Joel Albertacci Marques da Silva

Um estudo sobre a não resolubilidade de equações algébricas de grau maior ou igual a 5

Volta Redonda, RJ

2021

Joel Albertacci Marques da Silva

Um estudo sobre a não resolubilidade de equações algébricas de grau maior ou igual a 5

Trabalho de Conclusão de Curso submetido ao Curso de Matemática com ênfase em Matemática Computacional da Universidade Federal Fluminense como requisito parcial para a obtenção do título de Bacharel em Matemática.

Universidade Federal Fluminense

Instituto de Ciências Exatas

Curso de Matemática

Orientador: Profa. Dra. Rosemary Miguel Pires

Volta Redonda, RJ

2021

Ficha catalográfica automática - SDC/BAVR
Gerada com informações fornecidas pelo autor

S586e Silva, Joel Albertacci Marques da
Um estudo sobre a não resolubilidade de equações algébricas de grau maior ou igual a 5 / Joel Albertacci Marques da Silva ; Rosemary Miguel Pires, orientadora. Volta Redonda, 2021.
99 f. : il.

Trabalho de Conclusão de Curso (Graduação em Matemática)- Universidade Federal Fluminense, Instituto de Ciências Exatas, Volta Redonda, 2021.

1. Galois. 2. Grupos. 3. Polinômios. 4. Produção intelectual. I. Pires, Rosemary Miguel, orientadora. II. Universidade Federal Fluminense. Instituto de Ciências Exatas. III. Título.

CDD -

Bibliotecário responsável: Debora do Nascimento - CRB7/6368

Joel Albertacci Marques da Silva

Um estudo sobre a não resolubilidade de equações algébricas de grau maior ou igual a 5

Trabalho de Conclusão de Curso submetido ao Curso de Matemática com ênfase em Matemática Computacional da Universidade Federal Fluminense como requisito parcial para a obtenção do título de Bacharel em Matemática.

Trabalho aprovado. Volta Redonda, RJ, 30 de abril de 2021:

Profa. Dra. Rosemary Miguel Pires – UFF
Orientador

Prof. Dr. Carlos Henrique Pereira do Nascimento – UFF

Profa. Dra. Dylene Agda Souza de Barros – UFU

Volta Redonda, RJ
2021

Este trabalho é dedicado à todas as pessoas que sempre acreditaram em mim.

Agradecimentos

Agradeço primeiro a Deus por ter concedido a mim capacidade cognitiva e emocional para concluir este curso, e aos meus pais por todo o suporte que foi dado a mim durante todo este período. Agradeço também à minha maravilhosa namorada Elisa, que mesmo chegando em minha vida ao final desta caminhada, trouxe muito amor, apoio, alegria, iluminação e convicção para a minha caminhada profissional.

Agradeço aos meus estimados amigos da Univerisade Federal Flumimense: Guilherme Saroka, Guylherme Mattos, João Pedro, Mariana Macedo, Nelson de Assis, Orlando Warlem, Patrick Alves, Rayan Gustavo e Tais Carvalho. A vocês o meu muito obrigado pelo companheirismo, bons momentos, e por tornarem as coisas mais simples.

Agradeço também a todos os professores pela contribuição à minha formação. Em especial à professora Rosemary M. Pires, pela confiança, pelo entusiasmo, e pela oportunidade única de aprendizado no que diz respeito à área de pesquisa em Matemática Pura.

Faça ou não faça! Tentativa não há.
(Mestre Yoda, O Império Contra-Ataca)

Resumo

Este trabalho tem como objetivo estabelecer toda a base teórica referente ao conteúdo da Teoria de Galois, e posteriormente, utilizar todos estes coneceitos desenvolvidos para classificar os grupos de Galois de polinômios irredutíveis de grau $n \leq 4$ e, finalmente, mostrar que não é possível existir uma fórmula resolutiva geral para as equações polinomiais de grau $n \geq 5$. Para isto, incialmente foram estabelecidas as definições e os resultados preliminares mais importantes que são necessários para classificar os grupos de Galois, e mostrar a não resolubilidade das equações com grau superior a 5. Ao longo do trabalho todas as definições e resultados são ilustrados com exemplos práticos que permitem um entendimento mais claro sobre o assunto como um todo. Toda esta teoria desenvolvida permite a conclusão de que é necessário a utilização de métodos numéricos para obter as raízes de determinadas equações algébricas de grau superior a 5.

Palavras-chave: Galois. Grupos. Polinômios.

Abstract

This work aims to establish the entire theoretical basis regarding the content of Galois Theory, and then use all these concepts to classify the Galois groups of irreducible polynomials of degree $n \leq 4$ and, finally, to show that it is not possible to have a general resolutive formula for algebraic equations of degree $n \geq 5$. For this purpose, the most important preliminary definitions and results that are necessary to classify Galois groups were initially established, so we can finally show the non-solvability of equations with degree greater than 5. Throughout the work, all definitions and results are illustrated with practical examples that allow a better understanding of the subject as a whole. All this developed theory allows the conclusion that it is necessary to use numerical methods to obtain the roots of certain algebraic equations with a degree greater than 5.

Keywords: Galois. Group. Polynomial.

Lista de ilustrações

Lista de tabelas

Lista de símbolos

$irr(\alpha, K)$	Polinômio irredutível de menor grau com coeficientes no corpo K, que possui α como raiz.
$\partial(f(x))$	Grau do polinômio $f(x)$.
$Aut_K L$	Grupo de Galois associado a extensão de corpos $L \supset K$.
$L \supset K$	Extensão de corpos em que K é um subcorpo de L.
$\mathbb{V}$	O grupo de Klein.
ζ	Raíz primitiva n-ésima da unidade.

Sumário

1 Introdução

Considere o polinômio $p(x) = \sum_{i=0}^{n} a_i x^i$, com $a_i \in K$, $\forall i \in \{0, 1, \cdots, n\}$, onde K é um corpo tal que $\mathbb{Q} \subset K \subset \mathbb{C}$. Descobrir as raízes do polinômio $p(x)$ através de cálculos por operações algébricas com os coeficientes a_i sempre foi um problema desafiador e de extrema importância, não apenas no ramo da Matemática Pura, mas também na Matemática Aplicada e em qualquer outra ciência exata.

Se impormos que $n = 2$, teremos $i \in \{0, 1, 2\}$, e obtemos $p(x) = a_0 + a_1 x + a_2 x^2$. Qualquer estudante do ensino básico conhece a fórmula:

$$x = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2 a_0}}{2a_2}$$

que fornece as duas raízes da equação algébrica $a_0 + a_1 x + a_2 x^2 = 0$ em $\mathbb{C}$. O que poucos sabem é que também existem fórmulas resolutivas para equações polinomiais de terceira e quarta ordem. Porém, tais fórmulas são de alta complexidade e por isso, não são estudadas no ensino básico. Em relação a polinômios $p(x)$ com grau $n \geq 5$ temos o seguinte questionamento: é possível existir uma fórmula resolutiva envolvendo operações algébricas básicas (soma, subtração, multiplicação e divisão) e aplicação de radicais para determinarmos as raízes de $p(x)$ como função de seus coeficientes? Esta pergunta foi um problema em aberto na Matemática durante séculos, e foi respondida pelo jovem francês Évariste Galois no século XIX.

O problema da solubilidade de equações algébricas de quinta ordem foi o ponto de partida para Galois criar a teoria que leva o seu nome.

A ideia principal que Galois teve para resolver este problema foi considerar o conjunto das permutações das raízes da equação polinomial, essencialmente desenvolvendo a ideia de grupo, que era um conceito até então não formalizado. Foi Galois o responsável por introduzir o termo grupo pela primeira vez no seu sentido técnico, o qual conhecemos atualmente.

Um estudo completo sobre a Teoria de Galois exige uma abordagem ampla em conceitos de Álgebra, e além disso, motiva um estudo aprofundado de duas grandes subáreas da Álgebra Abstrata, que são: Teoria de Corpos e Teoria de Grupos. Com isto dito, para uma correta compreensão do assunto, devemos estabelecer primeiro certos conceitos preliminares necessários antes de chegarmos no ponto principal deste trabalho. É claro que iremos aceitar alguns resultados mais básicos, como toda a parte inicial referente a polinômios em uma variável, bem como o critério de irredutibilidade de Eisenstein, o qual usaremos algumas vezes no decorrer deste trabalho. Aceitaremos também toda a parte

inicial referente Teoria de Grupos, como resultados referentes a subgrupos, subgrupos normais, grupos de permutações, notação cíclica, Teorema dos Isomorfismos e Teoremas de Sylow. O objetivo do traballho é utilizar todo esse conhecimento prévio juntamente com o que será abordado aqui para que possamos mostrar a não solubilidade de polinômios de grau $n \geq 5$.

2 Extensões Algébricas dos Racionais

Neste capítulo, nosso objetivo é a construção de corpos K, de forma que $\mathbb{Q} \subset K \subset \mathbb{C}$. Veremos que tal processo construtivo se dá através da adjunção de raízes de um polinômio em um certo corpo. Serão enunciadas definições e certos resultados, bem como suas demonstrações. Tais resultados possuem grande importância para o desenvolvimento da Teoria de Galois. Este capítulo foi baseado especificamente nas referências [1], [2] e [3].

Um fato interessante é que a Teoria de Galois foi inicialmente concebida em termos de polinômios com coeficientes em $\mathbb{C}$. A abordagem moderna, que é feita atualmente na maioria dos livros, é uma consequência dos métodos utilizados nas pesquisas sobre generalização de Corpos que se iniciou no final do século XIX. Com esse novo ponto de vista, o objeto de estudo deixou de ser apenas um polinômio e se tornou uma extensão de Corpos associada a um certo polinômio. De fato, veremos que todo polinômio f com coeficientes em um certo corpo K define um outro corpo L tal que $L \supset K$. Como dissemos no parágrafo anterior, trabalharemos com extensões de $\mathbb{Q}$, isto significa que trabalharemos apenas com corpos de característica zero.

2.1 Extensões Algébricas e Transcendentes

Antes de começarmos o estudo sobre extensões de corpos, precisamos definir o que é uma extensão.

Definição 2.1.1. Dados dois corpos L e K tais que $K \subset L$, isto é, K é um sucorpo de L. Dizemos que L é uma extensão do corpo K.

Os exemplos mais clássicos de extensões de corpos são dados abaixo:

Exemplo 2.1.1. *Extensões de corpos.*

1. $\mathbb{C} \supset \mathbb{R}$.
2. $\mathbb{C} \supset \mathbb{Q}$
3. $\mathbb{R} \supset \mathbb{Q}$
4. $\mathbb{Q}[\sqrt{2}] \supset \mathbb{Q}$ *onde* $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$.

Em particular, o exemplo (4) e seus similares terão uma grande importância para o desenvolvimento deste trabalho. Isto nos motiva a enunciar a seguinte definição:

Definição 2.1.2. Seja $L \supset K$ uma extensão de corpos. Um elemento $\alpha \in L$ é algébrico sobre o corpo K se existe um polinômio $f(x) \in K[x] \setminus \{0\}$ tal que $f(\alpha) = 0$.

Observação 2.1.1. *Em outras palavras, dizer que um certo elemento $\alpha \in L$ é algébrico sobre K, significa dizer que existem elementos $a_0, a_1, \cdots, a_n \in K$, com $a_n \neq 0$ tais que*

$$\sum_{i=0}^{n} a_i \alpha^i = 0$$

Note que a partir da Observação 2.1.1 fica evidente o porquê de impormos que $f(x) \neq 0$ na Definição 2.1.2. E além disso, observe também que todo elemento $\alpha \in K$ é algébrico sobre K. Isto é verdade porque o polinômio $x - \alpha$ é anulado por α, $\forall \alpha \in K$.

Definição 2.1.3. Dizemos que $\alpha \in L$ é transcendente sobre K quando α não é algébrico sobre K.

Consideremos os exemplos abaixo:

Exemplo 2.1.2. *Alguns exemplos de extensões algébricas e transcendentes.*

- $\sqrt{2} \in \mathbb{R}$ *é algébrico sobre* $\mathbb{Q}$. *De fato,* $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ *e* $f(\sqrt{2}) = 0$.
- $i \in \mathbb{C}$ *é algébrico sobre* $\mathbb{R}$ *e sobre* $\mathbb{Q}$, *pois* $g(x) = x^2 + 1 \in \mathbb{R}[x]$ *e* $\mathbb{Q}[x]$ *é tal que* $g(i) = 0$.
- *Os números* π *e a constante de Euler são transcendentes sobre* $\mathbb{Q}$. *De fato, não existe polinômio* $f(x) \in \mathbb{Q}[x]$ *tal que* $f(\pi) = 0$ *e* $f(e) = 0$.

Definição 2.1.4. Uma extensão $L \supset K$ é algébrica quando α é algébrico sobre K, $\forall \alpha \in L$. Caso contrário, a extensão é chamada de transcendente.

Exemplo 2.1.3. *A extensão* $\mathbb{R} \supset \mathbb{Q}$ *é transcendente, pois* $\pi \in \mathbb{R}$ *é transcendente.*

Exemplo 2.1.4. *A extensão* $\mathbb{C} \supset \mathbb{R}$ *é algébrica, pois todo elemento de* $\mathbb{C}$ *satisfaz uma equação do segundo grau com coeficientes em* $\mathbb{R}$.

Teorema 2.1.5. *Sejam L e K corpos tais que $L \supset K$ seja uma extensão e $\alpha \in L$. Defina*

$$\begin{array}{rccc} \psi\colon & K[x] & \longrightarrow & L \\ & f(x) & \longmapsto & f(\alpha) \end{array}$$

Temos que ψ é um homomorfismo de anéis e que:

1. $\psi(K[x]) = K[\alpha]$ *e* $K \subset K[\alpha] \subset L$.
2. *O elemeto α é transcendente sobre K se, e somente se,* $Ker(\psi) = \{0\}$.

3. *Se $\alpha \in L$ é algébrico sobre K e $p(x) = irr(\alpha, K)$ então $Ker(\psi) = K[x] \cdot p(x)$ é um ideal maximal de $K[x]$.*

4. $\dfrac{K[x]}{Ker(\psi)} \simeq K[\alpha]$.

Sejam $L \supset K$ uma extensão de corpos e $\alpha \in L$. Se $f(x) \in K[x]$ é mônico, irredutível e $f(\alpha) = 0$, então $f = irr(\alpha, K)$.

Demonstração:

A demonstração pode ser encontrada em [1].

Lema 2.1.1. *Sejam $L \supset K$ uma extensão de corpos e $\alpha \in L$. Se $f(x) \in K[x]$ é um polinômio mônico, irredutível tal que $f(\alpha) = 0$, então $f(x) = irr(\alpha, K)$.*

Demonstração: Sabemos pelo Teorema 2.1.5 que $Ker(\psi) = K[x] \cdot irr(\alpha, K)$. Como $f(\alpha) = 0$, então $f(x) \in Ker(\psi)$. Como $f(x)$ é irredutível, existe $a \in K \setminus \{0\}$ tal que $f(x) = a \cdot irr(\alpha, K)$. Como $f(x)$ e $irr(\alpha, K)$ são mônicos, segue-se que $a = 1$ e portanto, $f(x) = irr(\alpha, K)$.

■

Corolário 2.1.1. *Sejam $L \supset K$ uma extensão de corpos. As seguintes afirmações são verdadeiras:*

1. *Se $\alpha \in L$ é algébrico sobre K, então $K[\alpha]$ é um subcorpo de L que contém K.*

2. *Se $\alpha \in L$ é transcendente sobre K então $K[\alpha]$ é um subdomínio de L que contém o corpo K e $K[\alpha] \simeq K[x]$.*

3. *Se $\alpha, \beta \in L$ e $f(x) \in K[x]$ é irredutível sobre K tal que $f(\alpha) = f(\beta) = 0$, então $K[\alpha] \simeq K[\beta]$.*

A demonstração pode ser encontrada em [1].

