ainda, se G é um grupo abeliano, então qualquer subgrupo H de G é normal em G, pois para cada $g \in G$, temos $H^g = \{g^{-1}hg; h \in H\} = \{h; h \in H\} = H$.

Dizemos que um grupo $G \neq \{e\}$ é *simples* se os únicos subgrupos normais de G são $\{e\}$ e G.

No que segue, veremos algumas proposições sobre subgrupos normais.

Proposição 4.5.1. *Seja G um grupo. Então,*

a) $N \triangleleft G \Leftrightarrow Ng = gN, \forall\, g \in G$, *onde* $gN = \{gn; n \in N\}$;

b) $N_1, N_2 \triangleleft G \Rightarrow N_1 \cap N_2 \triangleleft G$*;*

c) $H \leq G$ *e* $N \triangleleft G \Rightarrow HN = \{hn; h \in H, n \in N\}$ *é um subgrupo de* G*;*

d) $N_1 \triangleleft G, N_2 \triangleleft G \Rightarrow N_1N_2 \triangleleft G$*;*

e) $H \leq G, N \triangleleft G \Rightarrow H \cap N \triangleleft H$*.*

Demonstração. (a) Observemos que $N \triangleleft G \Leftrightarrow N^g = g^{-1}Ng = N \Leftrightarrow Ng = gN$, para cada $g \in G$.

(b) Seja $x \in N_1 \cap N_2$ e $g \in G$. Desta forma, temos que $x \in N_1$ e $x \in N_2$ e, assim, $x^g \in N_1^g = N_1$ e $x^g \in N_2^g = N_2$, ou seja, $x^g \in N_1 \cap N_2$. Logo, $(N_1 \cap N_2)^g = N_1 \cap N_2$, para cada $g \in G$.

(c) Seja $H \leq G$ e $N \triangleleft G$. Vamos provar que $L = HN = \{hn; h \in H, n \in N\}$ é um subgrupo de G. De fato,

i) $e = ee \in HN$.

ii) Note que

$$h_1n_1, h_2n_2 \in L \Rightarrow (h_1n_1)(h_2n_2) = h_1\big((h_2h_2^{-1})n_1h_2\big)n_2$$
$$\Rightarrow (h_1n_1)(h_2n_2) = (h_1h_2)\big(h_2^{-1}n_1h_2\big)n_2 = (h_1h_2)\big((n_1)^{h_2}n_2\big)$$

e tomando $h = h_1h_2$ e $n = n_1^{h_2}n_2$ teremos $h \in H$, $n_1^{h_2} \in N^{h_2} = N$ e $n = n_1^{h_2}n_2 \in N$ e, assim,

$$(h_1n_1)(h_2n_2) = hn \in L = HN.$$

iii) Observe que $x = hn \in L$ implica que $x^{-1} = (hn)^{-1} = n^{-1}h^{-1} = h^{-1}(hn^{-1}h^{-1})$. Porém, $h^{-1} \in H$ e $hn^{-1}h^{-1} = (n^{-1})^{h^{-1}} \in N^{h^{-1}} = N$ e, portanto, $x^{-1} \in L = HN$.

(d) Observamos que para cada $g \in G$, tem-se

$$(N_1N_2)^g = g^{-1}(N_1N_2)g = (g^{-1}N_1g)(g^{-1}N_2g) = N_1^gN_2^g.$$

Como $N_1^g = N_1$, $N_2^g = N_2$, para cada $g \in G$, segue que $(N_1N_2)^g = N_1N_2$, para cada $g \in G$.

(e) Seja $x \in H \cap N$ e $h \in H$. Então $x \in N$ e $x^h \in N^h = N$. Como $x, h \in H$, segue que $h^{-1}xh = x^h \in H$, e portanto, $x^h \in H \cap N$, para cada $h \in H$. □

Agora, considere G um grupo e $H \triangleleft G$. De acordo com a Proposição 4.4.4, temos que $G/H = \{\overline{g}; g \in G\}$ é o conjunto quociente de G pela relação de equivalência $x \cong y \Leftrightarrow xy^{-1} \in H$, dizemos que $\overline{g} = Hg = \{hg; h \in H\}$ é a classe de equivalência módulo H tendo g como representante.

Sendo $H \triangleleft G$ vamos agora introduzir uma operação no conjunto das classes G/H de modo que G/H seja um grupo com esta operação, tal grupo receberá o nome de *grupo quociente* de G por H. Defina $*$ por,

$$\begin{aligned} * : G/H \times G/H &\to G/H, \\ (Hx, Hy) &\mapsto Hxy \end{aligned}$$

ou seja, $\overline{x} * \overline{y} = \overline{xy}$.

Proposição 4.5.2. *Seja G um grupo e $H \triangleleft G$. Então, a operação $\overline{x} * \overline{y} = \overline{xy}$, para cada $x, y \in G$, define uma operação no conjunto das classes G/H e mais ainda, G/H é um grupo com essa operação.*

Demonstração. Para demonstrarmos que $\overline{x} * \overline{y} = \overline{xy}$ define uma operação em G/H temos que provar que a definição acima não depende da escolha dos representantes das classes. De fato, se $\overline{x} = \overline{a}$ e $\overline{y} = \overline{b}$ provaremos que $\overline{x} * \overline{y} = \overline{a} * \overline{b}$, isto é, $\overline{xy} = \overline{ab}$.

Para isso é suficiente provarmos que $Hxy = Hab$ ou ainda $(xy)(ab)^{-1} \in H$. Mas $xy(ab)^{-1} = xyb^{-1}a^{-1}$ e $\overline{x} = \overline{a}$, $\overline{y} = \overline{b}$ nos diz que $xa^{-1} \in H$, $yb^{-1} \in H$.

Se $xa^{-1} = h_1 \in H$, $yb^{-1} = h_2 \in H$ então,

$$(xy)(ab)^{-1} = x(yb^{-1})a^{-1} = x(h_2)a^{-1} = (h_1a)(h_2)a^{-1} = h_1(ah_2a^{-1})$$

e como $h_1 \in H$ e $ah_2a^{-1} \in H^{a^{-1}} = H$, pois $H \triangleleft G$, segue que

$$(xy)(ab)^{-1} \in H.$$

Assim, nossa definição não depende da escolha dos representantes.

Agora, se e é a identidade de G, então,

i) $\overline{e} = He = H$ é o elemento identidade de G/H, pois $\overline{e} * \overline{x} = \overline{ex} = \overline{x} = \overline{xe} = = \overline{x} * \overline{e}$, para cada $\overline{x} \in G/H$.

ii) $\overline{x} * (\overline{y} * \overline{z}) = \overline{x} * \overline{(yz)} = \overline{x(yz)} = \overline{(xy)z} = \overline{(xy)} * \overline{z} = (\overline{x} * \overline{y}) * \overline{z}$, para cada $\overline{x}, \overline{y}, \overline{z} \in G/H$.

iii) se $\overline{x} \in G/H$ então $\exists \overline{x^{-1}} \in G/H$ tal que $\overline{x^{-1}} * \overline{x} = \overline{x} * \overline{x^{-1}} = \overline{e}$, ou seja, todo elemento $\overline{x} \in G/H$ possui simétrico em G/H.

Portanto, $\overline{G} = G/H$ é um grupo com a operação definida pela regra $\overline{x} * \overline{y} = \overline{xy}$, para cada $\overline{x}, \overline{y} \in \overline{G}$. □

Proposição 4.5.3. *Seja G um grupo e $H \triangleleft G$. Então,*

a) Se G abeliano, então $\overline{G} = G/H$ é abeliano;

b) Se G cíclico, então $\overline{G} = G/H$ é cíclico.

Demonstração. (a) Sejam $\overline{x}, \overline{y} \in \overline{G} = G/H$. Então,

$$\overline{x} * \overline{y} = \overline{xy} = \overline{yx} = \overline{y} * \overline{x}.$$

(b) Se $G = \langle x \rangle = \{x^m; m \in \mathbb{Z}\}$ então para cada $\overline{y} = Hy \in \overline{G} = G/H$ temos que $y \in G = \langle x \rangle$ e, assim, $y = x^m$ para algum $m \in \mathbb{Z}$. Daí segue que

$$\overline{y} = \overline{x^m} = \overline{x}^m \in \langle \overline{x} \rangle = \{\overline{x}^r; r \in \mathbb{Z}\}.$$

Portanto, $\overline{G} = \langle \overline{x} \rangle$. □

Se estamos utilizando a notação aditiva para um grupo G e $H \triangleleft G$, então denotaremos também aditivamente o grupo quociente G/H. Desta forma,

$$(H + x) + (H + y) = \overline{x} + \overline{y} = \overline{x + y} = H + (x + y),$$

onde

$$\overline{x} = H + x = \{h + x; h \in H\}$$

e

$$\overline{y} = H + y = \{h + y; h \in H\}.$$

Proposição 4.5.4. *Sejam G um grupo, $H \triangleleft G$ e $\overline{G} = G/H$ o grupo quociente de G por H. Então,*

$$\pi : G \to \overline{G}$$
$$x \mapsto \pi(x) = \overline{x}$$

é uma função sobrejetiva (projeção canônica) tal que:

a) $\pi(xy) = \pi(x) * \pi(y), \forall\, x, y \in G$;

b) $H = \{x \in G; \pi(x) = \overline{e}\}$ *onde e é a identidade de G e $\overline{e}$ é a identidade de $\overline{G}$.*

Demonstração. (a) Note que $\pi(xy) = \overline{xy} = \overline{x} * \overline{y} = \pi(x) * \pi(y)$, para cada $x, y \in G$.

(b) Observe que

$$\pi(x) = \overline{e} \Leftrightarrow \overline{x} = \overline{e} \Leftrightarrow x \in H.$$

□

No que segue, vamos definir e ver alguns resultados sobre homomorfismos de grupos.

Definição 4.5.5. *Sejam G e G' grupos e $\psi : G \to G'$ uma função de G em G'. Dizemos que ψ é um homomorfismo de grupos se $\psi(xy) = \psi(x)\psi(y)$, para cada $x, y \in G$.*

Exemplo 4.5.6. *Observe que a projeção canônica $\pi : G \to \overline{G} = G/H$ definida na Proposição 4.5.4 é um homomorfismo de grupos de G sobre G/H.*

Proposição 4.5.7. *Seja $\psi : G \to G'$ um homomorfismo de grupos. Então:*

a) $\psi(e) = e'$, *onde e, e' são os neutros de G, G', respectivamente;*

b) $\psi(g)^{-1} = \psi(g^{-1}), \forall\, g \in G$.

Demonstração. Sejam $(G,\cdot)$ e $(G',*)$ grupos $\psi : G \to G'$ um homomorfismo. Temos que

(a) $\psi(e) = \psi(e\cdot e) = \psi(e) * \psi(e)$. Operando em ambos os lados da igualdade com $\big(\psi(e)\big)^{-1}$, obtemos $e' = \psi(e)$.

(b) $e' = \psi(e) = \psi(g\cdot g^{-1}) = \psi(g) * \psi(g^{-1})$. Analogamente, $e' = \psi(g^{-1}) * \psi(g)$. Dessas igualdades segue que $\psi(g^{-1}) = \psi(g)^{-1}$. □

Se a função $\psi : G \to G'$ for um homomorfismo de grupos bijetor, dizemos que ψ é um *isomorfismo*. Nesse caso podemos simplesmente dizer que G é *isomorfo* a G' e denotamos por $G \simeq G'$. Os isomorfismos de grupos de G sobre si mesmo, ou seja, $\psi : G \to G$, são chamados de *automorfismos* de G. A seguir, um exemplo de automorfismo.

Exemplo 4.5.8. *Seja p um número primo. A aplicação $f : \mathbb{Z}[\sqrt{p}] \longrightarrow \mathbb{Z}[\sqrt{p}]$, $f(a+b\sqrt{p}) = a - b\sqrt{p}$ é um automorfismo do grupo $(\mathbb{Z}[\sqrt{p}],+)$.*

De fato, sejam $a+b\sqrt{p}, c+d\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$. Temos que

$$\begin{aligned} f\big((a+b\sqrt{p}) + (c+d\sqrt{p})\big) &= f\big((a+c) + (b+d)\sqrt{p}\big) \\ &= (a+c) - (b+d)\sqrt{p} \\ &= (a - b\sqrt{p}) + (c - d\sqrt{p}) \\ &= f(a+b\sqrt{p}) + f(c+d\sqrt{p}). \end{aligned}$$

Portanto, f é homomorfismo de grupos.