Encerraremos esta seção com a proposição abaixo, a qual nos dá uma forma muito simples de obter os elementos de extensões do tipo $K[\alpha]$, onde $\alpha \in L$ é algébrico sobre K.

Proposição 2.1.1. *Sejam $L \supset K$ uma extensão de corpos, e $\alpha \in L$ algébrico sobre K. Se o grau de $irr(\alpha, K)$ é n, então são verdadeiras as afirmações abaixo:*

1. *Para todo $f(x) \in K[x]$, o número $f(\alpha)$ pode ser obtido de forma única como $f(\alpha) = \sum_{i=0}^{n-1} a_i \alpha^i$ onde $a_i \in K$, $\forall i \in \{0, \cdots, n-1\}$.*

2. $K[\alpha] = \{\sum_{i=0}^{n-1} a_i\alpha^i | a_i \in K\}$.

A demonstração pode ser encontrada em [1].

2.2 Grau de uma Extensão

Foi abordado na seção anterior sobre extensões algébricas, e agora, estudaremos extensões finitas, que é um conceito extremamente importante para a nossa teoria. Veremos aqui que as extensões finitas são casos especiais de extensões algébricas.

Dada uma extensão de corpos $L \supset K$, podemos considerar L como um K-espaço vetorial. Ora, tratando-se de um corpo, em L temos as seguintes operações binárias:

$$\begin{array}{rccc} +: & L \times L & \longrightarrow & L \\ & (x, y) & \longmapsto & x + y \end{array}$$

$$\begin{array}{rccc} \cdot: & L \times L & \longrightarrow & L \\ & (x, y) & \longmapsto & x \cdot y \end{array}$$

satisfazendo todas as propriedades que dão a estrutura algébrica a um corpo. Sendo K um subcorpo de L, as operações de K são as operações de L restritas. Assim, podemos considerar

$$\begin{array}{rccc} \cdot: & K \times L & \longrightarrow & L \\ & (x, y) & \longmapsto & x \cdot y \end{array}$$

que está claramente bem definida, uma vez que $K \subset L$. Isto é, esta restrição podemos interpretar como o produto por escalar do espaço vetorial, onde os elementos de L são os vetores e os elementos de K são os escalares. Assim, a operação soma juntamente com esta restrição da operação produto dão naturalmente a estrutura de K-espaço vetorial para L.

Observação 2.2.1. *Nessas condições, se M é um subcorpo de L contendo K, então M é um K-subespaço vetorial de L. De fato, se denotarmos o elemento nulo de L por 0_L, temos é claro, que $O_L \in M$, pois M é subcorpo de L. E, dados $x, y \in M$ e $\alpha \in K$, temos que $x + \alpha y \in M$, pois em particular, $\alpha \in M$ e M é fechado para as duas operações. Isto mostra que todo subcorpo de L que contém K será um K-subespaço vetorial de L.*

Agora, seguimos para a definição de extensão finita:

Definição 2.2.1. Seja $L \supset K$ uma extensão de corpos qualquer. Dizemos que $L \supset K$ é uma extensão finita se a dimensão do K-espaço vetorial L for finita. Caso contrário, dizemos que $L \supset K$ é uma extensão infinita.

Observação 2.2.2. *Neste contexto de extensão de corpos, a notação para $dimL$ é $[L : K]$, e é chamado de grau da extensão de L para K.*

Exemplo 2.2.1. *São exemplos de extensões finitas:*

1. $\mathbb{C} \supset \mathbb{R}$ *é uma extensão finita. Note que pela definição,* $\mathbb{C} = \{a + bi | a, b \in \mathbb{R}\}$. *Isto mostra que o conjunto* $\{1, i\}$ *é um gerador para* $\mathbb{C}$, *e mais ainda, tal conjunto trata-se de uma base, pois este é linearmente independente sobre* $\mathbb{C}$, *pois* $a + bi = 0$ *implica necessariamente que* $a = b = 0$. *Portanto,* $[\mathbb{C} : \mathbb{R}] = 2$.

2. $\mathbb{Q}[\sqrt{2}] \supset \mathbb{Q}$ *é uma extensão finita. De fato,* $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$. *Isto é,* $\{1, \sqrt{2}\}$ *é um conjunto gerador para* $\mathbb{Q}[\sqrt{2}]$. *O argumento para mostrarmos que este conjunto é lineramente independente sobre* $\mathbb{Q}[\sqrt{2}]$ *é bem simples. De fato, se* $a + b\sqrt{2} = 0$ *então* $b\sqrt{2} = -a$. *Agora, observe que se* $b \neq 0$, *emtão teríamos que* $\sqrt{2} = \dfrac{-a}{b}$. *Mas isto é uma contradição, pois* $\sqrt{2} \notin \mathbb{Q}$. *Logo,* $b = 0$ *e consequentemente* $a = 0$. *Portanto,* $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$.

Teorema 2.2.2. *Se* $L \supset K$ *é uma extensão finita, então* $L \supset K$ *é uma extensão algébrica.*

A demonstração pode ser encontrada em [1].

Exemplo 2.2.2. *A extensão* $\mathbb{R} \supset \mathbb{Q}$ *é uma extensão infinita. De fato, vimos na seção anterior que esta extensão é transcendente, e pela contrapositiva do Teorema anterior, segue-se que* $\mathbb{R} \supset \mathbb{Q}$ *é extensão infinita.*

Teorema 2.2.3. *Seja* $L \supset K$ *uma extensão de corpos. Se* $\alpha \in L$ *é algébrico sobre* K *e o grau de* $irr(\alpha, K) = n$, *então* $K[\alpha] \supset K$ *é uma extensão finita com* $[K[\alpha] : K] = n$. *Mais ainda, o conjunto* $\{1, \alpha, \cdots, \alpha^{n-1}\}$ *é uma base de* $K[\alpha]$.

A demonstração pode ser encontrada em [1].

Exemplo 2.2.3. *Considere os exemplos abaixo:*

1. *Já vimos que* $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$. *De fato, temos que* $irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2$. *De fato,* $x^2 - 2$ *é mônico e irredutível sobre* $\mathbb{Q}$.

2. $\sqrt[8]{7} \in \mathbb{R}$ *é algébrico sobre* $\mathbb{Q}$. *De fato,* $f(x) = x^8 - 7 \in \mathbb{Q}[x]$ *é mônico, irredutível sobre* $\mathbb{Q}$ *e* $f(\sqrt[8]{7}) = 0$. *Logo,* $[\mathbb{Q}[\sqrt[8]{7}] : \mathbb{Q}] = 8$, *pois* $irr(\sqrt[8]{7}, \mathbb{Q}) = x^8 - 7$. *E ainda pelo Teorema anterior, o conjunto* $\{1, \sqrt[8]{7}, (\sqrt[8]{7})^2, (\sqrt[8]{7})^3, \sqrt[8]{7}^4, (\sqrt[8]{7})^5, (\sqrt[8]{7})^6, (\sqrt[8]{7})^7\}$ *é uma base para o espaço vetorial* $\mathbb{Q}[\sqrt[8]{7}]$.

3. *De maneira geral, sendo* p *um número primo e* $n \in \mathbb{N}$, *temos que* $\sqrt[n]{p} \in \mathbb{R} \setminus \mathbb{Q}$ *é algébrico sobre* $\mathbb{Q}$. *O qual é anulado pelo polinômo* $x^n - p \in \mathbb{Q}[x]$, *que é irredutível e mônico em* $\mathbb{Q}$. *Isto implica, pelo Teorema anterior que* $\{1, \sqrt[n]{p}, \cdots, (\sqrt[n]{p})^{n-1}\}$ *é uma base para o espaço vetorial* $\mathbb{Q}[\sqrt[n]{p}]$ *sobre o corpo* $\mathbb{Q}$.

E como consequência do último teorema, temos o seguinte corolário:

Corolário 2.2.1. *Seja $L \supset K$ uma extensão de corpos e $\alpha \in L$. Os seguintes ítens são equivalentes:*

1. *α é algébrico sobre K.*
2. *$K[\alpha] \supset K$ é uma extensão finita.*
3. *$K[\alpha] \supset K$ é uma extensão algébrica.*

A demonstraçao pode ser encontrada em [1].

Proposição 2.2.1. *Seja $L \supset K$ uma extensão de corpos. Então $[L : K] = 1$ se, e somente se, $L = K$.*

Demonstração: Como $[L : K] = 1$ e como $\{1\}$ é linearmente independente tanto em L quando em K então da Álgebra Linear básica, sabemos que $\{1\}$ será uma base de L sobre o corpo K. Já sabemos que $K \subset K$. Assim, para mostrarmos que $L \subset K$, suponha que $x \in L$ então existe $\alpha \in K$ tal que $u = \alpha 1 = \alpha$, o que implica que $x \in K$. Portanto, $L = K$. Reciprocamente, como todo corpo é um espaço vetorial sobre ele mesmo de dimensão 1, então se $L = K$, o resultado é imediato. Basta tomarmos a base $\{1\}$, e teremos $[L : K] = 1$.

■

Dada as extensões finitas $L \supset K$ e $M \supset L$, isto naturalmente induz uma extensão maior $M \supset K$. O próximo resultado é de extrema importância, pois se as extensões $L \supset K$ e $M \supset L$ forem finitas, então a extensão $M \supset K$ também será finita. E mais ainda, este resultado nos dá uma forma de calcular o grau da extensao $[M : K]$, uma vez que $[M : L]$ e $[L : K]$ sejam valores conhecidos. Este resultado é tradicionalmente conhecido como Lei da Torre, pois o que teremos nada mais é do que uma torre de corpos, conforme o diagrama abaixo:

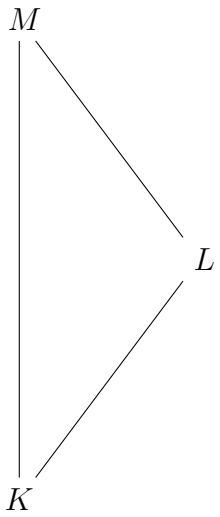

Figura 1 – Diagrama de corpos

Teorema 2.2.4 (Lei da Torre)**.** *Sejam $M \supset L \supset K$ extensões de corpos. Então $M \supset L$ e $L \supset K$ são finitas se, e somente se, $M \supset K$ for finita. E neste caso, teremos:*

$$[M : K] = [M : L][L : K]$$

Demonstração: Suponhamos primeiro que $M \supset K$ seja uma extensão finita. Vamos mostrar primeiro que $L \supset K$ é finita. Dde fato, como L é um K-subespaço vetorial de M, então $dimL \leq dimM$ e como $dimM$ é finita, então $dimL$ é finita, e assim, $L \supset K$ é uma extensão finita. Agora, mostraremos que $M \supset L$ é finita. Assim, seja $[M : K] = n$ e suponha por absurdo que $M \supset L$ seja uma extensão infinita. Então para cada $r \in \mathbb{N}$ fixado, existe um subconjunto linearmente independente com r elementos. Vamos tomar $r = n + 1$. Assim, existem $u_1, \cdots u_{n+1} \in M$ que são linearmente independentes sobre L.

Sejam $\alpha_1, \cdots \alpha_{n+1} \in K$ tais que,

$$\sum_{i=1}^{n+1} \alpha_i u_i = 0$$

como $K \subset L$ então $\alpha_1, \cdots \alpha_{n+1} \in L$ e como $\{u_1, \cdots, u_{n+1}\}$ é linearmente independente sobre L, então isso implica que $\alpha_i = 0$, $\forall i \in \{1, \cdots n + 1\}$. Logo, $\{u_1, \cdots, u_{n+1}\}$ é linearmente independente sobre K. Mas isto implica que $n + 1 \leq dimM = n$ e assim, concluímos que $1 \leq 0$, o que é absurdo. Portanto, $M \supset L$ é uma extensão finita como queríamos. A demonstração da recíproca e de que $[M : K] = [M : L][L : K]$ pode ser encontrada em 1.

■

A generalização deste resultado também é verdadeira. Isto é o que afirma o seguinte corolário:

Corolário 2.2.2. *Se $K_1 \subset \cdots \subset K_r$ é uma torre de corpos, onde $K_{i+1} \supset K_i$ é uma extensão finita para todo $i \in \{1, \cdots, r\}$, então $K_r \supset K_1$ é uma extensão finita e*

$$[K_r : K_1] = \prod_{i=1}^{n-1} [K_{i+1} : K_i]$$

A demonstração pode ser encontrada em [2].

2.3 Corpo de Decomposição de um Polinômio

Devido a facilidade de trabalhar com polinômios na forma de produtos de fatores lineares, é conveniente estabelecermos a seguinte definição:

Definição 2.3.1. Sejam $K \subset \mathbb{C}$ e f um polinômio com coeficientes em K. Diz-se que f pode ser fatorado sobre K se puder ser expresso como produto de fatores lineares. Isto é,

$$f(x) = m(x - \alpha_1) \cdots (x - \alpha_n)$$

onde $m, \alpha_1, \cdots, \alpha_n \in K$.

É claro que neste caso, $f(\alpha_i) = 0, \forall i \in \{1, \cdots, n\}$. Ou seja, as raízes de f pertencem ao corpo K. Além disso, o **Teorema Fundamental da Álgebra** garante que f pode ser fatorado sobre K se, e somente se, todas as suas raízes complexas estiverem em K. Ou seja, equivalentemente, K contém o subcorpo gerado por todas as raízes do polinômio f.

Exemplo 2.3.1. *Considere o polinômio $f(x) = x^4 - 4x^2 - 5 \in \mathbb{Q}[x]$. Note que f fatora-se sobre $\mathbb{Q}[i, \sqrt{5}]$. De fato, $f(x) = (x-i)(x+i)(x-\sqrt{5})(x+\sqrt{5})$. Entretanto, se considerarmos a extensão $\mathbb{Q}[i]$, obtemos $f(x) = (x - i)(x + i)(x^2 - 5)$. Veja que o último fator não é redutível e nem linear. Logo, f não se fatora sobre $\mathbb{Q}[i]$.*

Note que, se $L \supset K$ é uma extensão de corpos, e f é um polinômio sobre K, então é claro que f também é um polinômio sobre L, podendo ou não ser fatorado em L. Nesse caso, é válido dizer que dado um corpo K e um polinômio f, podemos construir uma extensão de $L \supset K$ tal que f se fatora sobre tal extensão. Podemos ainda restringir mais e exigir que f não se fatore sobre nenhum corpo menor do que L. Com isso, podemos enunciar a próxima definição.

Definição 2.3.2. Sejam $\Sigma \subset \mathbb{C}$ e f um polinômio com coeficientes em $K \subset \mathbb{C}$. Diz-se que Σ é o corpo de decomposição de f sobre K se $K \subset \Sigma$ e se as condições abaixo forem cumpridas:

- f se fatora sobre Σ
- Se existe um subcorpo Σ', tal que $K \subset \Sigma' \subset \Sigma$ e f se fatora sobre Σ', então $\Sigma' = \Sigma$.

Observação 2.3.1. *Por conveniência, a partir de agora, denotaremos o corpo de decomposição Σ do polinômio f sobre K como $Gal(f, K)$.*

Observação 2.3.2. *O segundo item da definição acima é equivalente a seguinte igualdade:*

$$Gal(f, K) = K[\sigma_1, \sigma_2, \cdots, \sigma_n]$$

onde $\sigma_1, \sigma_2, \cdots, \sigma_n$ são as raízes de f em $Gal(f, K)$. Isto é, o processo de adjunção de raízes é o método construtivo do corpo de decomposição de um polinômio $f \in K[x]$.

A observação anterior nos diz que para obtermos o corpo de decomposição de um polinômio $f \in K[x]$, basta adjuntarmos suas raízes em K. Mas nem sempre é necessário adjuntar todas as raízes. Ou seja, se $\alpha_1, \cdots, \alpha_r$ são as r raízes de f, às vezes basta adjuntar uma certa raiz a_i, $i \in \{1, \cdots, r\}$ que as demais automaticamente estarão inclusas. Considere o exemplo abaixo.

Exemplo 2.3.2. *Seja $\{\alpha_0, \alpha_1, \cdots, \alpha_{n-1}\}$ o conjunto das n raízes em $\mathbb{C}$ do polinômio $f(x) = x^n - 1 \in \mathbb{Q}[x]$ com $n > 1$. Suponha, sem perda de generalidade, que $\alpha_0 = 1$. Neste caso, sabemos que se $\alpha = cos\frac{2\pi}{n} + isen\frac{2\pi}{n} \in \mathbb{C}$, então $\alpha^n = 1$ e $\alpha_j = \alpha^j \in \mathbb{Q}[\alpha], \forall i \in \{0, \cdots, n-1\}$. Logo, é necessário adjuntar apenas α em $\mathbb{Q}$. E portanto, $Gal(f, K) = \mathbb{Q}[\alpha_1]$.*

Teorema 2.3.3. *Seja $K \subset \mathbb{C}$ um corpo qualquer. Se $f \in K[x]$, então existe um único corpo de decomposição $Gal(f, K)$. Além disso, a extnsão $Gal(f, K) \supset K$ é finita.*

Demonstração: Sendo $\alpha_1, \cdots, \alpha_n$ as n raízes de f em $\mathbb{C}$, para provarmos a existência, basta adjuntarmos as n raízes de f ao corpo K. Pela definição, obtemos $Gal(f, K) = K[\alpha_1, \cdots, \alpha_n]$. Pelo item 2 da Definição 2.3.2, segue-se que $Gal(f, K)$ é único. Além disso, como $K[\alpha_1, \cdots, \alpha_n]$ é finitamente gerado (seu elementos são combinações lineares de α_i, $i = 1, \cdots, n$) e é extensão algébrica, segue-se pela Lei da Torre que $Gal(f, K) \supset K$ é uma extensão finta, como queríamos.

■

Agora iremos enunciar e demonstrar alguns resultados a respeito de subcorpos isomorfos em $\mathbb{C}$. Mas antes devemos fazer algumas considerações.

Considere os corpos $K, K' \subset \mathbb{Q}$, $\sigma : K \longrightarrow K'$ um isomorfismo e o polinômio f com coeficientes em K. Sendo $f(x) = a_0 + a_1x + ... + a_nx^n$, definimos o polinômio $f^\sigma(x) = \sigma(a_0) + \sigma(a_1)x + ... + \sigma(a_n)x^n$ como a imagem de f pelo isomorfismo σ. Note que se $f(x) = f_1(x)...f_n(x)$ é um produto de polinômios irredutíveis, então $f^\sigma(x) = f_1^\sigma(x)...f_n^\sigma(x)$ também é um produto de polinômios irredutíveis. Em particular, se f possui todas as suas raízes em K, então f^σ também possui todas as suas raízes em K'.

Lema 2.3.1. *Sejam os corpos $K, K' \subset \mathbb{C}$, $\sigma : K \longrightarrow K'$ um isomorfismo e h um polinômio irredutível em K. Se $\alpha \in \mathbb{C}$ é uma raíz de h e β é uma raíz de h^σ, então existe um único isomorfismo $\hat{\sigma} : K[\alpha] \longrightarrow K'[\beta]$ tal que $\hat{\sigma}(\alpha) = \beta$ e $\hat{\sigma}|_K = \sigma$.*

Demonstração: Suponha que $\partial(h) = m$, e consequentemente, $\partial(h^\sigma) = m$. Sabemos que os corpos $K[\alpha]$ e $K'[\beta]$ possuem estrutura de espaço vetorial sobre os corpos K e K' respectivamente. Além disso, como vimos, tais conjuntos possuem as seguintes descrições:

- $K[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} | a_i \in K, i = 0, 1, \cdots, m-1\}$
- $K'[\beta] = \{b_0 + b_1\beta + \cdots + b_{m-1}\beta^{m-1} | b_i \in K', i = 0, 1, \cdots, m-1\}$

Ou seja, os conjuntos $\mathcal{B}_{K[\alpha]} = \{1, \alpha, \alpha^2, \cdots, \alpha^{m-1}\}$ e $\mathcal{B}_{K'[\beta]} = \{1, \beta, \beta^2, \cdots, \beta^{m-1}\}$ são bases de $K[\alpha]$ e $K'[\beta]$ respectivamente.

Defina $\hat{\sigma}: \ K[\alpha] \longrightarrow K'[\beta]$ dado por

$$\hat{\sigma}(x) = \hat{\sigma}(a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}) = \sigma(a_0) + \sigma(a_1)\beta + \cdots + \sigma(a_{m-1})\beta^{m-1}$$

com $x \in K[\alpha]$.

Afirmamos que $\hat{\sigma}$ é um isomorfismo de corpos. Para verificarmos isso, primeiro, provemos que se trata de um homomorfismo de corpos. Assim, dados, $x, y \in K[\alpha]$, tem-se:

$$\begin{aligned}
\hat{\sigma}(x+y) &= \hat{\sigma}\left(\sum_{i=0}^{m-1} a_i\alpha^i + \sum_{i=0}^{m-1} b_i\beta^i\right) \\
&= \sum_{i=0}^{m-1} \sigma(a_i)\beta^i + \sum_{i=0}^{m-1} \sigma(b_i)\beta^i \\
&= \hat{\sigma}\left(\sum_{i=0}^{m-1} a_i\alpha^i\right) + \hat{\sigma}\left(\sum_{i=0}^{m-1} b_i\alpha^i\right) \\
&= \hat{\sigma}(x) + \hat{\sigma}(y)
\end{aligned}$$

Além disso

$$\begin{aligned}
\hat{\sigma}(xy) &= \hat{\sigma}\left[\left(\sum_{i=0}^{m-1} a_i\alpha^i\right)\left(\sum_{j=0}^{m-1} b_j\alpha^j\right)\right] \\
&= \hat{\sigma}\left[\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_ib_j\alpha^{i+j}\right] \\
&= \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} \sigma(a_ib_j)\beta^{i+j} \\
&= \left(\sum_{i=0}^{m-1} \sigma(a_i)\beta^i\right)\left(\sum_{j=0}^{m-1} \sigma(b_j)\beta^j\right) \\
&= \hat{\sigma}\left(\sum_{i=0}^{m-1} a_i\alpha^i\right)\hat{\sigma}\left(\sum_{j=0}^{m-1} b_j\alpha^j\right) \\
&= \hat{\sigma}(x)\hat{\sigma}(y)
\end{aligned}$$

Ainda resta mostrarmos que $\hat{\sigma}$ é uma bijeção. Assim, se $\hat{\sigma}(x) = \hat{\sigma}(y)$, temos então que

$$\sum_{i=0}^{m-1} \sigma(\hat{a_i})\alpha^i = \sum_{i=0}^{m-1} \sigma(\hat{b_i})\alpha^i$$

O que, neste caso, é o mesmo que afirmar que $\sigma(a_i)\beta^i = \sigma(b_i)\beta^i$, $\forall i \in \{0, 1, \cdots, m-1\}$. E, portanto, $a_i = b_i$, $\forall i \in \{0, 1, \cdots, m-1\}$, o que nos dá $x = y$ e garante a injetividade.

Para a sobrejetividade, se $x \in K'[\beta]$ é um elemento arbitrário, então $x = b_0 + b_1\beta + \cdots + b_{m-1}\beta^{m-1}$. Como σ é isomorfismo, então para cada $b_j \in K'$, existe $a_j \in K$ tal que $\sigma(a_j) = b_j$. O que nos permite escrever que

$$\begin{aligned} x &= \sigma(a_0) + \sigma(a_1)\beta + \cdots + \sigma(a_{m-1})\beta^{m-1} \\ &= \hat{\sigma}(a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}) \\ &= \hat{\sigma}(y) \end{aligned}$$

para algum $y \in K[\alpha]$, o que garante a sobrejetividade, e finalmente prova nossa afirmação sobre $\hat{\sigma}$.

Além disso, temos:

$$\begin{aligned} \hat{\sigma}(\alpha) &= \hat{\sigma}(1\alpha) \\ &= \sigma(1)\beta \\ &= \beta \end{aligned}$$

Finalmente, para verificarmos a unicidade de $\hat{\sigma}$, suponha que exista $\phi\colon\ K[\alpha] \longrightarrow K'[\beta]$ isomorfismo que satisfaça as condições provadas acima. Isto nos dá que

$$\begin{aligned} \phi(x) &= \phi(a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}) \\ &= \sigma(a_0) + \sigma(a_1)\beta + \cdots + \sigma(a_{m-1})\beta^{m-1} \\ &= \hat{\sigma}(a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}) \\ &= \hat{\sigma}(x) \end{aligned}$$

$\forall x \in K[\alpha]$, o que prova o lema.

■

Lema 2.3.2. *Sejam os corpos $K, K' \subset \mathbb{C}$, $\sigma : K \longrightarrow K'$ um isomorfismo, f um polinômio com coeficientes em K e α uma raiz qualquer de f em $\mathbb{C}$. Então, existe $\beta \in \mathbb{C}$ raiz de f^σ e existe $\sigma_1 : K[\alpha] \longrightarrow K'[\beta]$ isomorfismo tal que $\sigma_1(\alpha) = \beta$ e $\sigma_1|_K = \sigma$.*

Demonstração: Seja $f(x) = f_1(x)^{m_1} \cdots f_k(x)^{m_k}$, onde cada f_i são os distintos fatores irredutíveis de f em K. Então, $f^\sigma(x) = f_1^\sigma(x)^{m_1} \cdots f_k^\sigma(x)^{m_k}$ são os distintos fatores irredutíveis de f^σ em K'.

Agora, se α é raiz de f, então existe $i \in \{1, \cdots, k\}$ tal que α é raiz de f_i. Como σ é isomorfismo, podemos admitir β como raiz de f_i^σ irredutível sobre K'. Agora, basta aplicarmos o Lema 2.3.1 para concluirmos a demonstração desse lema.

■

Teorema 2.3.4. *Sejam os corpos $K, K' \supset \mathbb{Q}$, $\sigma : K \longrightarrow K'$ um isomorfismo, $f \in K[x]$ e $\alpha_1, \cdots, \alpha_r$ as distintas raízes de f em $\mathbb{C}$. Se $L = Gal(f, K)$ e $L' = Gal(f^\sigma, K')$, então existe $\hat{\sigma} : L \longrightarrow L'$ isomorfismo tal que $\hat{\sigma}|_K = \sigma$ e $\hat{\sigma}(\alpha_1), \cdots, \hat{\sigma}(\alpha_r)$ são as distintas raízes de f^σ em $\mathbb{C}$.*

Demonstração: Primeiro, suponha que f possua uma única raiz α, isto é, $f(x) = (x - \alpha)^m$. Então $\alpha \in K$. Assim, $f^\sigma(x) = (x - \sigma(\alpha))^m$. Logo, $\sigma(\alpha) \in K'$, $L = K$ e $L' = K'$. Isto satisfaz o teorema.

Agora, suponha que $f(x) = f_1(x)^{m_1} \cdots f_k(x)^{m_k}$, onde f_i são polinômios distintos e irredutíveis sobre K. Então, $f^\sigma(x) = f_1^\sigma(x)^{m_1} \cdots f_k^\sigma(x)^{m_k}$. Onde cada f_i^σ são polinômios distintos e irredutíveis sobre K'.

Como cada f_i é irredutível, o número r de raízes distintas de f é dado pela soma dos graus de cada f_i. Portanto, é claro que f^σ também possui r raízes. Suponha que tais raízes (também distintas) sejam $\beta_1, \cdots, \beta_r \in \mathbb{C}$.

Agora, vamos adjuntar indutivamente tais raízes ao corpo K. Isto é, vamos construir extensões do corpo K:

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

Assim, como já era esperado, temos que $L = Gal(f, K) = K[\alpha_1, \cdots, \alpha_r] = K_r$.

Pelo Lema 2.3.2, existe uma raiz $\beta \in \{\beta_1, \cdots, \beta_r\}$ de f^σ e um isomorfismo $\sigma_1 : K[\alpha_1] \longrightarrow K'[\beta_1]$ tal que $\sigma_1(\alpha_1) = \beta_1$ e $\sigma_1|_K = \sigma$.

Note que como $K \subset K_1$, podemos dizer que f tem coeficientes em K_1. Além disso, $f^{\sigma_1} = f^\sigma$, pois $\sigma_1|_K = \sigma$. Agora, suponha sem perda de generalidade que $\beta = \beta_1 = \sigma_1(\alpha_1)$. Assim, temos que $\sigma_1 : K[\alpha_1] \longrightarrow K'[\beta_1]$. Considerando agora $K_1 = K[\alpha_1]$ e $K_1' = K'[\beta_1]$ e o isomorfismo $\sigma_1 : K_1 \longrightarrow K_1'$, temos novamente pelo Lema 2.3.2 que existe raiz $\beta \in \{\beta_1, \cdots, \beta_r\}$ (considere sem perda de generalidade que $\beta = \beta_2$) de f^{σ_1}. Além disso, existe o isomorfismo $\sigma_2 : K_1[\alpha_2] \longrightarrow K_1'[\beta_2]$ tal que $\sigma_2(\alpha_2) = \beta_2$ e $\sigma_2|_{K_1} = \sigma_1$.

Veja que, como $\alpha_1 \neq \alpha_2$ e σ_2 é isomorfismo, então $\beta_1 \neq \beta_2$. Assim, $\sigma_2|_K = \sigma$, $\sigma_2(\alpha_1) = \beta_1$ e $\sigma_2(\alpha_2) = \beta_2$.

Supondo que exista $\sigma_{k-1} : K[\alpha_1, \cdots, \alpha_{k-1}] \longrightarrow K'[\beta_1, \cdots, \beta_{k-1}]$ tal que $\sigma_{k-1}(\alpha_i) = \beta_i$, $i = 1, \cdots, k-1$ e $\sigma_{k-1}|_K = \sigma$, temos por um raciocínio análogo ao anterior que f possui coeficientes em K_{k-1} e $f^{\sigma_{k-1}} = f^\sigma$. Considerando os corpos $K_{k-1} = K[\alpha_1, \cdots, \alpha_{k-1}]$ e $K_{k-1}' = K'[\beta_1, \cdots, \beta_{k-1}]$ e o isomorfismo $\sigma_{k-1} : K_{k-1} \longrightarrow K_{k-1}'$, novamente pelo Lema 2.3.2 temos que existe β_k raiz de f^σ e $\sigma_k : K_{k-1}[\alpha_k] \longrightarrow K_{k-1}'[\beta_k]$ tal que $\sigma_k|_{K_{k-1}} = \sigma_{k-1}$ e $\sigma_k(\alpha_k) = \beta_k$.

Portanto, segue-se que existe $\sigma_k : K[\alpha_1, \cdots, \alpha_k] \longrightarrow K'[\beta_1, \cdots, \beta_k]$ tal que $\sigma_k(\alpha_i) = \beta_i$, com $i = 1, \cdots, k$ e $\sigma_k|_K = \sigma$, $\forall k \in \{1, \cdots, r\}$. Por construção, como $L = K_r$, concluímos a demonstração do teorema.

■

Exemplo 2.3.3. *Considere o polinômio $f(x) = x^5 - 3x^3 + x^2 - 3$ com coeficientes em $\mathbb{Q}$. Como vimos para obtermos o corpo de decomposição de f, basta adjuntarmos as raízes em $\mathbb{Q}$. Primeiro, veja que em $\mathbb{C}$, podemos obter f como produto de fatores lineares, ou seja:*

$$f(x) = (x - \sqrt{3})(t + \sqrt{3})(t + 1)\left(t - \frac{1 + i\sqrt{3}}{2}\right)\left(t - \frac{1 - i\sqrt{3}}{2}\right)$$

Assim, obtemos que

$$Gal(f, \mathbb{Q}) = \mathbb{Q}\left[\sqrt{3}, \frac{1 + i\sqrt{3}}{2}\right]$$

Ou de forma mais simplificada: $\mathbb{Q}[\sqrt{3}, i]$.