Note que para $a+b\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$, tomamos $a - b\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$, e obtemos que $f(a-b\sqrt{p}) = a+b\sqrt{p}$. Assim, temos que f é uma aplicação sobrejetiva.

Ainda, note que, se $f(a+b\sqrt{p}) = f(c+d\sqrt{p})$ então,

$$a - b\sqrt{p} = c - d\sqrt{p} \Rightarrow a = c \text{ e } b = d \Rightarrow (a+b\sqrt{p}) = (c+d\sqrt{p}),$$

ou seja, f é injetora.

Como f é injetora e sobrejetora, temos que f é um homomorfismo de grupos bijetor e, sendo f uma aplicação de $\mathbb{Z}[\sqrt{p}]$ em $\mathbb{Z}[\sqrt{p}]$, segue que f é automorfismo do grupo $\big(\mathbb{Z}[\sqrt{p}],+\big)$.

As funções $\psi_g : G \to G$, conjugação pelo elemento $g \in G$, apresentadas no início desta subseção são exemplos de automofirmos de G, chamados *automorfismos internos* de G. Denotaremos por $Inn\,(G)$ o conjunto dos automorfismos internos de G.

A seguir, veremos alguns resultados sobre homomorfismos de grupos.

Proposição 4.5.9. *Se G é um grupo e $f_1, f_2 \in Aut\,(G)$ então,*

a) $f_1 \circ f_2 \in Aut\,(G)$;

b) $f_1^{-1} \in Aut\,(G)$, *onde* f_1^{-1} *é a função inversa de* f_1.

Demonstração. (a) Sejam $f_1, f_2 \in Aut\,(G)$. Temos que

$$\begin{aligned}(f_1 \circ f_2)(xy) = f_1\big(f_2(xy)\big) &= f_1\big(f_2(x)f_2(y)\big)\\ &= f_1\big(f_2(x)\big)f_1\big(f_2(y)\big)\\ &= (f_1 \circ f_2)(x)(f_1 \circ f_2)(y),\ \forall\, x, y \in G.\end{aligned}$$

Da definição de automorfismo, temos que f_1 e f_2 são funções bijetoras e, como a composição de funções bijetoras é uma função bijetora, obtemos que $f_1 \circ f_2 \in Aut\,(G)$.

(b) Se $f_1 \in Aut\,(G)$ então, para cada $x', y' \in G$ existem $x, y \in G$ tais que $x' = f_1(x)$ e $y' = f_1(y)$.

Assim, se $h = f_1^{-1}$ temos,

$$h(x'y') = h\big(f_1(x)f_1(y)\big) = h\big(f_1(xy)\big) = (h \circ f_1)(xy) = (f_1^{-1} \circ f_1)(xy) = xy = h(x')h(y').$$

Logo, $f_1^{-1} = h \in Aut\,(G)$. □

Proposição 4.5.10. *Seja G um grupo.*

a) $\big(Aut\,(G), \circ\big)$ *é grupo;*

b) $Inn\,(G) \lhd Aut\,(G)$.

Demonstração. (a) Sejam $f, \varphi \in Aut\,(G)$. Segue da Proposição 4.5.9 que $\varphi \circ f \in Aut\,(G)$. Logo, a composição é uma operação em $Aut\,(G)$.

i) Como a composição de funções é uma operação associativa, temos que vale a associatividade em $\big(Aut\,(G), \circ\big)$.

ii) Note que a função identidade $id_G : G \to G$, $id(x) = x$, para cada $x \in G$, é o elemento neutro de $Aut\,(G)$.

iii) Seja $f \in Aut\,(G)$. Pela Proposição 4.5.9, temos que $f^{-1} \in Aut\,(G)$.

Portanto, $\big(Aut\,(G), \circ\big)$ é grupo.

(b) Mostramos primeiro que $Inn\,(G) \leq Aut\,(G)$.

Tomamos $\psi_g, \psi_h \in Inn\,(G)$ e, assim, devemos mostrar que $\psi_g \circ (\psi_h)^{-1} \in Inn\,(G)$. Note que $(\psi_h)^{-1} = \psi_{h^{-1}}$. Logo, para cada $n \in G$, temos:

$$\begin{aligned}(\psi_g \circ \psi_{h^{-1}})(x) = \psi_g\big(\psi_{h^{-1}}(x)\big) = \psi_g(h^{-1}xh) = gh^{-1}xhg^{-1} \\ = (gh^{-1})x(gh^{-1})^{-1} = \psi_{gh^{-1}}(x).\end{aligned}$$

Portanto, $\psi_g \circ \psi_{h^{-1}} = \psi_{gh^{-1}} \in Inn(G)$, ou seja, $Inn(G) \leq Aut(G)$.

Agora, tomando $\psi_g \in Inn\,(G), \varphi \in Aut\,(G)$, mostraremos que $\varphi \circ \psi_g \circ \varphi^{-1}$ é elemento de $Inn\,(G)$, ou seja, $\varphi \circ \psi_g \circ \varphi^{-1} \in Inn\,(G)$. Dado $x \in G$, temos

$$\begin{aligned}\big(\varphi \circ \psi_g \circ \varphi^{-1}\big)(x) = \varphi\Big(\psi_g\big(\varphi^{-1}(x)\big)\Big) = \varphi\Big(g\varphi^{-1}(x)g^{-1}\Big) \\ = \varphi(g)\varphi\Big(\varphi^{-1}(x)\Big)\varphi\big(g^{-1}\big) = \varphi(g)x\varphi\big(g^{-1}\big) = \varphi(g)x\varphi(g)^{-1} = \psi_{\varphi(g)}(x) \in Inn\,(G).\end{aligned}$$

Logo, $Inn\,(G) \lhd Aut\,(G)$. □

Teorema 4.5.11. *(1° Teorema do Homomorfismo) Sejam G e G' grupos com neutros "e" e "e'", respectivamente, e $\psi : G \to G'$ um homomorfismo de grupos. Então,*

a) $Im\,(\psi) = \psi(G) = \{\psi(G); g \in G\}$ é um subgrupo de G';

b) $Ker(\psi) = \{g \in G; \psi(g) = e'\}$ é um subgrupo normal de G (chamado de núcleo do homomorfismo de grupos ψ). Além disso, ψ é injetiva se, e somente se, $Ker(\psi) = \{e\}$.

Demonstração. (a) Note que $e' = \psi(e) \in Im\,(\psi)$ pois,

$$ee = e \Rightarrow \psi(e)\psi(e) \Rightarrow \psi(e) = e' \in Im\,(\psi).$$

Logo, $Im\,(\psi) \neq \varnothing$;

Considere agora $\psi(g_1)$, $\psi(g_2) \in Im\,(\psi)$. Logo,

$$\psi(g_1)\psi(g_2)^{-1} = \psi(g_1)\psi(g_2^{-1}) = \psi(g_1 g_2^{-1}) \in Im\,(\psi).$$

Segue portanto da Proposição 4.4.2, item c) que $Im(\psi) \leq G$.

(b) Note que $e \in Ker(\psi)$, pois $\psi(e) = e'$.

Considere agora $g_1, g_2 \in Ker(\psi)$. Logo, $\psi(g_1 g_2) = \psi(g_1)\psi(g_2) = e'e' = e'$. Assim, $g_1 g_2 \in Ker(\psi)$.

Seja $g \in Ker(\psi)$. Então $g^{-1} \in G$ e é tal que $\psi(g^{-1}) = \psi(g)^{-1} = = (e')^{-1} = e'$, o que implica, $g^{-1} \in Ker(\psi)$. Logo, pela Proposição 4.4.2, item b), temos que $Ker(\psi) \leq G$.

Agora, se $n \in Ker(\psi)$ e $g \in G$ temos que

$$\psi(g^{-1}ng) = \psi(g^{-1})\psi(n)\psi(g) = \psi(g)^{-1}e'\psi(g) = \psi(g)^{-1}\psi(g) = e',$$

ou seja, $g^{-1}ng \in Ker(\psi)$ para cada $n \in Ker(\psi), g \in G$. Assim, $Ker(\psi) \triangleleft G$.

Agora, resta ver a última afirmação. Sejam $x, y \in G$. Então

$$\begin{aligned}\psi(x) = \psi(y) &\Leftrightarrow \psi(x)\psi(y)^{-1} = \psi(y)\psi(y)^{-1} \\ &\Leftrightarrow \psi(x)\psi(y)^{-1} = e' \Leftrightarrow \psi(xy^{-1}) = e' \Leftrightarrow xy^{-1} \in Ker(\psi).\end{aligned}$$

Daí, se $Ker(\psi) = \{e\}$, temos que $\psi(x) = \psi(y)$ implica que $xy^{-1} = e$ e portanto $x = y$, ou seja, ψ é injetiva. Reciprocamente, se ψ é injetiva, note que para $x \in Ker(\psi)$ obtemos que $x = xe^{-1}$, e portanto $\psi(x) = \psi(e)$ então pela injetividade de ψ segue que $x = e$, neste caso $Ker(\psi) = \{e\}$. □

Teorema 4.5.12. *Seja $f : G \to G'$ um homomorfismo de grupos. Então,*

$$\begin{aligned}\overline{f} : \frac{G}{Ker(f)} &\to Im(f) \\ gKer(f) &\mapsto f(g)\end{aligned}$$

é isomorfismo de grupos.

Demonstração. Como os elementos de $\dfrac{G}{Ker(f)}$ são classes de equivalência, devemos mostrar que $\overline{f}$ não depende da escolha dos representantes da classe lateral.

Mostraremos que se $g_1Ker(f) = g_2Ker(f)$, então $\overline{f}\big(g_1Ker(f)\big) = \overline{f}\big(g_2Ker(f)\big)$.

Temos que $g_1Ker(f) = g_2Ker(f)$ implica em $g_1 \in g_2Ker(f)$. Assim,

$$\begin{aligned} g_1Ker(f) = g_2Ker(f) &\Rightarrow g_1 = g_2x \text{ para algum } x \in Ker(f) \\ &\Rightarrow f(g_1) = f(g_2x) = f(g_2)f(x) = f(g_2) \\ &\Rightarrow \overline{f}\big(g_1Ker(f)\big) = f(g_1) = f(g_2) = \overline{f}\big(g_2Ker(f)\big). \end{aligned}$$

Logo, $\overline{f}$ está bem definida.

Note que $\overline{f}$ é homomorfismo de grupos, pois dados $g_1Ker(f), g_2Ker(f) \in \dfrac{G}{Ker(f)}$ tem-se:

$$\begin{aligned} \overline{f}\big(g_1Ker(f)g_2Ker(f)\big) = \overline{f}\big(g_1g_2Ker(f)\big) &= f(g_1g_2) \\ &= f(g_1)f(g_2) = \overline{f}\big(g_1Ker(f)\big)\overline{f}\big(g_2Ker(f)\big). \end{aligned}$$

Note que $\overline{f}$ é sobrejetiva, pois dado $u \in Im(f)$, temos que $u = f(g)$, para algum $g \in G$. Tomando $gKer(f) \in \dfrac{G}{Ker(f)}$, vem que $\overline{f}\big(gKer(f)\big) = f(g) = u$.

Agora, mostraremos que $\overline{f}$ é injetiva, e faremos isso provando que $Ker\left(\overline{f}\right) = \{Ker(f)\}$.