3 Normalidade e Separabilidade

3.1 Normalidade

O conceito de normalidade de uma extensão é de extrema importância para este trabalho. Aqui e na seção de Separabilidade, os resultados e definições foram especificamente baseados na referência [2]. Assim, podemos iniciar este capítulo com a seguinte definição:

Definição 3.1.1. A extensão $L \supset K$ diz-se normal se todo polinômio f irredutível com coeficientes em K, que possui pelo menos uma raiz em L, fatora-se em L.

Exemplo 3.1.1. $\mathbb{C} \supset \mathbb{R}$ *é uma extensão normal.*

Exemplo 3.1.2. *Considere* $\alpha = \sqrt[3]{2}$ *e considere* $\mathbb{Q}[\alpha] \supset \mathbb{Q}$. *O polinômio* $f(x) = x^3 - 2$ *possui uma raiz* α *em* $\mathbb{Q}[\alpha]$, *mas não se fatora sobre* $\mathbb{Q}[\alpha]$. *De fato, as outras raízes de* f *são complexas. Portando, a extensão* $\mathbb{Q}[\alpha] \supset \mathbb{Q}$ *não é normal.*

Agora que já enunciamos a definição de extensão normal, podemos finalmente enunciar um importante corolário do Teorema 2.3.4.

Corolário 3.1.1. *Sejam* $L \supset K$ *uma extensão normal, e* M, M' *subcorpos de* L *tais que* $M, M' \supset K$. *Se* $\sigma\colon M \longrightarrow M'$ *é um isomorfismo tal que* $\sigma(x) = x$, $\forall x \in K$, *então existe isomorfismo* $\hat{\sigma} \in Aut_K L$ *tal que* $\hat{\sigma}|_M = \sigma$.

Demonstração: Seja $f(x) \in M[x]$. Como $L \supset K$ é extensão normal, então $L \supset M$ e $L \supset M'$ também são normais. Suponha que $M = M'$ e assuma, sem perda de generalidade, que $L = Gal(f, M) = Gal(f^\sigma, M')$. Note ainda que, neste caso, $f = f^\sigma$. Pelo Teorema 2.3.4 existe $\hat{\sigma}\colon L \longrightarrow L$ tal que $\hat{\sigma}|_M = \sigma$. Como por hipótese, $\sigma(x) = x$, $\forall x \in K$, segue-se que $\hat{\sigma}$ é um K-automorfismo, isto é, pertence ao grupo $Aut_K L$, como queríamos.

■

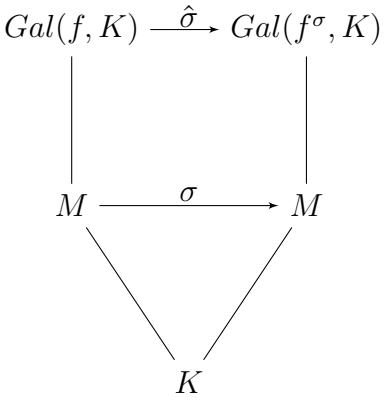

Figura 2 – Diagramas de corpos conforme Corolário 3.1.1

O próximo teorema estabelece uma equivalência muito importante para o objetivo deste capítulo.

Teorema 3.1.2. *Seja $L \supset K$ uma extensão de corpos. Esta extensão é normal e finita se, e somente se, $L = Gal(f, K)$, para algum polinômio f com coeficientes em K.*

Demonstração: Suponha que $L \supset K$ seja uma extensão normal e finita. Por ser finita, podemos admitir que $L = K[\alpha_1, \cdots, \alpha_s]$, onde α_j é algébrico sobre K, $\forall j \in \{1, \cdots, s\}$. Para cada $j \in \{1, \cdots, s\}$, tome $m_j = irr(\alpha_j, K)$, e $f = m_1 \cdots m_s$, onde cada m_j é irredutível sobre K e possui uma raiz $\alpha_j \in L$. Da normalidade de $L \supset K$, m_j se fatora sobre L, $\forall j\{1, \cdots, s\}$ e consequentemente, f também se fatora sobre L. Logo, como L é gerado por K e as raízes de f, segue-se que $L = Gal(f, K)$.

Reciprocamente, suponha que $L = Gal(g, K)$, para algum polinômio g com coeficientes em K. Neste caso, pelas observações 1 e 2 feitas após a Definição 2.3.2, é claro que $L \supset K$ é uma extensão finita. Resta mostrar que a extensão é normal.

Considere f um polinômio irredutível com coeficientes em K e com uma raiz em L Para provarmos a normalidade da extensão, basta mostrarmos que f se fatora sobre L.

Seja $M \supset L$, tal que $M = Gal(fg, K)$. Suponha que β_1 e β_2 são raízes de f em M. Como f é irredutível, então f é o polinômio mínimo de β_1 e β_2 sobre K.

Afirmamos que $[L[\beta_1] : L] = [L[\beta_2] : L]$. Para mostrarmos isso, considere os subcorpos de M: $K, L, K[\beta_1], L[\beta_1], K[\beta_2], L[\beta_2]$. É evidente que:

- $K \subset K[\beta_1] \subset L[\beta_1] \subset M$;
- $K \subset K[\beta_2] \subset L[\beta_2] \subset M$

Esquematicamente, temos:

para $i = 1, 2$.

Como tomamos $f = irr(\beta_i, K)$, $i = 1, 2$, então $[K[\beta_1] : K] = [K[\beta_2] : K]$. Pela Lei da Torre, vale:

$$[L[\beta_j] : L].[L : K] = [L[\beta_j] : K] = [L[\beta_j] : K[\beta_j]].[K[\beta_j] : K]$$

Note que $L[\beta_j] = Gal(g, K[\beta_j])$ e como β_1 e β_2 são raízes de f, temos que $K[\beta_1]$ é isomorfo a $K[\beta_2]$. Assim, o Teorema 2.3.4, garante a existência de um isomorfismo entre as extensões $L[\beta_j] \supset K[\beta_j]$, $\forall j \in \{1, 2\}$. Ou seja, $L[\beta_1] \simeq L[\beta_2]$. Consequentemente, estas extensões possuem o mesmo grau, e portanto:

$$[L[\beta_1] : K[\beta_1]] = [L[\beta_2] : K[\beta_2]]$$

Assim, temos que:

$$[L[\beta_1] : L][L : K] = [L[\beta_1] : K[\beta_1]][K[\beta_1] : K]$$

e

$$[L[\beta_2] : L][L : K] = [L[\beta_2] : K[\beta_2]][K[\beta_2] : K]$$

Ora, como

$$[L[\beta_1] : K[\beta_1]][K[\beta_1] : K] = [L[\beta_2] : K[\beta_2]][K[\beta_2] : K]$$

tome $p = [L[\beta_1] : K[\beta_1]][K[\beta_1] : K] = [L[\beta_2] : K[\beta_2]][K[\beta_2] : K]$.

Assim, segue-se que

$$[L[\beta_1] : L][L : K] = [L[\beta_2] : L][L : K] = p$$

e finalmente,

$$[L[\beta_1] : L] = [L[\beta_2] : L]$$

Agora, se $\beta_1 \in L$, então $[L[\beta_1] : L] = 1$ e assim, $[L[\beta_2] : L] = 1 \Rightarrow \beta_2 \in L$. Logo, f se fatora em L e, portanto, $L \supset K$ é normal, como queríamos demonstrar.

■

3.2 Separabilidade

Estudaremos nesta seção o conceito de separabilidade. Além disso, veremos que sobre $\mathbb{C}$, esta propriedade ocorre naturalmente.

Antes de definirmos separabilidade, é importante relembrarmos algumas definições mais básicas envolvendo polinômios.

Considere $K \subset \mathbb{Q}$. Seja f um polinômio com coeficientes em K, tal que o grau de f seja n e sejam $\alpha_1, \cdots, \alpha_r$ as distintas raízes de f em $\mathbb{C}$. Então, em $\mathbb{C}[x]$,

$$f(x) = c(x-\alpha_1)^{m_1} \cdots (x-\alpha_r)^{m_r}$$

com $c \in K$ e $r, m_1, \cdots, m_r \in \mathbb{N}$. Diz-se que m_i é a multiplicidade da raiz α_i, com $i \in \{1, \cdots, r\}$. Além disso, se $m_i = 1$, dizemos que α_i é uma raiz simples de f.

Outro conceito importante, que não será abordado em sua totalidade neste trabalho, é o conceito de derivada de um polinômio. Se $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, então a derivada de $f(x)$, a qual representaremos por $f'(x)$ é dada por

$$f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$$

É claro que $f'(x)$ também possui coeficientes em K.

Abaixo, listaremos algumas observações importantes a respeito da derivada de f, que não serão demonstradas aqui, pois seria um desvio do tema central deste trabalho.

- Se o grau de f é maior ou igual a 1, então $f'(x) \neq 0$
- Se o grau de f é n, então o grau de f' é $n-1$.
- Sendo f e g polinômios com coeficientes em K, então valem as igualdades: $(f+g)' = f' + g'$, $(af)' = af'$, $(fg)' = f'g + fg'$

Definição 3.2.1. Seja f um polinômio irredutível com coeficientes em $K \subset \mathbb{C}$. Dizemos que f é separável sobre K se possuir raízes simples em $Gal(f, K)$, ou de forma equivalente, se possuir raízes simples em $\mathbb{C}$.

A definição anterior significa que sobre $Gal(f, K)$, ou sobre $\mathbb{C}$, podemos obter f como:

$$f(x) = a(x-\alpha_1) \cdots (x-\alpha_n)$$

onde α_j são distintos $\forall j \in \{1, \cdots, n\}$.

Exemplo 3.2.1. *Note que o polinômio $f(x) = x^4 + x^3 + x^2 + x + 1$ é separável sobre $\mathbb{Q}$. Suas raizes complexas são: $e^{\frac{2\pi i}{5}}, e^{\frac{4\pi i}{5}}, e^{\frac{6\pi i}{5}}, e^{\frac{8\pi i}{5}}$.*

Lema 3.2.1. *Sejam $K \subset \mathbb{C}$, f um polinômio com coeficientes em K, tal que o grau de f seja maior ou igual a 1. Então para que $\alpha \in \mathbb{C}$ seja uma raiz simples de f é necessário e suficiente que $f'(\alpha) \neq 0$.*

Demonstração: Como α é raiz simples de f, podemos obter

$$f(x) = (x - \alpha)g(x)$$

onde g possui coeficientes também em K e $g(\alpha) \neq 0$

Assim, $f'(x) = g(x) + (x - \alpha)g'(x)$. Isto é, $f'(\alpha) = g(\alpha) \neq 0$

Reciprocamente, temos que $f(x) = (x - \alpha)^m g(x)$. Daí, $f'(x) = m(x - \alpha)^{m-1}g(x) + (x-\alpha)^m g'(x)$ e $f'(\alpha) \neq 0$. Logo, temos $m = 1$, pois, caso contrário, teríamos que $f'(\alpha) = 0$, o que contradiria a hipótese.

■

Teorema 3.2.2. *Todo polinômio irredutível com coeficientes em $K \subset \mathbb{C}$ é separável.*

Demonstração: Seja f um polinômio irredutível com coeficientes em K e α uma raiz de f com multiplicidade m.

Suponha que $p(x) = irr(\alpha, K)$. Pelo algoritmo da divisão, obtemos:

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

com $r(x) = 0$ ou $\partial r < \partial p$. Como $r(\alpha) = f(\alpha) = 0$, não podemos ter $\partial r < \partial p$. Com isso temos que, $r(x)$ é identicamente nulo e $f(x) = p(x)q(x)$. Além disso, como f é irredutível, temos que $f(x) = cp(x)$, com $c \in K$. Note ainda que, $f'(x) = cp'(x)$.

Agora, se $m > 1$, pelo Lema 3.2.1, temos $f'(\alpha) = cp'(\alpha) = 0$, ou seja, $p'(\alpha) = 0$. Mas ainda pelo Lema 3.2.1, α não é raiz simples de p, o que contradiz a minimalidade do grau de p. Logo, $m = 1$, e α é raiz simples de f, o que prova o teorema.

■

4 A correspondência de Galois

Nesta sessão, o objetivo é enunciar e demonstrar o Teorema Fundamental da Teoria de Galois para extensões $L \supset K$ finitas, tais que $\mathbb{C} \supset L$. Tal teorema é um dos principais resultados deste trabalho. Para isso, devemos estabelecer algumas definições e enunciar algumas proposições que são necessárias para o correto entendimento do teorema.

Antes de mais nada, devemos relembrar a noção de automorfismos. Todo automorfismo é um isomorfismo (homomorfismo bijetor) de uma estrutura algébrica nela mesma. Neste trabalho, consideraremos automorfismos entre corpos. Sendo $L \supset K$ uma extensão de corpos, considere o grupo de automorfismos de L que fixam K denotado por $Aut_K L = \{\sigma : L \to L | \sigma(x) = x, \forall x \in K\}$, onde a operação do grupo é a composição de funções. Este grupo será amplamente utilizado, e é conhecido como Grupo de Galois.

4.1 Extensões normais e automorfismos

Os próximo resultados estabelecem relações importantes entre extensões finitas, normais e automorfismos. Utilizaremos as notações apresentadas até aqui.

Lema 4.1.1. *Se $L \supset K$ é uma extensão finita, então $[L : K] \geq |Aut_K L|$.*

Demonstração: Suponha que $[L : K] = n$, então existe $a \in L$, tal que $L = K[a]$. Sejam $\sigma \in Aut_K L$ um K-automorfismo e $p = irr(a, K)$. Sabemos que $\alpha = \sigma(a)$ também é raiz de p e $\alpha \in L$. Além disso, como $K[\alpha] \subset L$ e $[K[\alpha] : K] = [L : K] = \partial p$, temos que

$$L = K[a] = K[\alpha].$$

Como $\sigma(x) = x, \forall x \in K$, então σ fica completamente determinado pelo valor de $\alpha = \sigma(a)$. Assim, $|Aut_K L|$ não supera o número de raízes α de p que pertencem a L, Isto é, $|Aut_K L| \leq \partial(p)$. Como $[L : K] = \partial(p)$, segue-se portanto que, $[L : K] \geq |Aut_K L|$.

■

Lema 4.1.2. *Se $L \supset K$ é uma extensão normal, então as afirmações abaixo são verdadeiras:*

1. $[L : K] = |Aut_K L|$
2. *Se $a \in L \setminus K$, então existe automorfismo $\sigma \in Aut_K L$ tal que $\sigma(a) \neq a$*

Demonstração:

1. Suponha que $L = K[a_1]$, para algum $a_1 \in L$. Se $h = irr(a_1, K)$, então pelo Teorema 3.1.2, $L = Gal(h, K)$, ou seja, L contém todas as raízes de h. Suponha que $\partial h = n$, isto é, $[L : K] = n$ e pelo Teorema 3.2.2, h possui exatamente n raízes distintas $a_1, \cdots, a_n$. Assim, pelo Lema 2.3.1, para todo $i \in \{1, ..., n\}$, existe isomorfismo $\sigma_i \colon K[a_1] \longrightarrow K[a_i]$ tal que $\sigma_i(a_1) = a_i$ e $\sigma(x) = x$, $\forall x \in K$. Por Corolário 3.1.1, existe $\hat{\sigma_i} \in Aut_K L$ tal que $\hat{\sigma_i}|_{K[a_1]} = \sigma_i$, ou seja, existem pelo menos n automorfismos $\hat{\sigma_1}, \hat{\sigma_2}, ..., \hat{\sigma_n} \in Aut_K L$. Isto mostra que $[L : K] \leq |Aut_K L|$. Logo, pelo Lema anterior, como $[L : K] \geq |Aut_K L|$, segue-se que $[L : K] = |Aut_K L|$.

2. Seja $a \in L \setminus K$, e tome $g = irr(a, K)$. Observe que $\partial(g) \geq 2$. De fato, se fosse $\partial(g) = 1$, então teríamos $g(x) = x - a$. Mas isso contradiz a hipótese, pois $a \notin K$. Pelo Teorema 3.2.2, existe $b \neq a$ tal que $g(b) = 0$. Note ainda que $b \in L$, pois pelo Teorema 3.1.2, L é o corpo de decomposição de g. Agora, pelo Lema 2.3.1, existe isomorfismo
$$\sigma \colon K[a] \longrightarrow K[b]$$
tal que $\sigma(x) = x$, $\forall x \in K$ e $\sigma(a) = b \neq a$. Além disso, pelo Corolário 3.1.1, existe $\hat{\sigma} \in Aut_K L$ tal que $\hat{\sigma}|_{K[a]} = \sigma$, como queríamos.

■

Teorema 4.1.1. *Sejam $L \supset M \supset K$ extensões finitas. Se $L \supset K$ é normal, então as afirmações abaixo são equivalentes:*

1. *$M \supset K$ é normal.*
2. *$\sigma(M) \subset M$, $\forall \sigma \in Aut_K L$*
3. *$Aut_M L \lhd Aut_K L$*

Demonstração:

(1) $\Longrightarrow$ (2): Seja $a \in L$ tal que $M = K[a]$. Se $h = irr(a, K)$ e $\sigma \in Aut_K L$, então $\sigma(a)$ também é raiz de h e pela normalidade de $M \supset K$, temos que $\sigma(a) \in M$. Logo, $\sigma(M) \subset M$.

(2) $\Longrightarrow$ (1): Sejam $a \in L$ tal que $M = K[a]$ e $h = irr(a, K)$. O objetivo aqui é mostrar que M é o corpo de decomposição de h, ou seja $M = Gal(h, K)$. É claro que $M \subset Gal(h, K)$. Para provarmos a inclusão contrária, suponha que b seja raiz de h e defina $N = K[b]$. Pelo Lema 2.3.1 existe isomorfismo $\sigma \colon M \longrightarrow N$ tal que $\sigma(a) = b$ e $\sigma(x) = x$, $\forall x \in K$. Pelo Teorema 2.3.4, existe $\hat{\sigma} \in Aut_K L$ tal que $\hat{\sigma}|_M = \sigma$. Como por hipótese $\hat{\sigma}(M) \subset M$ e $a \in M$, temos então que $\hat{\sigma}(a) = \sigma(a) = b \in M$. Portanto, $Gal(h, K) = M$ e pelo Teorema 3.1.2, $M \supset K$ é extensão normal.

(2) $\Longrightarrow$ (3): Dado $\phi \in Aut_M L$, provaremos que $\sigma^{-1} \circ \phi \circ \sigma \in Aut_M L$, para todo $\sigma \in Aut_K L$. De fato, sejam $\sigma \in Aut_K L$ e $\phi \in Aut_M L$. Fixado $p \in \sigma(M)$, existe $q \in M$ tal que $p = \sigma(q)$, uma vez que $\sigma(M) \subset M$. Assim, $\phi(p) = p$ e daí obtemos:

$$\begin{aligned}(\sigma^{-1} \circ \phi \circ \sigma)(q) &= \sigma^{-1}(\phi(\sigma(q))) \\ &= \sigma^{-1}(\phi(p)) \\ &= \sigma^{-1}(p) \\ &= q\end{aligned}$$

Portanto, $\sigma^{-1} \circ \phi \circ \sigma \in Aut_M L$, pois $q \in M$ foi fixado, e isto prova que $Aut_M L \lhd Aut_K L$.

(3) $\Longrightarrow$ (2): Suponha por absurdo que existam $\sigma \in Aut_K L$ e $a \in M$ tais que $\sigma(a) = b \notin M$. Como $L \supset K$ é extensão normal, então $L \supset M$ também é e pelo Lema 4.1.2, existe $\varphi \in Aut_M L$ tal que $\varphi(b) \neq b$. Assim, $\sigma^{-1} \circ \varphi \circ \sigma(a) = \sigma^{-1}(\varphi(b)) \neq \sigma^{-1}(b) = a$, ou seja, $\sigma^{-1} \circ \varphi \circ \sigma \notin Aut_M L$, o que é uma contradição.

■

Teorema 4.1.2. *Seja $L \supset K$ uma extensão finita. Então são equivalentes:*

1. *$L \supset K$ é normal.*
2. *$\forall a \in L \setminus K$, $\exists \varphi \in Aut_K L$ tal que $\varphi(a) \neq a$.*
3. *$[L : K] = |Aut_K L|$*

Demonstração:

(1) $\Longrightarrow$ (2): Decorre do último Lema.

(2) $\Longrightarrow$ (3): Pelo Lema 4.1.1, como $L \supset K$ é uma extensão finita, então $[L : K] \geq |Aut_K L|$. Para provar a igualdade desejada, basta provarmos que $[L : K] \leq |Aut_K L|$. Assim, suponha por absurdo que $[L : K] > |Aut_K L|$. Seja $Aut_K L = \{\sigma_1, \sigma_2, ..., \sigma_n\}$ e suponha sem perda de generalidade que $\sigma_1 = Id$, isto é, o automorfismo identidade.

Como $[L : K] > n$, então, L como K-espaço vetorial, possui uma base com mais de n elementos. Suponha que o conjunto $\beta = \{u_1, u_2, \cdots, u_n, u_{n+1}\}$ seja uma base de L.

Considere o seguinte sistema linear homogêneo com n equações e $n+1$ incógnitas:

$$\begin{cases} \sigma_1(u_1)a_1 + \cdots + \sigma_1(u_n)a_n + \sigma_1(u_{n+1})a_{n+1} = 0 \\ \quad\vdots \\ \sigma_j(u_1)a_1 + \cdots + \sigma_j(u_n)a_n + \sigma_j(u_{n+1})a_{n+1} = 0 \\ \quad\vdots \\ \sigma_n(u_1)a_1 + \cdots + \sigma_n(u_n)a_n + \sigma_n(u_{n+1})a_{n+1} = 0 \end{cases}$$

Onde as incógnitas são $a_1, \cdots, a_n, a_{n+1} \in L$. Como há mais incógnitas do que equações, então o sistema admite solução onde $a_1, \cdots, a_n, a_{n+1}$ não são todos nulos.

Considere uma solução não trivial com o maior número de zeros possíveis. Suponha sem perda de generalidade que $a_1, a_2, \cdots, a_r$, com $r < n$, são os valores não nulos que satisfazem o sistema. Assuma sem perda de generalidade que $a_1 = 1$. Assim, $1, a_2, \cdots, a_r, 0, \cdots, 0$ é uma solução para o sistema com uma quantidade máxima de zeros. Multiplicando-se as equações por a_1^{-1}, obtemos, para cada $i \in \{1, \cdots, n\}$:

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

Como σ_1 é o automorfismo identidade, e β é linearmente independentes em K, então existe $a_i \in L \setminus K$. Isto é verdade, pois caso contrário, na primeira equação, $u_1 1 + u_2 a_2 + \cdots + u_r a_r = 0$, teríamos $a_i = 0$, $\forall i \in \{1, \cdots, n\}$, isto é, uma contradição.

Suponha então que $a_r \notin K$. Por hipótese, como $a_r \in L \setminus K$, então existe $\varphi \in Aut_K L$ tal que $\varphi(a_r) \neq a_r$. Assim, para cada $i \in \{1, \cdots, n\}$, tem-se:

$$(\varphi \circ \sigma_i)(u_1) + (\varphi \circ \sigma_i)(u_2)\varphi(a_2) + \cdots + (\varphi \circ \sigma_i)(u_r)\varphi(a_r) = 0$$

Observe que $Aut_K L = \{\sigma_1, \cdots, \sigma_n\} = \{\varphi \circ \sigma_1, \cdots, \varphi \circ \sigma_n\}$. Por simplicidade de notação, considere $\varphi \circ \sigma_i = \sigma_k$. Assim, para cada $k \in \{1, \cdots, n\}$, reescrevemos a equação acima como:

$$\sigma_k(u_1) + \sigma_k(u_2)\varphi(a_2) + \cdots + \sigma_k(u_r)\varphi(a_r) = 0 \qquad (i)$$

E para cada $i \in \{1, \cdots, n\}$ tem-se:

$$\sigma_i(u_1) + \sigma_i(u_2)a_2 + \cdots + \sigma_i(u_r)a_r = 0 \qquad (ii)$$

Fazendo-se $(i) - (ii)$, e utilizando-se as propriedades de automorfismos, obtemos para cada $j \in \{1, \cdots, n\}$:

$$\sigma_j(u_2)(\varphi(a_2) - a_2) + \cdots + \sigma_j(u_r)(\varphi(a_r) - a_r) = 0$$

Como $\varphi(a_r) - a_r \neq 0$, temos uma contradição por causa da escolha feita de a_i como solução com quantidade máxima de zeros, pois σ_j é isomorfismo (homomorfismo bijetor) e o conjunto β é linearmente independente. Logo, $[L : K] \leq |Aut_K L|$, e portanto, $[L : K] = |Aut_K L|$.

(3) $\Longrightarrow$ (1): Seja $L \supset K$ uma extensão finita e $[L : K] = |Aut_K L|$. Suponha que $L = K[a]$ para algum $a \in L$ algébrico. Se h é tal que $h(x) = irr(u, K)$, então para todo $\sigma \in Aut_K L$ tem-se $\sigma(u) \in K$ e $h(\sigma(u)) = 0$. Assim, $|Aut_K L|$ é menor ou igual ao número de raízes de h em L. Mas se $[L : K] = |Aut_K L|$, então $|Aut_K L|$ coincide com o grau de h, e consequentemente, com o número de raízes de h em L. Logo, L contém todas as raízes de h, ou seja, L é o corpo de decomposição de h, e portanto $L \supset K$ é uma extensão normal.

■

4.2 Correspondência de Galois

Antes de chegarmos ao ponto principal de todo o capítulo, ainda precisamos de algumas definições e propriedades, as quais enunciaremos a seguir.

Definição 4.2.1. Seja $M \supset K$ uma extensão finita. Um corpo L diz-se intermediário de $M \supset K$ se L é um subcorpo de M contendo K. Isto é, $M \supset L \supset K$.

Seja $G = Aut_K M$ o conjunto de todos os K-automorfismos de M. Considere as seguintes notações:

- $\gamma(M, K) = \{L; M \supset L \supset K\}$ o conjunto de todos os corpos intermediários entre $M \supset K$.
- $\omega(G) = \{H; H \leq G\}$ o conjunto de todos os subgrupos de G.

Aqui, novamente estamos considerando apenas subcorpos de $\mathbb{C}$.

Proposição 4.2.1. *Considerando-se as notações acima, se $H \in \omega(G)$, então o conjunto $L = \{x \in M; \sigma(x) = x, \forall \sigma \in H\}$ é um subcorpo de M que contém K.*

Demonstração: Primeiro, veja que $0, 1 \in L$, uma vez que $L \supset \mathbb{Q}$. Fixado $\sigma \in H \leq G$, suponha que $x, y \in L$. Então temos

- $\sigma(x - y) = \sigma(x) - \sigma(y) = x - y \in L$.
- $\sigma(xy) = \sigma(x)\sigma(y) = xy \in L$.

Note ainda que, se $x \in L$, tal que $x \neq 0$, então $\sigma(x^{-1}) = (\sigma(x))^{-1} = x^{-1} \in L$. Como consideramos $G = Aut_K M$, segue-se que $M \supset L \supset K$.

■

Definição 4.2.2. O conjunto L, que conforme provamos é um corpo, chama-se Corpo Fixo de $H \leq G$.

Agora, definiremos as seguintes aplicações:

$$\begin{array}{rccc} \psi\colon & \gamma(M,K) & \longrightarrow & \omega(G) \\ & L & \longmapsto & Aut_L M \end{array}$$

$$\begin{array}{rccc} \theta\colon & \omega(G) & \longrightarrow & \gamma(M,K) \\ & H & \longmapsto & \theta(H) \end{array}$$

Onde, $\psi(L) = Aut_L M$ é o grupo de todos os L-automorfismos de M e $\theta(H) = \{x \in M; \sigma(x) = x, \forall \sigma \in H\}$ é o corpo fixo de H. Em outras palavras: cada corpo intermediário L de $M \supset K$, a aplicação ψ associa ao grupo de Galois de $L \supset K$. E cada subgrupo H de $G = Aut_K M$ é associado ao corpo fixo de H. Definidas estas correspondências, vamos listar abaixo algumas propriedades de ψ e θ que decorrem imediatamente de tudo que já foi explicitado nesta seção:

Proposição 4.2.2. *Seja $M \supset K$ uma extensão finita. Considerando-se as notações utilizadas acima, são verdadeiras as seguintes afirmações:*

1. $\psi(K) = Aut_K M = G$.
2. $\psi(M) = Aut_M M = \{I_d\}$.
3. $\theta(\{I_d\}) = \{x \in M; I_d(a) = a\} = M$.
4. $\theta(G) = \{x \in M; \sigma(x) = x, \forall \sigma \in G\} \supset K$.

Demonstração:

1. Segue-se direto das definições de K-automorfismos, Grupo de Galois e da construção de ψ. De fato, basta notar que o grupo de Galois $G = Aut_K M$ é o grupo de todos os K-automorfismos da extensão $M \supset K$.
2. Basta observar que, pelas definições dadas, o único automorfismo que fixa qualquer elemento de M é apenas o automorfismo identidade I_d. De fato, se houvesse $\sigma \in Aut_M M$ tal que $\sigma \neq id$, então existiria $x \in M \setminus M$ tal que $\sigma(x) \neq x$, o que é uma contradição, uma vez que a extensão considerada é $M \supset K$, e $M \setminus M = \emptyset$.
3. De forma análoga ao item anterior, basta notar que o corpo fixo de $\{I_d\}$ é o próprio corpo M.
4. Segue-se direto das definições dadas.

■

O próximo resultado estabelece uma interessante e ampla relação entre as inclusões de corpos intermediários L numa extensão $M \supset K$ e subgrupos do grupo de Galois $Aut_K M$.

Lema 4.2.1. *Se $M \supset K$ é uma extensão finita, então são verdadeiras as seguintes afirmações:*

1. *Se L_1, $L_2 \in \gamma(M,K)$ e $L_1 \subset L_2$ então $\psi(L_2) \leq \psi(L_1)$.*
2. *Se H_1, $H_2 \in \omega(G)$ e $H_1 \leq H_2$, então $\theta(H_2) \subset \theta(H_1)$.*
3. *Se $L \in \gamma(M,K)$ é um corpo intermediário qualquer, então $L \subset (\theta \circ \psi)(L)$.*
4. *Se $H \in \omega(G)$, tem-se $H \leq (\psi \circ \theta)(H)$.*

Demonstração: Primeiro, provemos (1): veja que é claro que $\psi(L_2) \neq \emptyset$, pois $\psi(L_2) = Aut_{L_2}M$ e $L_2 \in \gamma(M,K)$. Pela definição, temos $\psi(L_2) = Aut_{L_2}M$ e $\psi(L_1) = Aut_{L_1}M$. Observe que todos os automorfismos de $Aut_{L_2}M$ também fixam elementos de L_1, pois $L_1 \subset L_2$. Isto nos garante que $Aut_{L_2}M \subset Aut_{L_1}M$. Fixados $\sigma, \sigma^{-1} \in Aut_{L_2}M$ e $x \in L_2$ arbitrários, tem-se que: $(\sigma \circ \sigma^{-1})(x) = \sigma(\sigma^{-1}(x)) = \sigma(x) = x$. Portanto $\psi(L_2) = Aut_{L_2}M \leq Aut_{L_1}M = \psi(L_1)$. Isto prova (1).

Agora, provaremos (2), isto é, mostraremos que $\theta(H_2) \subset \theta(H_1)$. Temos que:

1. $\theta(H_1) = \{x \in M; \sigma(x) = x, \forall \sigma \in H_1\}$.
2. $\theta(H_2) = \{x \in M; \sigma(x) = x, \forall \sigma \in H_2\}$.