Seja $gKer(f) \in \dfrac{G}{Ker(f)}$ então,

$$\begin{aligned} gKer(f) \in Ker\left(\overline{f}\right) \Leftrightarrow \overline{f}\big(gKer(f)\big) = e' \Leftrightarrow f(g) = e' \\ \Leftrightarrow g \in Ker(f) \Leftrightarrow gKer(f) = Ker(f). \end{aligned}$$

Portanto, $Ker\left(\overline{f}\right) = \{Ker(f)\}$ e $\overline{f}$ é isomorfismo de grupos. □

Definição 4.5.13. *Sejam p um número primo e G um grupo. Se $|G| = p^n, n \in \mathbb{N}$, dizemos que G é um p-grupo.*

Corolário 4.5.14. *Sejam G um grupo finito e $\psi : G \to G'$ um homomorfismo de grupos. Então,*

a) $\big|\psi(G)\big|$ *é um divisor de* $|G|$*;*

b) Se G *é um p-grupo, então* $\psi(G) = Im\,(\psi)$ *é também um p-grupo.*

Demonstração. (a) Observe que $G/Ker(\psi) \simeq \psi(G)$ pelo Teorema 4.5.12 temos que $|G/Ker(\psi)| = |\psi(G)|$. Como $|G/Ker(\psi)| = |G|/|Ker(\psi)|$, segue que $|G| = |Ker(\psi)| \cdot |\psi(G)|$. Logo, $|\psi(G)|$ é divisor de $|G|$.

(b) Seja G é um p-grupo. Pelo item (a), temos que $\big|\psi(G)\big|$ é divisor de $|G|$. Como $|G| = p^n$, para algum $n \in \mathbb{N}$, temos que $|\psi(G)|\big|p^n$, e portanto $|\psi(G)| = p^k$, para algum $k \in \mathbb{N}$, $k \leq n$. Logo, $\psi(G)$ é também um p-grupo. □

Definição 4.5.15. *Seja* G *um grupo. Então, chamamos de centro do grupo* G*, e denotamos por* $Z(G)$*, o conjunto* $Z(G) = \{a \in G; ax = xa, \forall x \in G\}$.

Proposição 4.5.16. *Seja* G *um grupo. Então,* $Z(G)$ *é um subgrupo de* G.

Demonstração. Primeiro observamos que $e \in Z(G)$, pois $ex = x = xe$, para cada $x \in G$. Além disso, se $a, b \in Z(G)$, então $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$, para cada $x \in G$, ou seja, $ab \in Z(G)$. Por fim, se $a \in Z(G)$, então $ax = xa$, para cada $x \in G$, e portanto $xa^{-1} = a^{-1}x$, ou seja, $a^{-1} \in Z(G)$. Logo, pela Proposição 4.4.2, item b), segue que $Z(G) \leq G$. □

O próximo resultado é um corolário do Teorema 4.5.12:

Corolário 4.5.17. *Seja* G *um grupo e* $Z(G)$ *o centro do grupo* G*. Então,* $Inn\,(G) \simeq G/Z(G)$.

Demonstração. Observe que a função,

$$\begin{aligned} \psi : G &\to Inn\,(G) \\ g &\mapsto \psi_{g^{-1}} \end{aligned}$$

é um homomorfismo de grupos tal que: $Im(\psi) = Inn\,(G)$ e $Ker(\psi) = Z(G)$. De fato, ψ é um homomorfismo de grupos, pois $\psi(gh) = \psi_{(gh)^{-1}}$ e, para cada $x \in G$, temos

$$\begin{aligned} \psi_{(gh)^{-1}}(x) &= (gh)x(h^{-1}g^{-1}) \\ &= g(h \cdot xh^{-1})g^{-1} \\ &= \psi_{g^{-1}}\big(\psi_{h^{-1}}(x)\big), \end{aligned}$$

ou seja, $\psi(gh) = \psi_{(gh)^{-1}} = \psi_{g^{-1}} \circ \psi_{h^{-1}} = \psi(g)\psi(h)$, para cada $g, h \in G$.

Agora, $Im(\psi) = Inn(G)$ e

$$\begin{aligned} Ker(\psi) &= \{g \in G; \psi_{g^{-1}} = id_g\} \\ &= \{g \in G; gxg^{-1} = x, \forall\, x \in G\} \\ &= \{g \in G; gx = xg \,\forall,\, x \in G\} = Z(G). \end{aligned}$$

Portanto, $Ker(\psi) = Z(G)$. □

Teorema 4.5.18. *(Teorema da Correspondência) Sejam G e G' grupos e $\psi : G \to G'$ um homomorfismo sobrejetivo. Então*

a) Para cada $H \leq G$ tem-se $H' = \psi(H) = \{\psi(h); h \in H\} \leq G'$. Mais ainda, se $H \triangleleft G$, então $H' \triangleleft G'$.

b) Para cada $H' \leq G'$ existe um único $H \leq G$, onde $H = \psi^{-1}(H') = \{g \in G; \psi(g) \in H'\} \supseteq Ker(\psi)$ e é tal que $\psi(H) = H'$. Além disso, se $H' \triangleleft G'$, então $H \triangleleft G$.

A demonstração desse teorema pode ser encontrada em GONÇALVES (2015, p. 149).

Definição 4.5.19. *Um grupo G diz-se solúvel se existem subgrupos $\{e\} = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_{n-1} \leq G_n = G$ tais que*

a) $G_{i-1} \triangleleft G_i, \forall\, i \in \{1, 2, \cdots, n\}$;

b) G_i/G_{i-1} é abeliano, para cada $i \in \{1, 2, \cdots, n\}$.

Assim, grupos abelianos e p-grupos são exemplos de grupos solúveis.

Teorema 4.5.20. *O grupo A_n, com $n \geq 5$ é simples.*

A demonstração desse teorema pode ser encontrada em GONÇALVES (2015, p. 165).

Corolário 4.5.21. *O grupo S_n, como $n \geq 5$, não é solúvel.*

Demonstração. Basta observar que $A_n \leq S_n$ e A_n é não solúvel, pois A_n é um grupo simples, ou seja, os únicos subgrupos normais de A_n são os triviais. □

Corolário 4.5.22. *Seja G um grupo e $N \triangleleft G$. Então, todo subgrupo do grupo quociente $\overline{G} = G/N$ é do tipo $\overline{H} = H/N$ onde H é o único subgrupo de G contendo N tal que $\pi(H) = \overline{H}$ onde $\pi : G \to \overline{G} = \overline{G}/N$ é a projeção canônica (H recebe o nome de pré-imagem de $\overline{H}$ em G). Mais ainda,*

$$\overline{H} \triangleleft \overline{G} \Leftrightarrow H \triangleleft G.$$

Demonstração. Sejam G um grupo, $N \triangleleft G$ e $\pi : G \to \overline{G} = G/N$ a projeção canônica. Pelo Teorema 4.5.18, item b), temos que para cada $\overline{H} \leq \overline{G}$, existe único $H = \pi^{-1}(\overline{H}) = \{g \in G; \pi(g) \in \overline{H}\} \supseteq Ker(\pi)$, $H \leq G$ e é tal que $\pi(H) = \overline{H}$.

O resultado segue notando que $Ker(\pi) = N$. Além disso, note que $\overline{H} \triangleleft \overline{G}$ se, e somente se, $H \triangleleft G$, decorre dos itens a) e b) do Teorema 4.5.18. □

4.6 EXTENSÕES ALGÉBRICAS DOS RACIONAIS

4.6.1 Extensões de Corpos

Nesta subseção abordaremos alguns dos conceitos necessários para estudar a Teoria de Galois para extensões de corpos K tais que $\mathbb{Q} \subset K \subset \mathbb{C}$.

Definição 4.6.1. *Seja K um anel. Chamamos de polinômio sobre K em uma indeterminada x a expressão $p(x)$ dada por $p(x) = a_0 + a_1x + \cdots + a_mx^m + \cdots$, onde $a_i \in K$, com $i \in \mathbb{N}$ e, existe $n \in \mathbb{N}$ tal que $a_j = 0$ para todo $j \geq n$.*

Observação 4.6.2. *Como existe $n \in \mathbb{N}$ tal que $a_j = 0$ para todo $j > n$ e $a_n \neq 0$, então o polinômio $p(x)$ poderá ser escrito simplesmente por $p(x) = a_0 + a_1x + \cdots + a_nx^n$, onde $a_n \neq 0$.*

Observação 4.6.3. *Denotaremos por $K[x]$ o conjunto de todos os polinômios sobre K em uma indeterminada x.*

Seja K um corpo. Se $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in K[x]$ e $q(x) = b_0+b_1x+\cdots+b_mx^m \in K[x]$ com, por exemplo $n \geq m$, completando com coeficientes iguais a zeros, se for necessário, podemos escrever $q(x) = b_0+b_1x+\cdots+b_mx^m+\cdots+b_nx^n$. Definimos as operações de adição e multiplicação de $p(x)$ com $q(x)$, respectivamente, por

$$\begin{aligned} i)\, p(x) + q(x) &= (a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) + (b_0 + b_1x + b_2b^2 + \cdots + b_nx^n) \\ &= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_n + b_n)x^n \in K[x] \end{aligned}$$

$$\begin{aligned} ii)\, p(x) \cdot q(x) &= (a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) \cdot (b_0 + b_1x + b_2b^2 + \cdots + b_nx^n) \\ &= c_0 + c_1x + c_2x^2 + \cdots + c_{an}x^{an} \in K[x], \end{aligned}$$

onde $c_k = \sum_{i+j=k} a_ib_j = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0$.

Ainda, temos que existe o elemento neutro da adição de $K[x]$ e é o polinômio identicamente nulo de K, definido por $0 + 0 \cdot x + 0 \cdot x^2 + \cdots$, em que 0 indica o zero do corpo K. Observe que, $K[x]$ é um anel com estas operações.

A demonstração do que foi descrito acima pode ser encontrada em DOMINGUES E IEZZI (2003, p. 283).

Agora, considere $p(x) = a_0+a_1x+\cdots+a_nx^n$ um polinômio não nulo de $K[x]$ tal que $a_n = 1$. Neste caso, dizemos que $p(x)$ é um *polinômio mônico* em $K[x]$. Ainda, dizemos que $p(x)$ tem *grau* n quando $a_n \neq 0$ e $a_j = 0$ para todo $j > n$ e denotamos $\partial\, p(x) = n$ para simbolizar que $p(x)$ tem grau n.

Definição 4.6.4. *Seja $p(x) \in K[x]$ tal que $\partial\, p(x) \geq 1$. Dizemos que $p(x)$ é um polinômio irredutível sobre K se, sempre que $p(x)$ é expresso como um produto $p(x) = g(x) \cdot h(x)$, com $g(x), h(x) \in K[x]$, então $g(x) = a$ ou $h(x) = b$, com $a, b \in K$. Se $p(x)$ não for irredutível sobre K dizemos que $p(x)$ é redutível sobre K.*

Lema 4.6.5. *(Lema de Gauss) Seja $p(x) \in \mathbb{Z}[x]$ tal que $p(x)$ é irredutível sobre $\mathbb{Z}$. Então $p(x)$ é irredutível sobre $\mathbb{Q}$.*

A demonstração dessa proposição pode ser encontrada em GONÇALVES (2015, p. 82).

Teorema 4.6.6. *(Critério de Eisenstein) Seja $p(x) = a_0+a_1x+\cdots+a_nx^n$ um polinômio em $\mathbb{Z}[x]$. Suponhamos que exista um inteiro primo p tal que:*

a) $p \nmid a_n$;

b) $p \mid a_0, a_1, \cdots, a_{n-1}$;

c) $p^2 \nmid a_0$.

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

Demonstração. Pelo Lema 4.6.5 é suficiente provar que $p(x)$ é irredutível sobre $\mathbb{Z}$. Suponhamos por contradição que,

$$p(x) = g(x) \cdot h(x); \text{ com } g(x), h(x) \in \mathbb{Z}[x]$$

e

$$1 \leq \partial\, g(x), \partial\, h(x) < \partial\, p(x) = n.$$

Sejam

$$g(x) = b_0 + b_1 x + \cdots + b_r x^r \in \mathbb{Z}[x], \partial\, g(x) = r$$

e

$$h(x) = c_0 + c_1 x + \cdots + c_s x^s \in \mathbb{Z}[x], \partial\, h(x) = s.$$

Assim, $n = r + s$.

Agora, $b_0 \cdot c_0 = a_0$ e, assim, $p \mid b_0$ ou $p \mid c_0$. Como $p^2 \nmid a_0$ segue que p divide apenas um dos inteiros b_0, c_0. Vamos admitir, sem perda de generalidade, que $p \mid b_0$ e $p \nmid c_0$.