Se $y \in \theta(H_2)$, como $H_1 \leq H_2$, então $\sigma(y) = y$, $\forall \sigma \in H_1$. Logo, $y \in \theta(H_1)$ e portanto, $\theta(H_2) \subset \theta(H_1)$. Note ainda que a estrutura de subcorpo é preservada. Isto é, $\theta(H_2)$ é subcorpo de $\theta(H_1)$. A demonstração desta afirmação é análoga ao que foi feito na Proposição 4.2.1.

Provaremos agora (3), ou seja, que $(\theta \circ \psi)(L) \supset L$. Note que:

$$\begin{aligned} (\theta \circ \psi)(L) &= \theta(\psi(L)) \\ &= \theta(Aut_L M) \\ &= \{x \in M; \sigma(x) = x, \forall \sigma \in \psi(L)\} \\ &= \{x \in M; \sigma(x) = x, \forall \sigma \in Aut_L M\} \end{aligned}$$

Isto é, $(\theta \circ \psi)(L)$ é o corpo fixo de $Aut_L M$. Agora, se $x \in L \subset M$, então $\sigma(x) = x$, $\forall \sigma \in Aut_L M$. Logo, $x \in (\theta \circ \psi)(L)$, e portanto, $(\theta \circ \psi)(L) \supset L$. Novamente, a estrutura de subcorpo é preservada.

Finalmente, para provarmos o item (4), isto é, mostraremos que $H \leq (\psi \circ \theta)(H)$.

Observe que:

$$\begin{aligned} (\psi \circ \theta)(H) &= \psi(\theta(H)) \\ &= \psi(\{x \in M; \sigma(x) = x, \forall \sigma \in H\}) \\ &= Aut_{\theta(H)}M \end{aligned}$$

Assim, se $\sigma \in H$, então como $\sigma \in Aut_K M$, temos que $\sigma(x) = x$, $\forall x \in \theta(H)$. Logo, $\sigma \in Aut_{\theta(H)} M$. Portanto, $H \leq (\psi \circ \theta)(H)$. Observe que a estrutura de subgrupo também é preservada.

■

Lema 4.2.2. *Sejam $L \supset K$ uma extensão finita e $G = Aut_K L$ seu grupo de Galois. Então $L \supset K$ é normal se, e somente se, K é o corpo fixo de G.*

Demonstração: Suponha que $L \supset K$ seja uma extensão normal. Queremos provar aqui que $\theta(G) = K$. Observe que, pela Proposição 4.2.2, temos que $K \subset \theta(G)$, por isso, resta provar a inclusão contrária. Assim, suponha por absurdo, que $\theta(G) \not\subset K$. Então existe $a \in M \setminus K$ tal que $\forall \sigma \in G$, tenha-se $\sigma(a) = a$. Mas pelo Teorema 4.1.2, isto implica que $L \supset K$ não é extensão normal. O que é uma contradição com a hipótese.

Reciprocamente, suponha que $\theta(G) = K$. Provaremos que $L \supset \theta(G)$ é normal.

Pelo Lema 4.1.1, $[L : \theta(G)] \geq |G|$. Queremos provar que $[L : \theta(G)] = |G|$, para isso, basta mostrar que $[L : \theta(G)] \leq |G|$. Assim, suponha por absurdo que $[L : \theta(G)] > |G|$. Pelo mesmo raciocínio utilizado na demonstração do Teorema 4.1.2 em (2) $\Longrightarrow$ (3), chegamos a uma contradição. Logo, $[L : \theta(G)] = |G|$, e novamente pelo Teorema 4.1.2, $L \supset K = \theta(G)$ é extensão normal, e isto prova o que queríamos.

■

Os dois últimos resultados provados, em especial o Lema 4.2.1, possibilitam uma visão mais concreta da correspondência entre as extensões de corpos com seu grupo de Galois associado. De fato, considere a cadeia de corpos:

$$K \subset L_1 \subset L_2 \subset M$$

E a estrutura do seu grupo de Galois:

$$\{I_d\} \leq H_2 \leq H_1 \leq G = Aut_K M$$

Os diagramas abaixo mostram a reversão das inclusões. Observe que essa correspondência não necessariamente é bijetiva (conforme a Figura 3). O Teorema Fundamental da Teoria de Galois estabelece uma condição suficiente para que haja uma bijeção entre $\gamma(M, K)$ e $\omega(G)$. Isso é o que mostra a Figura 4.

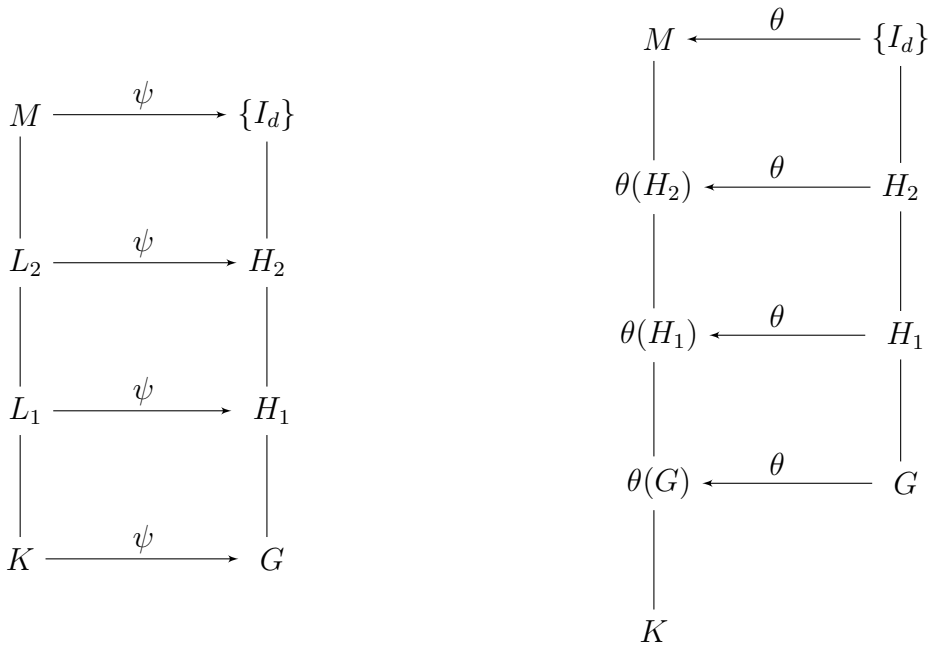

Figura 3 – Correspondências ψ e θ.

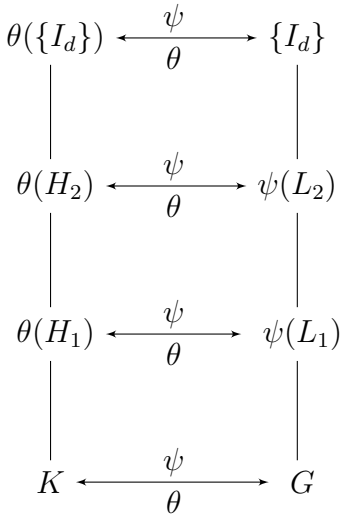

Figura 4 – Correspondência bijetiva conforme o Teorema

Os itens dos quais a Figura 4 dispõe, estão relacionados com as seguintes notações conforme a listagem abaixo. Novamente, observe que as aplicações ψ e θ são bijetivas, em que cada uma é a inversa correspondente da outra.

- $\theta(\{I_d\}) = M$.
- $\theta(H_i) = L_i$, $i \in \{1, 2\}$
- $\theta(G) = K$
- $H_i = Aut_{L_i}M$, $i \in \{1, 2\}$

- $G = Aut_K M = \psi(K)$

Teorema 4.2.3. ***(Teorema Fundamental da Teoria de Galois)****: Sejam $M \supset K$ uma extensão finita normal e $G = Aut_K M$ seu grupo de Galois. Com as notações estabelecidas anteriormente, as seguintes afirmações são verdadeiras.*

1. *Se $L \in \gamma(M, K)$, então $[M : L] = |\psi(L)|$ e $[L : K] = [G : \psi(L)]$ (o índice de $\psi(L)$ em G). Em particular, $|G| = [M : K]$.*
2. *Se $H \in \omega(G)$, então $[M : \theta(H)] = |H|$ e $[\theta(H) : K] = [G : H]$ (o índice de H em G).*
3. *As aplicações ψ e θ são inversas. Isto é, $\psi \circ \theta = I_{\omega(G)}$ e $\theta \circ \psi = I_{\gamma(M,K)}$.*
4. *Seja $L \in \gamma(M, K)$. Então $L \supset K$ é normal se, e somente se, $\psi(L) \lhd G$.*
5. *Seja $L \in \gamma(M, K)$. Se $L \supset K$ é normal, então $[L : K] = |Aut_K L|$ e $G/\psi(L) \simeq Aut_K L$.*

Demonstração:

1. Fixe $L \in \gamma(M, K)$ arbitrário. Como $M \supset K$ é normal, então $M \supset L$ também é. Assim, pelo Teorema 4.1.2, tem-se:

   $$[M : L] = |Aut_L M| = |\psi(L)|.$$

   Isso prova a primeira afirmação.

   Pela Lei da Torre, tem-se:

   $$[M : K] = [M : L][L : K]$$

   Considerando-se o que acabamos de provar, segue-se que $|G| = |\psi(L)|[L : K]$. O que nos dá:

   $$\begin{aligned} [L : K] &= \frac{|G|}{|\psi(L)|} \\ &= [G : \psi(L)] \end{aligned}.$$

   Isto prova o item (1).

2. Fixe $H \in \omega(G)$. Pelo item anterior, tem-se:

   $$[M : \theta(H)] = |\psi(\theta(H))|.$$

   Pelo Lema 4.2.1, $H \leq \psi(\theta(H))$, e por isso, $[M : \theta(H)] \geq |H|$. Precisamos provar que $[M : \theta(H)] \leq H$. Assim, considere $|H| = n$ e, suponha por absurdo, que $[M : \theta(H)] > |H| = n$.

Considerando-se M como um $\theta(H)$-espaço vetorial, existem, digamos, $n+1$ vetores linearmente independentes sobre o corpo $\theta(H)$. Com um raciocínio análogo ao usado na demonstração do Teorema 4.1.2, chega-se numa contradição. Logo, $[M : \theta(H)] \leq |H|$, e portanto, $[M : \theta(H)] = |H|$ o que prova a primeira afirmação.

Para provarmos a segunda afirmação, utilizaremos novamente a Lei da Torre. Tal resultado nos garante que $[M : K] = [M : \theta(H)][\theta(H) : K]$, onde $[M : \theta(H)] = |H|$ e $[M : K] = |G|$. Portanto,

$$\begin{aligned} [\theta(H) : K] &= \frac{|G|}{|H|} \\ &= [G : H] \end{aligned}$$

e o item (2) está provado.

3. Para provar o item (3), mostraremos que $\psi(\theta(H)) = H$, $\forall H \in \omega(G)$. Para isso, fixe $H \in \omega(G)$ arbitrário. Pela Lema 4.2.1, $H \leq \psi(\theta(H))$. Pelo item (1),

$$[\theta(H) : K] = \frac{|G|}{|\psi(\theta(H))}$$

Pelo item (2),

$$[\theta(H) : K] = \frac{|G|}{|H|}$$

Comparando-se a equação do dada pelo item (1) com a dada pelo item (2), uma simples substituição nos mostra que

$$|H| = |\psi(\theta(H))|.$$

Como, G é um grupo finito, então segue-se que $H = \psi(\theta(H))$. Da arbitrariedade de $H \in \omega(G)$, concluímos que

$$\psi \circ \theta = I_{\omega(G)}.$$

Agora, provaremos que $\theta(\psi(L)) = L$, $\forall L \in \gamma(M, K)$. Fixe $L \in \gamma(M, K)$. Pelo Lema 4.2.1, temos que $L \subset \theta(\psi(L))$, assim resta provar a inclusão contrária. Pelo item (2), tem-se que

$$[M : \theta(\psi(L))] = |\psi(L)|$$

E pelo item (1), tem-se que

$$|\psi(L)| = [M : L]$$

Isto mostra que $[M : \theta(\psi(L))] = [M : L]$ e consequentemente, $L = \theta(\psi(L))$. Portanto, da arbitrariedade de $L \in \gamma(M, K)$, segue-se que

$$\theta \circ \psi = I_{\gamma(M,K)}$$

e o item (3) está provado.

4. Este item segue imediatamente do Teorema 4.1.1, pois como $M \supset L \supset K$ são extensões finitas e $M \supset K$ é extensão normal, então é $L \supset K$ é extensão normal se, e somente se $Aut_M L \lhd Aut_K M$.

5. Seja $L \in \gamma(M, K)$, tal que $L \supset K$ seja normal. Pelo Teorema 4.1.1, o fato de $L \supset K$ ser extensão normal, implica que $\sigma(L) \subset L$, $\forall \sigma \in G$. Assim, $\forall \in G$, $\exists \hat{\sigma} = \sigma|L \in Aut_K L$. Isto nos permite definir a seguinte função:

$$\begin{array}{rccc} \Gamma\colon & G & \longrightarrow & Aut_K L \\ & \sigma & \longmapsto & \sigma|L \end{array}$$

Afirmamos que Γ é homomorfismo de grupos. De fato, para provarmos esta afirmação, tomemos $\sigma, \varphi \in G$. Temos $\forall x \in L$ que:

$$\begin{array}{rcl} (\sigma \circ \varphi)|_L(x) & = & (\sigma \circ \varphi)(x) \\ & = & \sigma(\varphi(x)) \end{array}$$

Por outro lado, temos que:

$$\begin{array}{rcl} (\sigma|_L \circ \varphi|_L)(x) & = & \sigma|_L(\varphi|_L(x)) \\ & = & \sigma|_L(\underbrace{\varphi(x)}_{\in L}) \\ & = & \sigma(\varphi(x)) \end{array}$$

O que prova que

$$\Gamma(\sigma \circ \varphi) = \Gamma(\sigma) \circ \Gamma(\varphi)$$

e assim, Γ é homomorfismo de grupos.

Além disso, tem-se que:

$$\begin{array}{rcl} Ker(\Gamma) & = & \{\sigma \in G; \hat{\sigma} = I_L\} \\ & = & Aut_L M \\ & = & \psi(L) \end{array}$$

Neste caso, o Teorema do Isomorfismo garante que:

$$\frac{G}{\psi(L)} \simeq \Gamma(G)$$

Note ainda que se $\varphi \in Aut_K L$, então por definição, $\varphi\colon \ L \longrightarrow L$, onde $\varphi(x) = x$, $\forall x \in K$. Assim, pelo Corolário 3.1.1, existe $\hat{\varphi} \in G = Aut_M K$, tal que $\hat{\varphi}|_L = \varphi$, isto é, $\Gamma(\hat{\varphi}) = \varphi$, o que prova a sobrejetividade de Γ. Logo,

$$\frac{G}{\psi(L)} \simeq Aut_K L$$

Finalmente, pelo item (1), temos que $|G|/|\psi(L)| = [L : K]$ e pelo que acabamos de provar, $|Aut_K L| = |G/\psi(L)|$. Portanto, $[L : K] = |Aut_K L|$ como queríamos e isto prova o teorema.

■

4.3 Exemplos de grupos de Galois e seus corpos fixos

Dado um polinômio $f(x) \in K[x]$, com $L = Gal(f, K)$, iremos exibir seu grupo de Galois e calcular todos os corpos fixos intermediários entre K e L. Para isso, utilizaremos fortemente o Teorema Fundamental da Teoria de Galois (Teorema 4.2.3), assim como as propriedades da correspondência de Galois, que vimos no capítulo anterior. Lembre que estamos considerando apenas extensões dos racionais. Isto é, $K \supset \mathbb{Q}$. Começaremos com dois exemplos bem simples e depois iremos para os mais elaborados.