Agora, $a_n = b_r \cdot c_s$ é o coeficiente de $x^n = x^{r+s}$ e portanto $p \nmid b_r$ e $p \mid b_0$. Seja b_i o primeiro coeficiente de $g(x)$ tal que $p \nmid b_i$.

Agora, $a_i = b_0 \cdot c_i + b_1 \cdot c_{i-1} + \cdots + b_i \cdot c_0$ e, portanto, como $p \mid b_0, \cdots, b_{i-1}$, mas $p \nmid b_i$ e $p \nmid c_0$. Logo $p \nmid a_i$, e portanto $i = n$, o que é um absurdo, pois $1 \leq i \leq r < n$. □

Definição 4.6.7. *Seja* K *um corpo. Dizemos que* $L \supset K$ *é uma extensão de* K *se* K *for um subcorpo de* L.

Definição 4.6.8. *Sejam* K *um corpo e* $L \supset K$. *Dizemos que* $\alpha \in L$ *é algébrico sobre* K *se existe* $p(x) \in K[x] - \{0_K\}$ *tal que* $p(\alpha) = 0_K$. *Caso contrário, dizemos que* α *é transcendente sobre* K.

Observação 4.6.9. *Se $\alpha \in K$, então α é algébrico sobre K, pois é raiz de $p(x) = x - \alpha$ com $p(x) \in K[x] - \{0_K\}$.*

Definição 4.6.10. *Uma extensão de corpos $L \supset K$ é dita algébrica se para todo $\alpha \in L$, α é algébrico sobre K.*

Desta forma, supondo $\alpha \in L$ algébrico sobre K e $p(x) \in K[x]$, mônico, de menor grau tal que $p(\alpha) = 0_K$, temos, pela minimalidade do grau de $p(x)$, que este é o único polinômio mônico irredutível em $K[x]$ tal que $p(\alpha) = 0_K$. Assim, denotaremos por $p(x) = irr(\alpha, K)$ tal polinômio.

Definição 4.6.11. *Se $\alpha \in L \supset K$, definimos $K[\alpha] = \big\{p(\alpha); p(x) \in K[x]\big\}$.*

Note que $K[\alpha]$ é um subdomínio de L que contém K. De fato, se $a \in K$ tomamos o polinômio de grau zero $p(x) = a$ e, assim, $a = p(\alpha) \in K[\alpha]$.

Teorema 4.6.12. *Se $\alpha \in L \supset K$ e $\Psi : K[x] \to L$ é definida por $\Psi\big(p(x)\big) = p(\alpha)$, então Ψ é um homomorfismo de anéis tal que:*

i) $Im(\Psi) = K[\alpha]$ e $K \subset K[\alpha] \subset L$;

ii) α é transcendente sobre $K \Leftrightarrow Ker(\Psi) = \{0_K\}$;

iii) se α é algébrico sobre K e $p(x) = irr(\alpha, K)$ então, $Ker(\Psi) = K[x] \cdot p(x)$ é um ideal maximal de $K[x]$;

iv) $K[x]/Ker(\Psi) \simeq K[\alpha]$.

Corolário 4.6.13. *Seja $\alpha \in L \supset K$.*

a) Se α é algébrico sobre K, então $K[\alpha]$ é um subcorpo de L que contém K.

b) Se α é transcendente sobre K, então $K[\alpha]$ é um subdomínio de L isomorfo ao domínio $K[x]$ dos polinômios em uma indeterminada x.

As demonstrações do Teorema 4.6.12 e do Corolário 4.6.13 serão omitidas e podem ser encontradas em Gonçalves (2015, p. 89).

Corolário 4.6.14. *Se $\alpha, \beta \in L \supset K$ são raízes de um mesmo polinômio irredutível sobre K então $K[\alpha]$ e $K[\beta]$ são corpos isomorfos.*

A demonstração desse corolário pode ser encontrada em GONÇALVES (2015, pg. 90).

Proposição 4.6.15. *Sejam $L \supset K$ e $\alpha \in L$ algébrico sobre K. Se o grau do polinômio $irr(\alpha, K)$ é n, então:*

a) dado $p(x) \in K[x]$, temos que $p(\alpha)$ pode ser expresso de modo único na forma $p(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$, onde $a_i \in K$;

b) $K[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}; a_i \in K\}$ é um subcorpo de L que contém K.

A demonstração desta proposição pode ser encontrada em GONÇALVES (2015, p. 90).

Definição 4.6.16. *Seja K um corpo. Se todo polinômio não constante de $K[x]$ tem pelo menos uma raiz em K, diz-se que K é um corpo algebricamente fechado.*

Consideraremos agora K um subcorpo de $\mathbb{C}$. Se $p(x) \in K[x]$ é um polinômio de grau $n \geq 1$ e $\alpha_1, \alpha_2, \cdots, \alpha_r$ são todas as raízes distintas de $p(x)$ em $\mathbb{C}$, temos que

$$p(x) = a_n \cdot (x - \alpha_1)^{m_1} \cdots (x - \alpha_r)^{m_r} \text{ em } \mathbb{C}[x],$$

onde $a_n \in K$ e $r, m_1, \cdots, m_r$ são inteiros positivos. Neste caso, dizemos que o inteiro m_i é a *multiplicidade da raiz* α_i e, em particular, se $m_i = 1$ dizemos que α_i é uma *raiz simples* de $p(x)$.

Para definirmos a derivada de $p(x)$, suponha que $p(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$. Representamos a *derivada de* $p(x)$ por $p'(x)$ onde, $p'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} \in K[x]$. Observe que se $\partial\, p(x) = n \geq 1$, então $p'(x) \neq 0$ e $\partial\, p'(x) = n - 1$.

Sejam $p(x), q(x) \in K[x]$ e $a \in K$. Seguem as seguintes propriedades:

i) $\big(p(x) + q(x)\big)' = p'(x) + q'(x)$;

ii) $\big(a \cdot p(x)\big)' = a \cdot p'(x)$;

iii) $\big(p(x) \cdot q(x)\big)' = p'(x) \cdot q(x) + p(x) \cdot q'(x)$.

Proposição 4.6.17. *Sejam $p(x) \in K[x]$, $\partial p(x) = n \geq 1$ e $\alpha \in \mathbb{C}$ uma raiz de $p(x)$. Então,*

a) α é raiz simples de $p(x)$ se, e somente se, $p(\alpha) = 0$ e $p'(\alpha) \neq 0$;

b) se $p(x)$ é irredutível sobre K, então todas as raízes de $p(x)$ são simples.

A demonstração dessa proposição pode ser encontrada em GONÇALVES (2015, p. 92).

Definição 4.6.18. *Chamamos de corpo de decomposição de um polinômio $p(x) \in K[x]$ sobre K o subcorpo de $\mathbb{C}$ que contém K e todas as raízes de $p(x)$ em $\mathbb{C}$, o qual será denotado por $L = Gal(p, K)$.*

Exemplo 4.6.19. *Sejam $\alpha = \sqrt[3]{2} \in \mathbb{R}$ e $\beta = \sqrt[3]{2} \cdot \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) \in \mathbb{C}$ uma raiz complexa de $x^3 - 2 \in \mathbb{Q}[x]$. Também temos que o conjugado de β dado por $\overline{\beta} = \sqrt[3]{2} \cdot \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) \in \mathbb{C}$ é solução de $x^3 - 2$. Assim, α, β e $\overline{\beta}$ são as 3 distintas raízes de $x^3 - 2 \in \mathbb{Q}[x]$ e nesse caso, $Gal(x^3 - 2, \mathbb{Q}) = \mathbb{Q}[\alpha, \beta]$.*

Pela fórmula de De Moivre, temos que $u = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$ é uma raiz n-ésima da unidade. De fato,

$$\begin{aligned} u^n &= \left(cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)\right)^n = cos\left(\frac{2\pi n}{n}\right) + isen\left(\frac{2\pi n}{n}\right) \\ &= cos(2\pi) + isen(2\pi) = 1 + i \cdot 0 = 1. \end{aligned}$$

Exemplo 4.6.20. *Vamos mostrar que se $\alpha = \sqrt[n]{2} \in \mathbb{R}$ e $u = cos\left(\frac{2\pi}{n}\right) + i \cdot sen\left(\frac{2\pi}{n}\right)$, então $Gal(x^n - 2, \mathbb{Q}) = \mathbb{Q}[\alpha, u] = \mathbb{Q}[\alpha, \beta]$, onde $\beta = \alpha \cdot u$ é uma raiz de $x^n - 2 \in \mathbb{C}[x]$.*

Por definição, temos que $Gal(x^n - 2, \mathbb{Q}) = \mathbb{Q}[\alpha, \alpha u, \alpha u^2, \cdots, \alpha u^{n-1}]$, onde $\alpha, \alpha u, \cdots, \alpha u^{n-1}$ são as raízes do polinômio $x^n - 2$.

Tomando $K = Gal(x^n - 2, \mathbb{Q})$, vamos mostrar que $u \in K; \forall\, i \leq i \leq n - 1$. Como $\alpha \in K$ temos que $\alpha^{-1} \in K$, pois K é corpo. Assim,

$$u^i = \alpha^{-1}(\alpha u^i) \in K, \forall\, 1 \leq i \leq n - 1.$$

Portanto, $K \supseteq \mathbb{Q}[\alpha, u, u^2, \cdots, u^{n-1}] \supseteq \mathbb{Q}[\alpha, u]$.

No entanto, $u \in \mathbb{Q}[\alpha, u]$ e, portanto, $u^i \in \mathbb{Q}[\alpha, u], \forall\, 1 \leq i \leq n - 1$. Logo, $\alpha u^i \in \mathbb{Q}[\alpha, u]$, para cada $1 \leq i \leq n - 1$.

4.6.2 Grau de uma Extensão Algébrica

Definição 4.6.21. *Seja K um corpo. Uma extensão de corpos $L \supset K$ diz-se finita se $[L : K] = n$, caso contrário $L \supset K$ diz-se uma extensão infinita.*

Proposição 4.6.22. *Sejam K um corpo e $L \supset K$ uma extensão de K. Então,*

a) se $L \supset K$ é finita, então $L \supset K$ é algébrica;

b) se $\alpha \in L \supset K$ é um elemento algébrico sobre K e $\partial\, irr(\alpha, K) = n$, então $\{1, \alpha, \cdots, \alpha^{n-1}\}$ é uma base do espaço vetorial $K[\alpha]$ sobre K e $[K[\alpha] : K] = n$;

c) se $\alpha \in L \supset K$ é um elemento transcendente sobre K então, $K[\alpha] \supset K$ é uma extensão infinita.

Demonstração. (a) Sejam $[L : K] = m$ e $\alpha \in L \supset K$. Sendo $K[\alpha]$ um subespaço de L, segue que $[K[\alpha] : K] \leq m$. Se $[K[\alpha] : K] = n \leq m$, então $\{1, \alpha, \cdots, \alpha^n\}$ é L.D., pois n é o número máximo de elementos L.I. e, portanto, existem escalares $a_0, a_1, \cdots, a_n \in K$ não todos nulos tais que

$$a_0 + a_i\alpha + \cdots + a_n\alpha^n = 0,$$

e isso nos diz que α é algébrico sobre K.

(b) Seja $\alpha \in L \supset K$ um elemento algébrico sobre K tal que $\partial\, irr(\alpha, K) = n$. Vimos na Proposição 4.6.15, item a), que todo elemento de $K[\alpha]$ pode ser escrito de forma única como combinação linear sobre K de $1, \alpha, \cdots, \alpha^{n-1}$. Assim, $\{1, \alpha, \cdots, \alpha^{n-1}\}$ é uma base de $K[\alpha]$ sobre K e isto nos diz que $[K[\alpha] : K] = n$.

(c) Seja $\alpha \in L \supset K$ um elemento transcendente sobre K. Temos que não existe $0 \neq p(x) \in K[x]$ tal que $p(\alpha) = 0$. Assim, $\{1, \alpha, \cdots, \alpha^n\}$ é L.I, para todo $n \in \mathbb{N}$. De fato, suponhamos que para algum $n \in \mathbb{N}\{1, \alpha, \cdots, \alpha^n\}$ é L.D. Daí, existem $a_i \in K$ tais que $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. Então $p(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ é tal que $p(\alpha) = 0$, um absurdo. Portanto, $K[\alpha]$ sobre K é uma extensão infinita. □

Corolário 4.6.23. *Seja $\alpha \in L \supset K$. Então, as seguintes afirmações são equivalentes:*

i) α é algébrico sobre K;

ii) $[K[\alpha] : K] = n$, *para algum* $n \in \mathbb{N}$;

iii) $K[\alpha]$ *é uma extensão algébrica de* K.

Demonstração. (i) $\Rightarrow$ (ii) Como α é algébrico sobre K, temos que existe $p(x) = irr(\alpha, K) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n$ com $\partial\, irr(\alpha, K) = n$. Portanto, pela Proposição 4.6.22 segue que $\big[K[\alpha] : K\big] = n$.

(ii) $\Rightarrow$ (iii) Por hipótese, temos que $K[\alpha] \supset K$ é finita. Logo, pela Proposição 4.6.22, $K[\alpha] \supset K$ é algébrica.

(iii) $\Rightarrow$ (i) Por hipótese temos que $K[\alpha] \supset K$ é algébrica e, como $\alpha \in K[x]$, pela definição de extensão algébrica, concluímos que α é algébrico sobre K. □

Proposição 4.6.24. *Sejam* $M \supset L \supset K$ *corpos tais que* $M \supset L$ *e* $L \supset K$ *são extensões finitas. Então,* $M \supset K$ *é uma extensão finita e* $[M : K] = [M : L] \cdot [L : K]$.

A demonstração dessa proposição pode ser encontrada em GONÇALVES (2015, p. 99).

Corolário 4.6.25.

a) $\bar{\mathbb{Q}}_{\mathbb{C}} = \{\alpha \in \mathbb{C}; \alpha$ *algébrico sobre* $\mathbb{Q}\}$ *é um subcorpo de* $\mathbb{C}$, *que é uma extensão algébrica infinita de* $\mathbb{Q}$.

b) $\bar{\mathbb{Q}}_{\mathbb{R}} = \{\alpha \in \mathbb{R}; \alpha$ *algébrico sobre* $\mathbb{Q}\}$ *é um subcorpo de* $\mathbb{R}$, *que é uma extensão algébrica infinita de* $\mathbb{Q}$.

A demonstração desse corolário pode ser encontrada em GONÇALVES (2015, p. 100).

Corolário 4.6.26. *Sejam* $K \supset \mathbb{Q}$ *tal que* $[K : \mathbb{Q}] = m$ *e* $p(x) \in \mathbb{Q}[x]$ *um polinômio irredutível sobre* $\mathbb{Q}$ *de grau* n. *Se* $m.d.c(m, n) = 1$, *então* $p(x)$ *é um polinômio irredutível sobre* K.

A demonstração desse corolário pode ser encontrada em GONÇALVES (2015, p. 101).

Corolário 4.6.27. *Seja* $L = Gal(x^p - 2, \mathbb{Q})$, *onde* p *é primo. Então,* $[L : \mathbb{Q}] = p \cdot (p - 1)$.

Demonstração. De fato, sabemos pelo Exemplo 4.6.20 que $L = Gal(x^p - 2, \mathbb{Q}) = \mathbb{Q}[\alpha, u]$, onde $\alpha = \sqrt[p]{2} \in \mathbb{R}$ e $u = cos\left(\frac{2\pi}{p}\right) + i \cdot sen\left(\frac{2\pi}{p}\right) \in \mathbb{C}$ é uma raiz p-ésima primitiva da unidade.

Agora, pela Proposição 4.6.24, $[L : \mathbb{Q}] = \big[L : \mathbb{Q}[\alpha]\big] \cdot \big[\mathbb{Q}[\alpha] : \mathbb{Q}\big]$ e pelo Teorema 4.6.6 temos que $p(x) = x^p - 2$ é irredutível sobre $\mathbb{Q}$, e pela Proposição 4.6.22, concluímos que $\big[\mathbb{Q}[\alpha] : \mathbb{Q}\big] = p$, pois $p(x) = irr(\alpha, \mathbb{Q})$. Note que, se $K = \mathbb{Q}[\alpha]$, obtemos $L = K[u] \supset K \supset \mathbb{Q}$.

Como u é raiz p-ésima primitiva da unidade, u é raiz de $x^{p-1} + x^{p-2} + \cdots_x + 1$ e este é irredutível pelo Teorema 4.6.6. Como $[K : \mathbb{Q}] = p$ e $m.d.c.\{p, p-1\} = 1$, temos, pelo Corolário 4.6.26 que $x^{p-1} + x^{p-2} + \cdots + x + 1$ é irredutível sobre K, tendo u como raiz. Portanto, $\big[K[u] : K\big] = p - 1$, onde $L = K[u]$ e $K = \mathbb{Q}[\alpha]$, como queríamos. □

Teorema 4.6.28. *Seja $L \supset K \supset \mathbb{Q}$ tal que $L \supset K$ é uma extensão finita. Então, existe $u \in L$ tal que $L = K[u]$.*

Corolário 4.6.29. *Seja $L \supset K \supset \mathbb{Q}$ tal que $L \supset K$ é uma extensão finita. Então, $[L : K] \geq |Aut_K\, L|$, onde $|Aut_K\, L|$ denota o número de elementos do conjunto*

$$Aut_K\, L = \{f \in Aut\, L; f(\lambda) = \lambda, \forall\, \lambda \in K\}.$$

As demonstrações do Teorema 4.6.28 e do Corolário 4.6.29 podem ser encontradas em Gonçalves (2015, p. 102).

5 TEORIA DE GALOIS ELEMENTAR

Nessa seção veremos alguns resultados para extensões $L \supset K$ finitas, tais que $\mathbb{C} \supset L \supset K \supset \mathbb{Q}$, ou seja, todas as extensões $L \supset K$ serão de subcorpos de $\mathbb{C}$ contendo $\mathbb{Q}$.

5.1 EXTENSÕES GALOISIANAS E EXTENSÕES NORMAIS

Definição 5.1.1. *Seja $L \supset K$ uma extensão finita. Dizemos que $L \supset K$ é uma extensão galoisiana se existe $p(x) \in K[x]$ tal que $L = Gal(p, K)$.*

Definição 5.1.2. *Seja $L \supset K$ uma extensão algébrica. Dizemos que $L \supset K$ é normal se para todo $q(x) \in K[x]$, irredutível sobre K, que possui uma raiz $\alpha \in L$, possui todas as raízes complexas em L.*

Observe que se $L \supset M \supset K$ são extensões tais que $L \supset K$ é galoisiana, então $L \supset M$ é também galoisiana. No entanto, $M \supset K$ não é, necessariamente, galoisiana. De fato, considere $L = Gal(x^3 - 2, \mathbb{Q})$, $M = \mathbb{Q}\left[\sqrt[3]{2}\right]$ e $K = \mathbb{Q}$, temos, pelo Exemplo 4.6.19, que $L \supset M \supset K$ e ainda $L \supset K$ é galoisiana, pois $p(x) = x^3 - 2 \in K[x] = \mathbb{Q}[x]$, então $L \supset M$ também é galoisiana. Porém, $M \supset K$ não é galoisiana, pois se fosse galoisiana, teríamos $M = Gal(p(x), \mathbb{Q})$ para algum $p(x) \in \mathbb{Q}[x]$ tal que $p\left(\sqrt[3]{2}\right) = 0$. Neste caso, temos que $(x^3 - 2)/p(x)$, ou seja, $p(x) = (x^3 - 2)g(x)$, para algum $g(x) \in \mathbb{Q}[x]$. Daí, note que β (como no Exemplo 4.6.19) é raiz de $p(x)$, e portanto $\beta \in M$, pois $M = Gal(p(x), \mathbb{Q})$. Mas isto é um absurdo, pois $\beta \notin M$, uma vez que $M = \mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{R}$ e $\beta \notin \mathbb{R}$.

No que segue, mostraremos que uma extensão finita $L \supset K$ é galoisiana se, e somente se, $L \supset K$ é normal. Porém, precisaremos de algumas definições e de alguns resultados sobre extensões de isomorfismos.

Sejam K, K' corpos e

$$\begin{aligned} \sigma : K &\to K' \\ a &\mapsto \sigma(a) = a' \end{aligned}$$

um isomorfismo de corpos de K sobre K'. Se $p(x) = a_0 + a_1x + \cdots + a_nx^n$ é um polinômio em $K[x]$, definimos $p^\sigma(x) = a'_0 + a'_1x + \cdots + a'_nx^n \in K'[x]$, onde $a'_i = \sigma(a_i)$ para $i = 0, 1, \cdots, n$.

Note que se $p(x) = p_1(x)p_2(x)\cdots p_k(x)$, onde $p_j(x) \in K[x]$, para $j = 1, \cdots, k$, são irredutíveis sobre K, então $p^\sigma(x) = p_1^\sigma(x) \cdot p_2^\sigma(x)\cdots p_k^\sigma(x)$, onde $p_j^\sigma(x) \in K'[x]$, com $j = 1, \cdots, k$, são irredutíveis sobre K'.

Em particular, se todas as raízes de $p(x)$ estão em K, temos que cada $p_j(x)$ possui grau 1 e, portanto, cada $p_j^\sigma(x)$ também possui grau 1. Daí, segue que todas a raízes de $p^\sigma(x)$ estão em K'.

Proposição 5.1.3. *Sejam $K, K' \supset \mathbb{Q}$ corpos, $\sigma : K \to K'$ um isomorfismo e $h(x) \in K[x]$ um polinômio irredutível sobre K. Se $\alpha \in \mathbb{C}$ é uma raiz de $h(x)$ e $\beta \in \mathbb{C}$ é uma raiz de $h^\sigma(x)$ então, existe um único isomorfismo de corpos $\hat{\sigma} : K[\alpha] \to K'[\beta]$ tal que $\hat{\sigma}(\alpha) = \beta$ e $\hat{\sigma}\Big|_K = \sigma$.*

Demonstração. Seja α uma raiz de $h(x) \in K[x]$ e β uma raiz de $h^\sigma(x) \in K'[x]$. Como α e β são raízes de polinômios em $K[x]$ e $K'[x]$, respectivamente, temos que são algébricos sobre K e K', respectivamente. Daí, pelo Corolário 4.6.13 temos que $K[\alpha]$ e$K'[\beta]$ são corpos e ainda, se $\partial\, h(x) = \partial\, h^\sigma(x) = r$ segue, da Proposição 4.6.22, que

i) $K[\alpha] = \{p(\alpha); p(x) \in K[x]\} = \{a_0 + a_1\alpha + \cdots + a_{r-1}\alpha^{r-1}; a_i \in K\}$ e $\{1, \alpha, \alpha^2, \cdots, \alpha^{r-1}\}$ é uma base do espaço vetorial $K[\alpha]$ sobre o corpo K.

ii) $K'[\beta] = \{p(\beta); p(x) \in K'[x]\} = \{a'_0 + a'_1\beta + \cdots + a'_{r-1}\beta^{r-1}; a_i \in K\}$ e $\{1, \beta, \beta^2, \cdots, \beta^{r-1}\}$ é uma base do espaço vetorial $K'[\beta]$ sobre o corpo K'.