A primeira extensão para a qual calcularemos o grupo de Galois e seus corpos fixos é $Gal(x^2 - 2, \mathbb{Q}) \supset \mathbb{Q}$. Assim, considere $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. As raízes de $f(x)$ são $\sqrt{2}$ e $-\sqrt{2}$. De fato, em $Gal(f, \mathbb{Q})$, temos:

$$\begin{aligned} f(x) &= x^2 - 2 \\ &= (x - \sqrt{2})(x + \sqrt{2}) \end{aligned}$$

Logo, $Gal(f, \mathbb{Q}) = \mathbb{Q}[\sqrt{2}]$. É claro que $\mathbb{Q}[\sqrt{2}] \supset \mathbb{Q}$ é extensão normal. Logo, pelo Teorema 4.1.2, $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = |Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt{2}]|$.

Podemos tomar $irr(\sqrt{2}, \mathbb{Q}) = f(x) = x^2 - 2$. Portanto,

$$[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = |Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt{2}]| = 2$$

Neste caso, existem apenas dois automorfismos: $Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt{2}] = \{id, \sigma\}$. E podemos concluir prontamente que $Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt{2}] \simeq (\mathbb{Z}_2, \cdot)$. Como $\sqrt{2}$ é raiz de f, então $\sigma(\sqrt{2})$ também é. E portanto, $\sigma(\sqrt{2}) = -\sqrt{2}$.

Automorfismos	Ação em $\sqrt{2}$
id	$\sqrt{2}$
σ	$-\sqrt{2}$

Tabela 1 – Ação do grupo de Galois no conjunto de raízes

O grupo de Galois de $f(x)$ tem uma estrutura muito simples, assim como a estrutura de corpos fixos. Temos o seguinte diagrama onde $G = Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt{2}]$:

$$\begin{array}{cc} \mathbb{Q}[\sqrt{2}] & \{I_d\} \\ | & | \\ \mathbb{Q} & G \end{array}$$

Figura 5 – Diagrama de grupo e corpos fixos.

Observe que as inclusões das estruturas algébricas são reversas exatamente como vimos na seção anterior.

Agora, pelo Teorema Fundamental da Teoria de Galois: $\mathbb{Q}[\sqrt{2}] \supset \mathbb{Q}$ é extensão normal, pois $\{id\} \lhd Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt{2}]$. Além disso:

- $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = |Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt{2}]| = 2$
- $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = |Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt{2}]|/|\{id\}| = 2$

O segundo exemplo de extensão que calcularemos o grupo de Galois e seus corpos fixos é $Gal(x^2+1, \mathbb{Q})$. Consideremos agora $f(x) = x^2 + 1 \in \mathbb{Q}[x]$ As raízes de f são $\pm i$. De fato, em $Gal(f, \mathbb{Q})$ podemos obter:

$$\begin{aligned} f(x) &= x^2 - 2 \\ &= (x-i)(x+i) \end{aligned}$$

Logo, $Gal(f, \mathbb{Q}) = \mathbb{Q}[i]$ e a análise deste exemplo é análoga à do exemplo anterior. Portanto, concluímos prontamente que $Aut_{\mathbb{Q}}\mathbb{Q}[i] \simeq \mathbb{Z}_2$. E temos o mesmo diagrama de grupos e corpos fixos onde $G = Aut_{\mathbb{Q}}\mathbb{Q}[i]$.

$$\begin{array}{cc} \mathbb{Q}[i] & \{I_d\} \\ | & | \\ \mathbb{Q} & G \end{array}$$

Figura 6 – Diagrama de grupo e corpos fixos.

Agora, iremos calcular o grupo de Galois e os corpos fixos da extensão $Gal(x^4-5x^2+6, \mathbb{Q}) \supset \mathbb{Q}$. Seja $f(x) = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$. Observe que $f(x)$ não é irredutível em $\mathbb{Q}$, e podemos obter: $f(x) = (x^2-2)(x^2-3)$. Assim fica evidente que as raízes de $f(x)$ são $\pm\sqrt{2}$ e $\pm\sqrt{3}$. E assim, $Gal(f, \mathbb{Q}) = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, donde $f(x) = (x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{3})(x+\sqrt{3}) \in \mathbb{Q}[\sqrt{2}, \sqrt{3}][x]$. Pelo Teorema 3.1.2, tem-se que $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \supset \mathbb{Q}$ é extensão normal. Agora, pela Lei da Torre, temos:

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

Note que $irr(\sqrt{3}, \mathbb{Q}) = x^2 - 3$. Logo, $[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = 2$. E, $irr(\sqrt{2}, \mathbb{Q}[\sqrt{3}]) = x^2 - 2$. Logo, $[\mathbb{Q}[\sqrt{3}, \sqrt{2}] : \mathbb{Q}[\sqrt{3}]] = 2$. Consequentemente,

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

Como $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \supset \mathbb{Q}$ é extensão normal, então

$$[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}] = |Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt{2}, \sqrt{3}]| = 4.$$

Isto nos garante que:

$$Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \{id, \sigma_1, \sigma_2, \sigma_3\}$$

Como $\sqrt{2}$ e $\sqrt{3}$ são raízes de f, então $\sigma_i(\sqrt{2})$ e $\sigma_i(\sqrt{3})$ também são, $\forall i \in \{1, 2, 3\}$.

Observação 4.3.1. *Ao analisarmos a ação de cada automorfismo sobre as raízes de $f(x)$, note que não é possível termos $\sqrt{2} \longmapsto \sqrt{3}$ e vice-versa. De fato, se $\sigma_i(\sqrt{2}) = \sqrt{3}$, para algum $i \in \{1, 2, 3\}$, teríamos*

$$\begin{aligned} 2 &= \sigma_i(2) \\ &= \sigma_i(\sqrt{2}\sqrt{2}) \\ &= \sqrt{3}\sqrt{3} \\ &= 3 \end{aligned}$$

o que é absurdo.

Podemos dispor os automorfismos na seguinte tabela, conforme a ação de cada um nas raízes de $f(x)$:

Automorfismos	Ação em $\sqrt{2}$	Ação em $\sqrt{3}$
id	$\sqrt{2}$	$\sqrt{3}$
σ_1	$-\sqrt{2}$	$\sqrt{3}$
σ_2	$\sqrt{2}$	$-\sqrt{3}$
σ_3	$-\sqrt{2}$	$-\sqrt{3}$

Tabela 2 – Ação do grupo de Galois no conjunto de raízes

Observe que todo elemento de $Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ possui ordem igual a 2.

1. $o(\sigma_1) = 2$, pois $\sigma_1^2(\sqrt{2}) = id(\sqrt{2})$ e $\sigma_1^2(\sqrt{3}) = id(\sqrt{3})$.
2. $o(\sigma_2) = 2$, pois $\sigma_2^2(\sqrt{2}) = id(\sqrt{2})$ e $\sigma_2^2(\sqrt{3}) = id(\sqrt{3})$.
3. $o(\sigma_2) = 2$, pois $\sigma_3^2(\sqrt{2}) = id(\sqrt{2})$ e $\sigma_3^2(\sqrt{3}) = id(\sqrt{3})$.

Como $|Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt{2}, \sqrt{3}]| = 4$, então este é abeliano, e como vimos, há apenas subgrupos de ordem 1 e 2, os quais estão enumerados logo abaixo:

1. $\langle \sigma_1 \rangle = \{id, \sigma_1\}$
2. $\langle \sigma_2 \rangle = \{id, \sigma_2\}$
3. $\langle \sigma_3 \rangle = \{id, \sigma_3\}$

Abaixo está o diagrama do grupo de Galois de $f(x)$, onde $G = Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

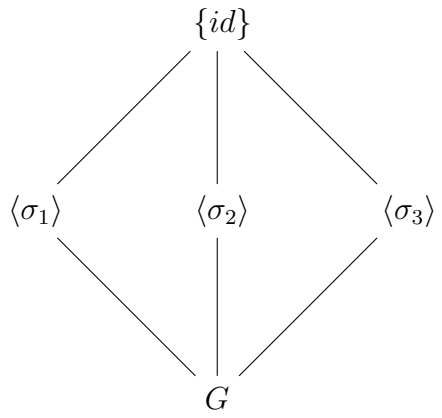

Figura 7 – Diagrama do grupo de Galois de $f(x) = x^4 - 5x^2 + 6$.

Note ainda que $Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt{2}, \sqrt{3}] \simeq \mathbb{V}_4$.

Agora iremos determinar os corpos fixos de cada subgrupo correspondente através da resolução de um sistema linear. Mas primeiro, temos que $\theta(\{id\}) = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, e como $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \supset \mathbb{Q}$ é extensão normal, tem-se:

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

Lembremos que a definição de corpo fixo é:

$$\theta(\langle\sigma_i\rangle) = \{x \in M; \sigma_i(x) = x, \forall\sigma_i \in \langle\sigma_i\rangle\}$$

$\forall i \in \{1, 2, 3\}$.

Como sabemos, podemos considerar $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ como um $\mathbb{Q}$-espaço vetorial. E como $irr(\sqrt{3}, \mathbb{Q}) = x^2 - 3$ e $irr(\sqrt{2}, \mathbb{Q}[\sqrt{3}]) = x^2 - 2$, então $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ é uma base para $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Assim, para determinar cada corpo fixo, basta utilizar a definição que já conhecemos, montar e resolver o sistema linear correspondente.

Vamos calcular agora o corpo fixo $\theta(\langle\sigma_1\rangle)$. Seja $x \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Por definição, existem $a, b, c, d \in \mathbb{Q}$ tais que

$$x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

Devemos encontrar a, b, c, d de forma que $\sigma_1(x) = x$. Agora, basta consultarmos a Tabela 2 para sabermos como cada automorfismo age nas raízes. Teremos então:

$$\sigma_1(x) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

Assim, obtemos:

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

Comparando-se termo a termo da igualdade, temos: $b = d = 0$ e $a, c \in \mathbb{Q}$ variáveis livres. Logo, $x \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ é tal que $x = a + c\sqrt{3}$. Portanto, $\theta(\langle\sigma_1\rangle) = \mathbb{Q}[\sqrt{3}]$.

Vamos calcular agora o corpo fixo $\theta(\langle\sigma_2\rangle)$. Seja $x \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Por definição existem $e, f, g, h \in \mathbb{Q}$ tais que

$$x = e + f\sqrt{2} + g\sqrt{3} + h\sqrt{6}$$

De forma análoga, devemos encontrar e, f, g, h de forma que $\sigma_2(x) = x$.

Pela Tabela 2 temos:

$$\sigma_2(x) = e + f\sqrt{2} - g\sqrt{3} - h\sqrt{6}$$

Assim, obtemos:

$$e + f\sqrt{2} + g\sqrt{3} + h\sqrt{6} = e + f\sqrt{2} - g\sqrt{3} - h\sqrt{6}$$

Comparando-se termo a termo da igualdade, concluímos que: $g = h = 0$ e $a, b \in \mathbb{Q}$ variáveis livres. Logo, $x \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ é tal que $x = a + b\sqrt{2}$. E assim, $\theta(\langle\sigma_2\rangle) = \mathbb{Q}[\sqrt{2}]$.

De forma análoga aos cálculos já feitos, obtemos que:

$$\theta(\langle\sigma_3\rangle) = \mathbb{Q}[\sqrt{6}].$$

Uma vez com todos os corpos fixos obtidos, obtemos o seguinte diagrama:

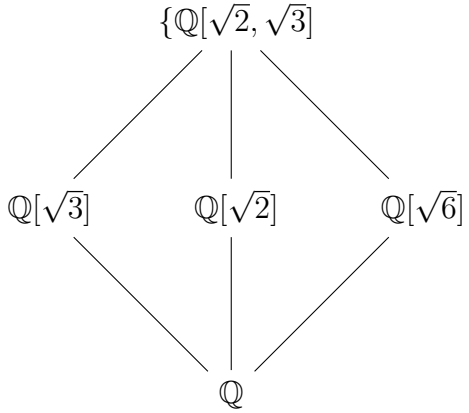

Figura 8 – Diagrama de corpos fixos.

Agora, usando o Teorema 4.2.3 (Teorema Fundamental da Teoria de Galois), concluímos:

- Todas as extensões de corpos são normais, uma vez que todos os subgrupos de $Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ são normais.
- $[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}[\sqrt{3}]] = |\psi(\langle\sigma_1\rangle)| = 2$

- $[\mathbb{Q}[\sqrt{2},\sqrt{3}]:\mathbb{Q}[\sqrt{2}]] = |\psi(\langle\sigma_2\rangle)| = 2$
- $[\mathbb{Q}[\sqrt{2},\sqrt{3}]:\mathbb{Q}[\sqrt{6}]] = |\psi(\langle\sigma_3\rangle)| = 2$
- Todas as extensões são normais, assim como os subgrupos de $Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt{2},\sqrt{3}]$.
- $[\mathbb{Q}[\sqrt{3}]:\mathbb{Q}] = \dfrac{|Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt{2},\sqrt{3}]|}{|\langle\sigma_1\rangle|} = 2.$
- $[\mathbb{Q}[\sqrt{2}]:\mathbb{Q}] = \dfrac{|Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt{2},\sqrt{3}]|}{|\langle\sigma_2\rangle|} = 2.$
- $[\mathbb{Q}[\sqrt{6}]:\mathbb{Q}] = \dfrac{|Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt{2},\sqrt{3}]|}{|\langle\sigma_3\rangle|} = 2.$

Como último exemplo, vamos considerar a extensão $Gal(x^3-2,\mathbb{Q}) \supset \mathbb{Q}$. Seja $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Suas raízes são: $\sqrt[3]{2}$, $\alpha\sqrt[3]{2}$, $\alpha^2\sqrt[3]{2}$, onde: $\alpha = -\dfrac{1}{2} + i\dfrac{\sqrt{3}}{2}$. Note que:

$$\begin{aligned} \alpha^2 &= \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)^2 \\ &= -\frac{1}{2} - i\frac{\sqrt{3}}{2} \\ &= \overline{\alpha} \end{aligned}$$

Temos que $Gal(x^3-2,\mathbb{Q}) = \mathbb{Q}[\sqrt[3]{2},\alpha]$. E pela Lei da Torre:

$$[\mathbb{Q}[\sqrt[3]{2},\alpha]:\mathbb{Q}] = \underbrace{[\mathbb{Q}[\sqrt[3]{2},\alpha]:\mathbb{Q}[\sqrt[3]{2}]]}_{x^2+x+1}\overbrace{[\mathbb{Q}[\sqrt[3]{2}]:\mathbb{Q}]}^{x^3-2}$$

Logo, $[\mathbb{Q}[\sqrt[3]{2},\alpha]:\mathbb{Q}] = 6$. Como $\mathbb{Q}[\sqrt[3]{2},\alpha] \supset \mathbb{Q}$ é extensão normal, então: $|Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt[3]{2},\alpha]| = 6$. Agora vamos obter os automorfismos de $Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt[3]{2},\alpha]$ os quais ficam bem determinados por suas ações em $\{\sqrt[3]{2},\alpha\}$:

Automorfismos	Ação em $\sqrt[3]{2}$	Ação em α
id	$\sqrt[3]{2}$	α
σ_1	$\sqrt[3]{2}$	α^2
σ_2	$\alpha\sqrt[3]{2}$	α
σ_3	$\alpha\sqrt[3]{2}$	α^2
σ_4	$\alpha^2\sqrt[3]{2}$	α
σ_5	$\alpha^2\sqrt[3]{2}$	α^2

Tabela 3 – Ação do grupo de Galois no conjunto de raízes

Como $|Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt[3]{2},\alpha]| = 6$, então são possíveis subgrupos próprios apenas de ordem 1, 2 e 3. Abaixo, calculamos a ordem o de cada um deles:

- $o(\sigma_1) = 2$, pois $\sigma_1^2(\sqrt[3]{2}) = \sqrt[3]{2}$ e $\sigma_1^2(\alpha) = \alpha$.
- $o(\sigma_2) = 3$, pois $\sigma_2^3(\sqrt[3]{2}) = \sqrt[3]{2}$ e $\sigma_2^3(\alpha) = \alpha$.
- $o(\sigma_3) = 2$, pois $\sigma_3^2(\sqrt[3]{2}) = \sqrt[3]{2}$ e $\sigma_3^2(\alpha) = \alpha$.
- $o(\sigma_5) = 2$, pois $\sigma_5^2(\sqrt[3]{2}) = \sqrt[3]{2}$ e $\sigma_5^2(\alpha) = \alpha$.