Definindo a aplicação,

$$\begin{aligned} \hat{\sigma} : K[\alpha] &\to K'[\beta] \\ \sum_{i=1}^{r-1} a_i\alpha^i &\mapsto \sum_{i=1}^{r-1} \sigma(a_i)\beta^i \end{aligned}$$

temos que

$$\hat{\sigma}\big(p(x)\big) = \hat{\sigma}\left(a_0 + a_1\alpha + \cdots + a_{r-1}\alpha^{r-1}\right) = \sigma\left(a_0\right) + \sigma\left(a_1\right)\beta + \cdots + \sigma\left(a_{r-1}\right)\beta^{r-1}$$

é um isomorfismo do corpo $K[\alpha]$ sobre o corpo $K'[\beta]$ tal que $\hat{\sigma}(\alpha) = \beta$ e $\hat{\sigma}\Big|_K = \sigma$, e ainda, $\hat{\sigma}$ é o único com essas duas condições. □

Corolário 5.1.4. *Sejam K, K' corpos, $\sigma : K \to K'$ um isomorfismo de corpos, $p(x) \in K[x]$ e $\alpha \in \mathbb{C}$ uma raiz de $p(x)$. Então, existe $\beta \in \mathbb{C}$ raiz de $p^\sigma(x) \in K'[x]$ e existe um*

isomorfismo

$$\sigma_1 : K[\alpha] \to K'[\beta]$$

tal que

$$\sigma_1(\alpha) = \beta \text{ e } \sigma_1\Big|_K = \sigma.$$

Demonstração. Seja $p(x) = p_1(x)^{m_1}p_2(x)^{m_2}\cdots p_k(x)^{m_k}$, onde $p_1(x), \cdots, p_k(x)$ são os distintos fatores irredutíveis de $p(x)$ em $K[x]$. Desta forma, temos que $p^\sigma(x) = p_1^\sigma(x)^{m_1}p_2^\sigma(x)^{m_2}\cdots p_k^\sigma(x)^{m_k}$, onde $p_1^\sigma(x), \cdots, p_k^\sigma(x)$ são os distintos fatores irredutíveis de $p^\sigma(x)$ em $K'[x]$.

Como α é raiz de $p(x)$, podemos assumir que α é raiz de $p_1(x)$. Logo, para β qualquer raiz do polinômio $p_1^\sigma(x)$, segue pela Proposição 5.1.3 que existe um isomorfismo de corpos $\sigma_1 : K[\alpha] \to K'[\beta]$ tal que $\sigma_1(\alpha) = \beta$ e $\sigma_1\Big|_K = \sigma$. □

Teorema 5.1.5. *Sejam K, K' corpos, $\sigma : K \to K'$ um isomorfismo de corpos, $p(x) \in K[x]$ e $\alpha_1, \cdots, \alpha_r$ as distintas raízes de $p(x)$ em $\mathbb{C}$. Se $L = Gal(p, K)$ e $L' = Gal(p^\sigma, K')$, então existe um isomorfismo $\hat{\sigma} : L \to L'$ tal que $\hat{\sigma}\Big|_K = \sigma$ e mais ainda, $\hat{\sigma}(\alpha_1), \cdots, \hat{\sigma}(\alpha_r)$ são as distintas raízes de $p^\sigma(x)$ em $\mathbb{C}$.*

Demonstração. Suponhamos que $p(x) \in K[x]$ possua uma única raiz α_1, então temos $p(x) = (x - \alpha_1)^m$ em $\mathbb{C}[x]$, porém, isto implica que $\alpha_1 \in K$ e, portanto, $\sigma(\alpha_1) \in K'$ é a única raiz de $p^\sigma(x)$ em $\mathbb{C}$ e neste caso $L = K$, $L' = K'$ e existe um isomorfismo de corpos satisfazendo $\hat{\sigma} = \sigma : L \to L'$ e $\hat{\sigma}\Big|_L = \sigma$.

Agora, se $p(x) = p_1(x)^{m_1}\cdots p_k(x)^{m_k}$, onde $p_i(x) \in K[x]$ são distintos polinômios irredutíveis sobre K, temos que $p^\sigma(x) = p_1^\sigma(x)^{m_1}\cdots p_k^\sigma(x)^{m_k}$, onde $p_i^\sigma(x) \in K'[x]$ são distintos polinômios irredutíveis sobre K'.

Sabemos, pela Proposição 4.6.17 que o número r de raízes distintas de $p(x)$ em $\mathbb{C}$ é dado por $r = \partial\, p_1(x) + \partial\, p_2(x) + \cdots + \partial\, p_k(x)$ e, portanto, temos como consequência que o número de raízes distintas de $p^\sigma(x)$ em $\mathbb{C}$ é também igual a r. Tome $\beta_1, \beta_2, \cdots, \beta_r$ como sendo as r distintas raízes em $\mathbb{C}$ do polinômio $p^\sigma(x) \in K'[x]$.

Seja $K_1 = K[\alpha_1], K_2 = K_1[\alpha_2], \cdots, K_r = K_{r-1}[\alpha_r]$.

Pela Proposição 5.1.4, temos que existe $\beta \in \{\beta_1, \cdots, \beta_r\}$ e existe isomorfismo de corpos $\sigma_1 : K[\alpha_1] \to K'[\beta]$ tal que $\sigma_1(\alpha_1) = \beta$ e $\sigma_1\Big|_K = \sigma$. Renomeando $\beta_1 = \sigma_1(\alpha_1) = \beta$, temos que existe $\beta \in \{\beta_1, \cdots, \beta_r\}$ e o isomorfismo $\sigma_1 : K[\alpha_1] \to K'[\beta_1]$ tal que

$$\sigma_1(\alpha_1) = \beta_1 \text{ e } \sigma_1\Big|_K = \sigma.$$

Seja $K'[\beta_1] = K_1'$. Assim, temos $\sigma_1 : K_1 \to K_1'$ isomorfismo de corpos tal que $\sigma_1(\alpha_1) = \beta_1$ e $\sigma_1\Big|_K = \sigma$.

Agora, como $p(x) \in K[x]$ e $\sigma_1\Big|_K = \sigma$ segue que $p(x) \in K_1[x]$ e $p^{\sigma_1}(x) = p^{\sigma}(x)$.

Aplicando novamente a Proposição 5.1.4, para os corpos K_1, K_1' e $\sigma_1 : K_1 \to K_1'$, concluímos que existe $\beta \in \{\beta_2, \beta_3, \cdots, \beta_k\}$, o qual renomearemos de β_2, e existe o isomorfismo de corpos $\sigma_2 : K_1[\alpha_2] \to K_1'[\beta_2]$ tal que $\sigma_2(\alpha_2) = \beta_2$ e $\sigma_2\Big|_{K_1} = \sigma_1$.

Note que σ_2 isomorfismo e $\alpha_1 \neq \alpha_2$ implica que $\beta_1 = \sigma_2(\alpha_1) \neq \sigma_2(\alpha_2) = \beta_2$.

Como $\sigma_1\Big|_K = \sigma$, segue que $\sigma_2\Big|_K = \sigma_1\Big|_K = \sigma$, ou seja,

$$\sigma_2\Big|_K = \sigma \text{ e } \sigma_2(\alpha_1) = \beta_1, \sigma_2(\alpha_2) = \beta_2$$

e $\sigma_2 : K[\alpha_1, \alpha_2] \to K'[\beta_1, \beta_2]$ é um isomorfismo. Procedendo indutivamente desta forma, concluímos que existe $\sigma_{k-1} : K[\alpha_1, \cdots, \alpha_{k-1}] \to K'[\beta_1, \cdots, \beta_{k-1}]$ isomorfismo tal que $\sigma_{k-1}(\alpha_i) = \beta_i, i = 1, 2, \cdots, k-1$ e $\sigma_{k-1}\Big|_K = \sigma$. Além disso, temos que $p(x) \in K_{k-1}[x]$ e $p^{\sigma_{k-1}}(x) = p^{\sigma}(x)$, onde $K_{k-1} = K[\alpha_1, \cdots, \alpha_{k-1}]$.

Aplicando novamente a Proposição 5.1.4 para os corpos $K_{k-1} = K[\alpha_1, \cdots, \alpha_{k-1}]$ e $K_{k-1}' = K'[\beta_1, \cdots, \beta_{k-1}]$ com $\sigma_{k-1} : K_{k-1} \to K_{k-1}'$ temos que existe β o qual renomearemos por β_k, raiz de $p^{\sigma}(x)$ e existe o isomorfismo $\sigma_k : K_{k-1}[\alpha_k] \to K_{k-1}'[\beta_k]$ tal que $\sigma_k\Big|_{K_{k-1}} = \sigma_{k-1}$ e $\sigma_k(\alpha_k) = \beta_k$.

Desta forma temos que existe o isomorfismo $\sigma_k : K[\alpha_1, \cdots, \alpha_k] \to K'[\beta_1, \cdots, \beta_k]$ tal que $\sigma_i(\alpha_i) = \beta_i$ para todo $i \in \{1, 2, \cdots, k\}$ e $\sigma_k\Big|_K = \sigma$. Como $L = K_r = K[\alpha_1, \cdots, \alpha_r]$, temos o que se pede. □

Corolário 5.1.6. *Seja $L \supset K$ uma extensão galoisiana e sejam M, M' subcorpos de L contendo K. Se $\sigma : M \to M'$ é um isomorfismo de corpos tal que $\sigma(a) = a$, para cada $a \in K$, então existe $\hat{\sigma} \in Aut_K L$ tal que $\hat{\sigma}\Big|_M = \sigma$.*

Demonstração. Seja $L = Gal(p, K)$, para algum $p(x) \in K[x]$. Então a demonstração é consequência do Teorema 5.1.5 pois $p^\sigma(x) = p(x)$ e considerando $L = Gal(p, M) = L' = Gal(p^\sigma, M')$. □

Corolário 5.1.7. *Seja $L \supset K$ uma extensão finita. Então, $L \supset K$ é galoisiana se, e somente se, $L \supset K$ é normal.*

Demonstração. ($\Leftarrow$) Suponhamos $L \supset K$ normal. Como $L \supset K$ é uma extensão finita, segue do Teorema 4.6.28 que $L = K[u]$, para algum $u \in L$. Agora, como $L \supset K$ é normal, temos que $L = Gal(h, K)$ onde $h(x) = irr(u, K)$.

($\Rightarrow$) Suponhamos agora $L \supset K$ galoisiana com $L = Gal(p, K)$, para algum $p(x) \in K[x]$. Seja $q(x) \in K[x]$ um polinômio irredutível tal que exista $\alpha \in L$, com $q(\alpha) = 0$. Vamos provar que para todo $\beta \in \mathbb{C}$, $q(\beta) = 0$, tem-se $\beta \in L$.

De fato, seja $\beta \neq \alpha$ uma raiz de $q(x)$ em $\mathbb{C}$. Pela Proposição 5.1.3 que existe $\sigma : K[\alpha] \to K[\beta]$ isomorfismo tal que $\sigma(\alpha) = \beta$ e $\sigma(a) = a$, para cada $a \in K$.

Sejam $M = K[\alpha], M' = K[\beta]$ e $L' = Gal(p, M')$. Note que, como $K \subset M \subset L$ e $K \subset M'$ temos que

$$L = Gal(p, K) = Gal(p, M)$$

e também

$$L = Gal(p, K) \subset L' = Gal(p, M'). \tag{5.1.1}$$

Agora como $\sigma(a) = a$, para cada $a \in K$, temos que $p^\sigma(x) = p(x)$ e, pelo Teorema 5.1.5, existe um isomorfismo de corpos

$$\hat{\sigma} : L = Gal(p, M) \to L' = Gal(p^\sigma, M')$$

tal que $\hat{\sigma}\Big|_M = \sigma$, ou seja, $\hat{\sigma}(a) = a$, para cada $a \in K$ e $\hat{\sigma}(\alpha) = \beta$.

Em particular, temos

$$[L : K] = [L' : K]. \tag{5.1.2}$$

Assim, de (5.1.1) e (5.1.2) obtemos que $L = L'$, e como $\beta \in L'$ temos o que se pede. □

Corolário 5.1.8. *Se $L \supset K$ galoisiana, então:*

a) $[L : K] = |Aut_K L|$;

b) Se $\alpha \in L - K$, *existe* $\sigma \in Aut_K L$ *tal que* $\sigma(\alpha) \neq \alpha$.

Demonstração. (a) Seja $L = K[u]$. Se $h(x) = irr(u, K)$, então pelo Corolário 5.1.7 temos $L = Gal\big(h(x), K\big)$ e L contém todas as raízes de $h(x)$.

Pela Proposição 4.6.15, se grau $h(x) = n$ temos $[L : K] = n$ e pela Proposição 4.6.17 temos que $h(x)$ possui exatamente n raízes distintas $u_1 = u, u_2, \cdots, u_n$.

Agora, para cada $i \in \{1, 2, \cdots, n\}$ existe um isomorfismo $\sigma_i : K[u] \to K[u_i]$ tal que $\sigma_i(a) = a$, para cada $a \in K$. Pelo Corolário 5.1.6, segue que existe $\hat{\sigma_i} \in Aut_K L$ tal que $\hat{\sigma_i}\Big|_{K[u]} = \sigma_i$, ou seja, existem pelo menos n automorfismos $\hat{\sigma_1}, \hat{\sigma_2}, \cdots, \hat{\sigma_n} \in Aut_K L$. Como, pelo Corolário 4.6.29, $|Aut_K L| \leq [L : K] = n$ segue a igualdade desejada.

(b) Seja $\alpha \in L, \alpha \notin K$. Se $g(x) = irr(\alpha, K)$ segue que $\partial\, g(x) = r \geq 2$ e pela Proposição 4.6.17, existe $\beta \neq \alpha$ tal que $g(\beta) = 0$. Pelo Corolário 5.1.7 temos que $\beta \in L$, pois L é normal.

Agora, pela Proposição 5.1.3 existe $\sigma : K[\alpha] \to K[\beta]$ isomorfismo de corpos tal que $\sigma(a) = a$, para cada $a \in K$ e $\sigma(\alpha) = \beta \neq \alpha$.

Novamente, pelo Corolário 5.1.6, temos que existe $\hat{\sigma} \in Aut_K L$ e $\hat{\sigma}\Big|_{K[\alpha]} = \sigma$. □

Teorema 5.1.9. *Se $L \supset M \supset K$ são extensões finitas e $L \supset K$ é galoisiana, então as seguintes afirmações são equivalentes:*

a) $M \supset K$ *galoisiana;*

b) $\sigma(M) \subseteq M, \forall\, \sigma \in Aut_K L$;

c) $Aut_M L \triangleleft Aut_K L$.

Demonstração. (a) ⇒ (b) Seja $u \in L$ tal que $M = K[u]$. Se $M \supset K$ é galoisiana, segue pelo Corolário 5.1.7 que $M \supset K$ é uma extensão normal.

Agora, se $h(x) = irr(u, K)$ e $\sigma \in Aut_K L$, sabemos que $v = \sigma(u)$ é também raiz de $h(x)$ e pela normalidade de $M \supset K$ temos $v = \sigma(u) \in M$, ou seja, $\sigma\big(K[u]\big) \subseteq K[u]$.

(b) $\Rightarrow$ (a) Seja $u \in L$ tal que $M = K[u]$ e seja $h(x) = irr(u, K)$. Vamos provar que se $\sigma(M) \subseteq M$, para cada $\sigma \in Aut_K L$, então temos $M = Gal(h, K)$.

Sejam v raiz de $h(x)$ e $M' = K[v]$. Pela Proposição 5.1.3 existe um isomorfismo de corpos, $\sigma_0 : M \to M'$ tal que

$$\sigma_0(u) = v \text{ e } \sigma_0(a) = a, \forall\, a \in K.$$

Pelo Teorema 5.1.5 existe $\sigma \in Aut_K L$ tal que $\sigma\Big|_M = \sigma_0$ onde $L = Gal(h, K)$. Como $\sigma(M) \subseteq M$ e $u \in M$, teremos $v = \sigma_0(u) \in M$.

(b) $\Rightarrow$ (c) Sejam $\sigma \in Aut_K L$ e $\gamma \in Aut_M L$. Vamos provar que se $\sigma(M) \subseteq M$, então $\sigma^{-1} \circ \gamma \circ \sigma \in Aut_M L$. De fato, se $\sigma(M) \subseteq M$ e $m' = \sigma(m), m \in M$, temos $\gamma(m') = m'$ e $\big(\sigma^{-1} \circ \gamma \circ \sigma\big)(m) = \sigma^{-1}\big(\gamma(m')\big) = \sigma^{-1}(m') = m$.

(c) $\Rightarrow$ (b) Suponhamos por absurdo que existam $\sigma \in Aut_K L$ e $u \in M$ tal que $\sigma(u) = v \notin M$. Como $L \supset K$ é galoisiana temos que $L \supset M$ é galoisiana e pelo Corolário 5.1.8, segue que, existe $\gamma \in Aut_M L$ tal que $\gamma(v) \neq v$.

Assim, $\big(\sigma^{-1}\circ\gamma\circ\sigma\big)(u) = \sigma^{-1}\big(\gamma(v)\big) \neq \sigma^{-1}(v) = u$, ou seja, $\sigma^{-1}\circ\gamma\circ\sigma \notin Aut_M L$ contrariando a hipótese $Aut_M L \triangleleft Aut_K L$. □

Teorema 5.1.10. *Seja $L \supset K$ uma extensão finita. Então, as seguintes condições são equivalentes:*

a) $L \supset K$ galoisiana;

b) $L \supset K$ normal;

c) Para cada $\alpha \in L - K$, existe $\sigma \in Aut_K L$ tal que $\sigma(\alpha) \neq \alpha$;

d) $[L : K] = |Aut_K L|$.

Demonstração. (a) $\Rightarrow$ (b) Sejam $L \supset K$ uma extensão finita e $L \supset K$ galoisiana. Pelo Corolário 5.1.7, temos que $L \supset K$ é normal;

(b) $\Rightarrow$ (c) Seja $L \supset K$ uma extensão finita e normal, pelo Corolário 5.1.7, temos que $L \supset K$ é galoisiana. Assim, pelo Corolário 5.1.8 temos o que se pede;

(c) $\Rightarrow$ (d) Sabemos do Corolário 4.6.29 que $[L : K] \geq |Aut_K L|$. Suponhamos (c) e, por absurdo, $[L : K] > |Aut_K L|$.

Seja $Aut_K L = \{\varphi_1 = id_L, \varphi_2, \varphi_3, \cdots, \varphi_n\}$ onde id_L representa o automorfismo identidade de L. Se $[L : K] > n$, então, existem $u_1, u_2, \cdots, u_n, u_{n+1} \in L$ linearmente independentes sobre o corpo K. Consideremos agora o seguinte sistema linear homogêneo com n equações e $(n + 1)$ incógnitas $a_1, a_2, \cdots, a_{n+1}$ em L:

$$(*) \begin{cases} \varphi_1(u_1)a_1 + \varphi_1(u_2)a_2 + \cdots + \varphi_1(u_j)a_j + \cdots + \varphi_1(u_n)a_n + \varphi_1(u_{n+1})a_{n+1} = 0 \\ \varphi_2(u_1)a_1 + \varphi_2(u_2)a_2 + \cdots + \varphi_2(u_j)a_j + \cdots + \varphi_2(u_n)a_n + \varphi_2(u_{n+1})a_{n+1} = 0 \\ \vdots \quad \vdots \\ \varphi_i(u_1)a_1 + \varphi_i(u_2)a_2 + \cdots + \varphi_i(u_j)a_j + \cdots + \varphi_i(u_n)a_n + \varphi_i(u_{n+1})a_{n+1} = 0 \\ \vdots \quad \vdots \\ \varphi_n(u_1)a_1 + \varphi_n(u_2)a_2 + \cdots + \varphi_n(u_j)a_j + \cdots + \varphi_n(u_n)a_n + \varphi_n(u_{n+1})a_{n+1} = 0 \end{cases}$$

Como o número de equações de $(*)$ é menor do que o número de incógnitas, então $(*)$ admite uma solução com $a_1, a_2, \cdots, a_{n+1}$ não todos nulos, ou seja, uma solução não-trivial.

Consideremos agora uma solução não trivial de $(*)$ com o maior número de zeros possível e renomearemos os $a_i's$ não nulos dessa solução por $a_1, a_2, \cdots, a_r$.

Multiplicando por a_1^{-1} se necessário, podemos assumir que $a_1 = 1$. Assim, $1, a_2, a_3, ..., a_r$ não nulos são tais que $(1, a_2, a_3, \cdots, a_r, 0, \cdots, 0)$ é uma solução de $(*)$ com um número máximo de valores zeros. Então, temos,

$$\forall\, i \in \{1, 2, \cdots, n\}, \varphi_i(u_1)a_1 + \varphi_i(u_2)a_2 + \cdots + \varphi_i(u_r)a_r = 0.$$

Como $\varphi_1 = id_L$ e $u_1, \cdots, u_r, \cdots, u_{n+1}$ são linearmente independentes sobre K então segue que existe $a_i \in L$ tal que $a_i \notin K$. Note que $a_i \leq 1 = a_1$. Podemos, sem perda de generalidade, supor que $i = r$, ou seja, $a_r \in L \backslash K$. Assim, por (c), existe $\sigma \in Aut_K L$ tal que

$$\sigma(a_r) \neq a_r.$$

Daí, segue que, para cada $i \in \{1, 2, \cdots, n\}$,

$$(\sigma \circ \varphi_i)(u_1) + (\sigma \circ \varphi_i)(u_2)\sigma(a_2) + \cdots + (\sigma \circ \varphi_i)(u_r)\sigma(a_r) = 0.$$

Como $Aut_K L$ é um grupo e $\sigma \in Aut_K L$ temos que

$$Aut_K L = \{\varphi_1, \varphi_2, \cdots, \varphi_n\} = \{\sigma \circ \varphi_1, \sigma \circ \varphi_2, \cdots, \sigma \circ \varphi_n\}.$$

Portanto, $\sigma\ circ\varphi_i$, para cada $k \in \{1, 2, \cdot, n\}$,

$$\varphi_k(u_1) + \varphi_k(u_2)\sigma(a_2) + \cdots + \varphi_k(u_r)\sigma(a_r) = 0$$

e já tínhamos que para cada $i \in \{1, 2, \cdots, n\}$, que

$$\varphi_i(u_1) + \varphi_i(u_2)a_2 + \cdots + \varphi_i(u_r)a_r = 0.$$

Desta forma, segue que para cada $j \in \{1, 2, \cdots, n\}$,

$$\varphi_j(u_2)\big(\sigma(a_2) - a_2\big) + \cdots + \varphi_j(u_r)\big(\sigma(a_r) - a_r\big) = 0.$$

Como $\sigma(a_r) - a_r \neq 0$ temos uma contradição pela nossa escolha dos $a_i's$ com número máximo de zeros.

(d) $\Rightarrow$ (a) Suponhamos que $L \supset K$ seja uma extensão finita e $[L : K] = |Aut_K L|$. Vamos provar que $L \supset K$ é galoisiana.

Seja $L = K[u]$. Sabemos que se $h(x)$ é definido por $h(x) = irr(u, K)$, então para cada $\sigma \in Aut_K L$ tem-se $\sigma(u) \in L$ e $\sigma(u)$ raiz de $h(x)$. Assim, $|Aut_K L|$ é menor ou igual ao número de raízes de $h(x)$ em L. Agora, se $[L : K] = |Aut_K L|$, então, $|Aut_K L| = \partial\, h(x)$ e, portanto, igual ao número de raízes de $h(x)$ em L.

Assim, segue que L contém todas as raízes de $h(x)$, ou seja, $L = Gal(h, K)$.

□

Antes de encerrar esse parágrafo vamos ver alguns resultados úteis na determinação da estrutura do grupo $G = Aut_K L$.

Proposição 5.1.11. *Se $L \supset K$ é uma extensão galoisiana de grau n, então $G = Aut_K L$ é isomorfo a algum subgrupo de S_n.*

Demonstração. Sejam $L = K[u]$, $h = irr(u, K)$, $[L : K] = \partial\, h(x) = n$ e $\Omega = \{u_1 = u, u_2, \cdots, u_n\}$ o conjunto de todas as raízes complexas de $h(x)$. Como $L \supset K$ é galoisiana, temos $\Omega \subset L$. Sabemos também que para cada $\sigma \in G = Aut_K L$ e para

cada $u_i \in \Omega$ tem-se $\sigma(u_i) \in \Omega$, e como Ω é um conjunto finito e σ injetiva, segue que $\sigma_0 = \sigma\Big|_\Omega : \Omega \to \Omega$ define uma permutação do conjunto Ω.

Seja $\mathscr{P}(\Omega)$ o grupo das permutações do conjunto Ω. Então, é suficiente provarmos que G é isomorfo a um subgrupo de $\mathscr{P}(\Omega)$ pois, $\mathscr{P}(\Omega) \simeq S_n$.

Agora, verificamos que a função ψ definida a seguir define um homomorfismo de grupos, pois $(\sigma \circ \tau)\Big|_\Omega = \left(\sigma\Big|_\Omega\right) \circ \left(\tau\Big|_\Omega\right)$,

$$\begin{aligned} \psi : G &\to \mathscr{P}(\Omega). \\ \sigma &\mapsto \sigma_0 = \sigma\Big|_\Omega \end{aligned}$$

Mais ainda, se $\psi(\sigma) = \sigma\Big|_\Omega = id_\Omega$ (identidade em Ω) segue que $\sigma(u) = u$, e isto nos diz que $\sigma = id_L$, pois para cada $b \in L, b = a_0 + a_1u + \cdots + a_{n-1}u^{n-1}$, onde $a_i \in K$ e, para cada $\sigma \in G = Aut_K L$ tem-se, $\sigma(b) = a_0 + a_1\sigma(u) + \cdots + a_{n-1}\sigma(u)^{n-1} = a_0 + \cdots + a_{n-1}u^{n-1} = b$.

Portanto, ψ é injetiva e, assim, pelo Teorema 4.5.12 temos, $G \simeq \psi(G) \leq \mathscr{P}(\Omega)$. □

Exemplo 5.1.12. *Se $L = Gal(x^3 - 2, \mathbb{Q})$ então $Aut_\mathbb{Q} L \simeq S_3$.*

De fato, pelo Corolário 4.6.27, sabemos que $[L : \mathbb{Q}] = 6$, onde $L = Gal(x^3 - 2, \mathbb{Q})$ e, portanto $|Aut_K L| = 6$ e, como $|S_3| = 6$, o resultado segue da Proposição 5.1.11.

Proposição 5.1.13. *Se $L = Gal(x^n - 2, K)$ onde K contém uma raiz n-ésima primitiva da unidade ζ, então $G = Aut_K L$ é um grupo abeliano.*

Demonstração. Seja $\alpha = \sqrt[n]{2} \in \mathbb{R}$ e $\zeta = \cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right) \in \mathbb{C}$ então $\alpha, \alpha\zeta, \alpha\zeta^2, \cdots, \alpha\zeta^{n-1}$ são as n distintas raízes de $x^n - 2$ em $\mathbb{C}$.

Sabemos que $L = K[\alpha, \alpha\zeta, \alpha\zeta^2, \cdots, \alpha\zeta^{n-1}] = K[\alpha, \zeta] = K[\zeta, \alpha] = K[\alpha]$, pois $\zeta \in K$. Assim, se $\sigma, \tau \in Aut_K L$, eles são determinados completamente pelos valores $\sigma(\alpha)$ e $\tau(\alpha)$. Ainda, $\sigma, \tau \in Aut_K L$ implica que $\sigma(\alpha) = \alpha\zeta^i$ para algum $i \in \{0, 1, 2 \cdots, n-1\}$ e $\tau(\alpha) = \alpha\zeta^j$ para algum $j \in \{0, 1, 2 \cdots, n-1\}$. Daí segue, considerando $\zeta \in K$, que

$$(\sigma \circ \tau)(\alpha) = \sigma(\alpha\zeta^j) = \sigma(\alpha)\zeta^j = \alpha\zeta^{i+j}$$

e

$$(\tau \circ \sigma)(\alpha) = \tau(\alpha\zeta^i) = \tau(\alpha)\zeta^i = \alpha\zeta^{j+i}.$$

Desta forma, $\sigma \circ \tau(\alpha) = \tau \circ \sigma(\alpha)$, para cada $\sigma, \tau \in G = Aut_K L$. □

Teorema 5.1.14. *Seja p um divisor da ordem de um grupo finito G, p primo. Então existe $a \in G$ tal que a ordem de a é igual a p.*

A demonstração desse teorema pode ser encontrada em GONÇALVES (2015, p. 150).

Proposição 5.1.15. *Sejam p um número primo e $f(x) \in \mathbb{Q}[x]$ um polinômio irredutível sobre $\mathbb{Q}$ de grau p. Se $f(x)$ possui exatamente duas raízes não reais, então $Aut_{\mathbb{Q}} L \simeq S_p$ onde $L = Gal(f, \mathbb{Q})$.*

Demonstração. Seja $L = Gal(f, \mathbb{Q})$. Como $\partial f(x) = p$ e $f(x)$ irredutível sobre $\mathbb{Q}$, $f(x)$ possui exatamente p raízes distintas e pela Proposição 5.1.11, $G = Aut_{\mathbb{Q}} L$ é isomorfo a um subgrupo H de S_p, pois $[L : \mathbb{Q}] = p$.

Se α é uma raiz de $f(x)$ então, $\mathbb{Q} \subset \mathbb{Q}[\alpha] \subset L$ e $|G| = |H| = [L : \mathbb{Q}] = \big[L : \mathbb{Q}[\alpha]\big]\big[\mathbb{Q}[\alpha] : \mathbb{Q}\big]$. Portanto, $\big[\mathbb{Q}[\alpha] : \mathbb{Q}\big] = p$ divide $|H|$. Como $H \leq S_p$ segue do Teorema 5.1.14 que existe $a \in H$ tal que $|a| = p$. Sem perda de generalidade vamos denotar $a = (12 \cdots p)$.

Se $K = \mathbb{Q}[\alpha_1, \cdots, \alpha_{p-2}]$ onde $\alpha_1, \cdots, \alpha_{p-2}$ são as raízes reais de $f(x)$ então, segue que $L = K[\beta]$ onde β é uma raiz complexa de $f(x)$. Ainda, existe $\sigma \in Aut_K L$ tal que $\sigma(\beta) = \bar{\beta}$ pois $[L : K] = |Aut_K L| = 2$ e $\beta, \bar{\beta}$ são as raízes complexas, não reais, de $f(x)$ onde $\bar{\beta}$ é o complexo conjugado de β. Portanto, $\sigma \in Aut_{\mathbb{Q}} L$ e $\sigma(\alpha_i) = \alpha_i$ para cada $i = 1, 2, \cdots, p-2$ e $\sigma(\beta) = \bar{\beta}$. Renumerando os índices das raízes, se necessário, segue que a imagem de σ em S_p é uma transposição que podemos notar por $(12) \in H$.

Ora $(12 \cdots p)$, $(12) \in H \leq S_p$ o que implica, pelo Lema 4.3.7 que $G \simeq H = S_p$, como queríamos demonstrar. □

Exemplo 5.1.16. *Seja $p(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ e $L = Gal(p, \mathbb{Q})$. Então $G = Aut_{\mathbb{Q}} L \simeq S_5$. Em partiular, $Aut_{\mathbb{Q}} L$ não é um grupo solúvel. De fato, pelo Teorema 4.6.6, temos que $p(x)$ é irredutível sobre $\mathbb{Q}$. De fato, tomando $p = 3$ um inteiro primo, e sejam $a_0 = 3, a_1 = -6, a_2 = a_3 = a_4 = 0$ e $a_5 = 1$, tem-se*

a) $p \nmid a_5$;

b) $p \mid a_0, a_1, a_2, a_3, a_4$;

c) $p^2 \nmid a_0$.

Agora, como $\partial\, p(x) = 5$ *é um número primo e* $p(x)$ *é irredutível sobre* $\mathbb{Q}$, *pela Proposição 5.1.15, é suficiente provarmos que* $p(x)$ *possui exatamente três raízes reais. Faremos isso observando os valores*

$$p(-2) = (-2)^5 - 6 \cdot (-2) + 3 = -32 + 12 + 3 = -17$$
$$p(-1) = (-1)^5 - 6 \cdot (-1) + 3 = -1 + 6 + 3 = 8$$
$$p(0) = 0^5 - 6 \cdot 0 + 3 = 3$$
$$p(1) = 1^5 - 6 \cdot 1 + 3 = 1 - 6 + 3 = -2$$
$$p(2) = 2^5 - 6 \cdot 2 + 3 = 32 - 12 + 3 = 23.$$

Calculando a derivada, $p'(x) = 5x^4 - 6$, *vemos que* $p(x)$ *possui dois pontos críticos, justamente onde* $p'(x) = 0$. *São eles* $x_1 = \sqrt[4]{\frac{6}{5}} \approx 1,04664$ *e* $x_2 = -\sqrt[4]{\frac{6}{5}} \approx -1,04664$. *Com estas informações mais os pontos que conhecemos, temos que* x_1 *é um máximo local e* x_2 *é um mínimo local. Além disso, note que* $p(x)$ *é crescente nos intervalos* $(-\infty, -2]$ *e* $[2, +\infty)$, *pois* $p'(x) > 0$ *nestes intervalos. Logo,* $p(x)$ *possui uma raiz entre* -2 *e* -1, *outra raiz entre* 0 *e* 1, *e uma terceira raiz entre* 1 *e* 2, *e estas são todas as raízes reais. Logo,* $p(x)$ *possui três raízes reais e duas complexas.*

Logo, $G = Aut_{\mathbb{Q}}L \simeq S_5$.

Por fim, observamos que $Aut_{\mathbb{Q}}L$ *não é um grupo solúvel. Pelo Corolário 4.5.21, temos que* S_5 *não é solúvel, e como* $Aut_{\mathbb{Q}}L \simeq S_5$, *segue que* $Aut_{\mathbb{Q}}L$ *não é solúvel.*

Na continuidade do estudo sobre Teoria de Galois e Solubilidade por meio de radicais, pode-se resolver novamente o Exemplo 5.1.16, mostrando que este não é solúvel por meio de radicais.

6 CONSIDERAÇÕES FINAIS

Este trabalho possibilitou a ampliação dos conhecimentos de Álgebra Abstrata, partindo da retomada e complementação dos conteúdos que já haviam sido estudados, tais como, anéis, ideais, grupos e corpos, além de tópicos de Álgebra Linear. Também foi possível compreender a extensão de corpos, onde, de um corpo K se pode construir um outro corpo L tal que $L \supset K$, bem como as propriedades das extensões, os elementos e as extensões algébricas e transcendentais. No capítulo cinco, podemos entender a parte introdutória à Teoria de Galois, com o estudo de extensões Galoisianas e extensões normais, possibilitando um posterior estudo à Teoria de Galois e a solubilidade de polinômios de grau maior ou igual a cinco por meio de radicais.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] ANDRADE J. F. S. **Tópicos Especiais em Álgebra** 1. ed. Rio de Janeiro: SBM, 2013.

[2] BAUMGART J. K. **Tópicos de história da matemática para uso em sala de aula - Álgebra**. Tradução: Hygino H. D. São Paulo: Atual, 1992.

[3] BUENO H. P. **Álgebra Linear: um Segundo Curso**. 1. ed. Rio de Janeiro: SBM, 2006.

[4] DOMINGUES H. H., IEZZI G. **Álgebra Moderna**. 4. ed. São Paulo: Atual, 2003.

[5] LIMA E. L. **Álgebra Linear**. 9. ed. Rio de Janeiro: IMPA, 2016.

[6] EVES H. **Introdução à História da Matemática**. Campinas, São Paulo: Editora da UNICAMP, 2004.

[7] GALLIAN J. A., **Contemporary Abstract Algebra**. 8. ed. Edição Internacional: CENGAGE Learning, 2013.

[8] GARCIA A., LEQUAIN Y. **Elementos de Álgebra**. 6. ed. Rio de Janeiro: IMPA, 2015.

[9] GIL A. C. **Como Elaborar Projetos de Pesquisa**. 5. ed. São Paulo: Atlas, 2010.

[10] GONÇALVES A. **Introdução à Álgebra**. 5. ed. Rio de Janeiro: IMPA, 2015.

[11] KATZ V. J. **História da Matemática**. 2. ed. Lisboa: Fundação Calouste Gulbenkian, 2010.

[12] MARTIN P. A. **Grupos, Corpos e Teoria de Galois**. 1 ed. São Paulo: Editora Livraria da Física, 2010.