Portanto, os subgrupos são:

- $\langle\sigma_1\rangle = \{id, \sigma_1\}$.
- $\langle\sigma_2\rangle = \{id, \sigma_2, \sigma_4\} = \langle\sigma_4\rangle$.
- $\langle\sigma_3\rangle = \{id, \sigma_3\} = \langle\sigma_2\sigma_1\rangle$.
- $\langle\sigma_5\rangle = \{id, \sigma_5\} = \langle\sigma_2^2\sigma_1\rangle$.

Podemos concluir que o grupo de Galois, o qual é isomorfo ao grupo S_3, tem a seguinte estrutura:

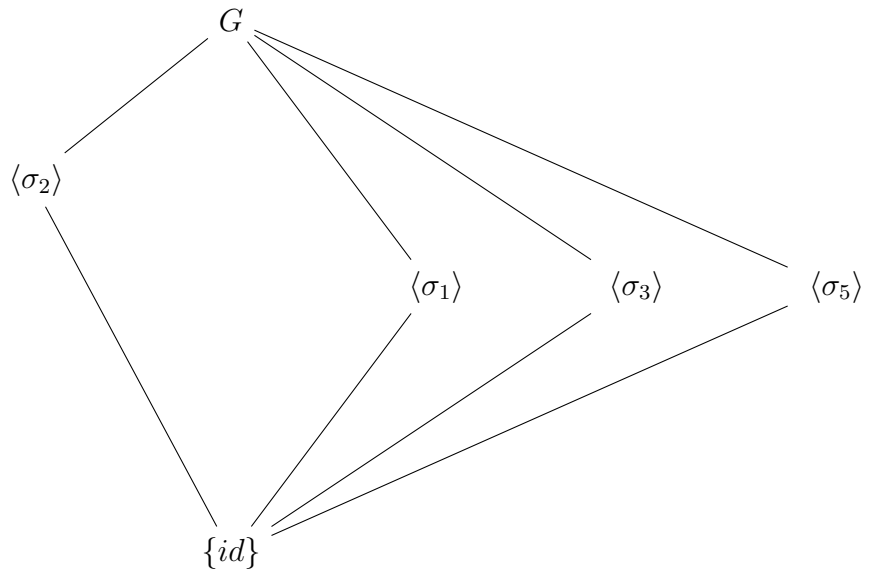

Figura 9 – Estrutura de $Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt[3]{2}, \alpha]$

Agora que já temos toda a estrutura do Grupo de Galois, iremos calcular todos os corpos fixos associados. Primeiro, notemos que: $\theta(\{id\}) = \mathbb{Q}[\sqrt[3]{2}, \alpha]$, e $\theta(Aut_{\mathbb{Q}}\mathbb{Q}[\sqrt[3]{2}, \alpha]) = \mathbb{Q}$.

Vamos agora calcular o corpo fixo $\theta(\langle\sigma_2\rangle)$. Seja $x \in \mathbb{Q}[\sqrt[3]{2}, \alpha]$. Como já vimos, existem $a, b, c, d, e, f \in \mathbb{Q}$, tais que: $x = a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\alpha + e\alpha\sqrt[3]{2} + f\alpha\sqrt[3]{4}$. Daí, basta

determinar x, tal que $\sigma_2(x) = x$ e $\sigma_4(x) = x$ com o auxílio da Tabela 3. Teremos então o seguinte sistema:

$$\begin{cases} \sigma_2(x) = x \\ \sigma_4(x) = x \end{cases}$$

E pela Tabela 3, este sistema será dado por:

$$\begin{cases} a + b\alpha\sqrt[3]{2} + c\alpha^2\sqrt[3]{4} + d\alpha + e\alpha^2\sqrt[3]{2} + f\sqrt[3]{4} = a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\alpha + e\alpha\sqrt[3]{2} + f\alpha\sqrt[3]{4} \\ a + b\alpha^2\sqrt[3]{2} + c\alpha\sqrt[3]{4} + d\alpha + e\sqrt[3]{2} + f\alpha^2\sqrt[3]{4} = a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\alpha + e\alpha\sqrt[3]{2} + f\alpha\sqrt[3]{4} \end{cases}$$

nas variáveis a, b, c, d, e e f. Uma comparação termo a termo direta já nos mostra que a e d são variáveis livres. Isto é, quaisquer $a, d \in \mathbb{Q}$ satisfazem o sistema. Além disso, analisando a primeira equação teremos que:

- $b\alpha\sqrt[3]{2} = b\sqrt[3]{2} \Longrightarrow b\underbrace{(\alpha - 1)}_{\neq 0} = 0 \Longrightarrow b = 0$
- $c\alpha^2\sqrt[3]{4} = c\sqrt[3]{4} \Longrightarrow c\underbrace{(\alpha^2 - 1)}_{\neq 0} = 0 \Longrightarrow c = 0$
- $e\alpha^2\sqrt[3]{2} = e\alpha\sqrt[3]{2} \Longrightarrow e\underbrace{(\alpha^2 - 1)}_{\neq 0} = 0 \Longrightarrow e = 0$
- $f\sqrt[3]{4} = f\alpha\sqrt[3]{4} \Longrightarrow f\underbrace{(1 - \alpha)}_{\neq 0} = 0 \Longrightarrow f = 0$

A análise termo a termo na segunda equação é análoga e a conclusão é a mesma. Logo, $b = c = e = f = 0$ e os automorfismos de $\langle\sigma_2\rangle$ fixam $a, d \in \mathbb{Q}$. Portanto, $\theta(\langle\sigma_2\rangle) = \mathbb{Q}[\alpha]$.

Agora iremos calcular o corpo fixo $\theta(\langle\sigma_1\rangle)$.

Primeiro, lembremos que a definição de corpo fixo é:

$$\theta(\langle\sigma_1\rangle) = \{x \in \mathbb{Q}[\sqrt[3]{2}, \alpha]; \sigma(x) = x, \forall\sigma \in \langle\sigma_1\rangle\}$$

Assim, tomemos $x \in \mathbb{Q}[\sqrt[3]{2}, \alpha]$. Isto implica que $x = a + b\sqrt[3]{2} + c\sqrt[4]{3} + d\alpha + e\alpha\sqrt[3]{2} + f\alpha\sqrt[3]{4}$ para algum $a, b, c, d, e, f \in \mathbb{Q}$. Como, $\langle\sigma_1\rangle = \{id, \sigma_1\}$, basta determinarmos os coeficientes de forma que $\sigma_1(x) = x$. Consultando-se a Tabela 3, obtemos $\sigma_1(x) = a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\alpha^2 + e\alpha^2\sqrt[3]{2} + f\alpha^2\sqrt[3]{4}$. E obtemos a seguinte equação:

$$a + b\alpha\sqrt[3]{2} + c\sqrt[3]{4} + d\alpha^2 + e\alpha^2\sqrt[3]{2} + f\alpha^2\sqrt[3]{4} = a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\alpha + e\alpha\sqrt[3]{2} + f\alpha\sqrt[3]{4}$$

Comprando-se termo a termo da igualdade, concluímos rapidamente que as variáveis livres são $a, b, c \in \mathbb{Q}$. E além disso:

- $d\alpha^2 - d\alpha = 0 \Longrightarrow d_\alpha\underbrace{(\alpha - 1)}_{\neq 0} = 0 \Longrightarrow d = 0.$

- $e\underbrace{(\alpha-1)}_{\neq 0} = 0 \Longrightarrow e = 0.$
- $f\underbrace{(\alpha-1)}_{\neq 0} = 0 \Longrightarrow f = 0.$

Portanto, podemos concluir que $\theta(\langle\sigma_1\rangle) = \mathbb{Q}[\sqrt[3]{2}]$.

O processo para determinarmos os demais corpos fixos é idêntico ao que fizemos anteriormente. Assim, por comodidade, os passos não serão exibidos novamente. O corpo fixo associado a $\langle\sigma_3\rangle$ é $\mathbb{Q}[\alpha^2\sqrt[3]{2}]$.

Finalmente, corpo fixo $\theta(\langle\sigma_5\rangle)$ associado a $\langle\sigma_5\rangle$ é $\theta(\langle\sigma_5\rangle) = \mathbb{Q}[\alpha\sqrt[3]{2}]$.

E portanto, o diagrama correspondente com todos os corpos fixos determinados, tem o seguinte aspecto:

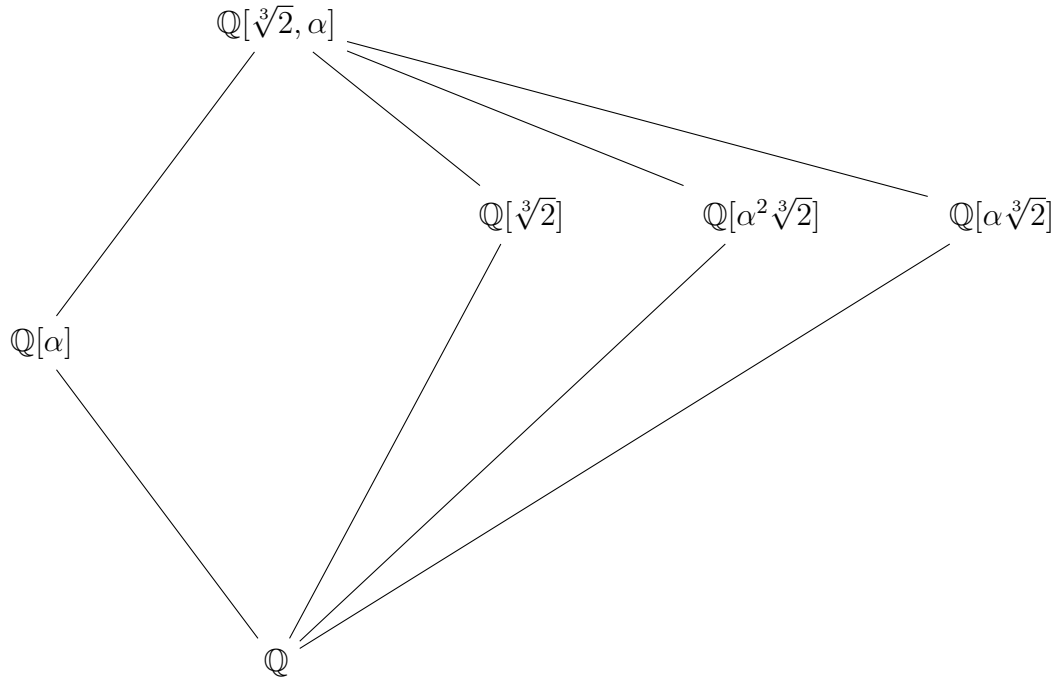

Figura 10 – Estrutura de corpos fixos.

5 Solubilidade e Simplicidade de Grupos

O foco deste capítulo é sobre a teoria de Grupos. Aqui serão enunciados e demonstrados alguns resultados importantes para o estudo da não resolubilidade de equações algébricas de grau maior ou igual a 5. Tais resultados estão intimamente ligados a solubilidade de polinômios por radicais, conforme veremos no decorrer deste trabalho.

Será abordado primeiro o conceito de solubilidade de grupos, assim como os principais resultados e definições. Depois será abordado o conceito de simplicidade de grupos. E finalmente, tudo será relacionado no teorema principal deste capítulo, assim como em seu corolário. Nossa atenção aqui será voltada, em especial, para o grupo das permutações de n elementos, o qual, conforme sabemos, é denotado por S_n, com $n = 1, 2, ..., n$, e o nosso objetivo principal aqui é mostrar a não solubilidade do grupo das permutações S_n para $n \geq 5$. Finalmente, mostraremos algumas definições e resultados importantes que estendem o conceito de grupos solúveis, os quais são de extrema importância para a demonstração do resultado principal deste trabalho.

5.1 Grupos Solúveis

Definição 5.1.1. Um grupo G diz-se solúvel se admitir uma cadeia finita de subgrupos: $id = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_n = G$, tal que:

- $G_i \lhd G_{i+1}$, $\forall i \in \{0, 1, \cdots, n-1\}$
- G_{i+1}/G_i é abeliano $\forall i \in \{0, 1, \cdots, n-1\}$

Tal cadeia é chamada de cadeia de solubilidade de G. Além disso, note que a definição acima não implica que $G_i \lhd G$, assim como $G_i \lhd G_{i+1} \lhd G_{i+2}$ não implica que $G_i \lhd G_{i+2}$.

A seguir, serão enunciados alguns exemplos.

Exemplo 5.1.1. *Todo grupo abeliano G é solúvel com a cadeia $id \lhd G$.*

De fato, se G é abeliano, então para todo subgrupo H, tal que $H \neq G$, tem-se que $H \lhd G$. Além disso, se G é abeliano, então $G/\{id\}$ também é grupo abeliano.

Exemplo 5.1.2. *O grupo S_3 é solúvel.*

De fato, como $S_3 = \{(1), (12), (13), (23), (123), (132)\}$, basta considerarmos a cadeia

$$G_0 \leq G_1 \leq G_2$$

onde $G_0 = \{(1)\}$, $G_1 = \langle(123)\rangle$ e $G_2 = S_3$.

Note que $[G_2 : G_1] = |G_2|/|G_1| = 2$. Logo, $G_1 \lhd G_2$ e o grupo quociente G_2/G_1 é abeliano, uma vez que tem ordem prima. Além disso, G_1 tem ordem 3 e portanto é abeliano e $G_0 \lhd G_1$. Logo, G_1/G_0 é abeliano e portanto, S_3 é solúvel.

Exemplo 5.1.3. *O grupo S_4 é solúvel.*

Basta tomar a cadeia

$$G_0 \leq G_1 \leq G_2 \leq G_3$$

onde $G_0 = \{(1)\}$, $G_1 = \{(1), (12)(34), (13)(24), (14)(23)\}$ é o grupo de *Klein*, denotado por $\mathbb{V}$, $G_2 = A_4$, ou seja, o grupo das permutações pares e $G_3 = S_4$.

Temos:

$$G_0 \lhd G_1 \lhd G_2 \lhd G_3$$

Além disso:

- $\mathbb{V}/\{(1)\} \simeq \mathbb{V}$ é abeliano.
- $A_2/\mathbb{V} \simeq \mathbb{Z}_3$ é abeliano de ordem 3.
- $S_4/A_4 \simeq \mathbb{Z}_2$ é abeliano de ordem 2

Portanto, S_4 é solúvel.

Exemplo 5.1.4. *O grupo S_n, onde $n \geq 5$ não é solúvel.*

Ainda precisamos de algumas definições e resultados para mostrarmos a não solubilidade do grupo S_5. Mais adiante neste capítulo estaremos a par de todo o conhecimento necessário para mostrar isso. Além disso, a não solubilidade de S_5 é um fator fundamental para o estudo da não resolubilidade de equações algébricas de grau 5, mais ainda, a não resolubilidade de equações de grau maior ou igual a 5.

O teorema a seguir estabelece um resultado importante para este capítulo.

Teorema 5.1.2. *Seja G um grupo. Se H é um subgrupo qualquer de G e N é um subgrupo normal de G, então valem as seguintes afirmações:*

1. *Se G é solúvel, então H é solúvel.*
2. *Se G é solúvel, então G/N é solúvel.*
3. *Se N e G/N são solúveis, então G é solúvel.*

Demonstração: Provaremos primeiro o item (1): Seja G um grupo solúvel e suponha que

$$\{id\} = G_0 \leq G_1 \leq \cdots \leq G_{n-1} \leq G_n = G$$

seja uma cadeia de solubilidade de G, onde $G_i \lhd G_{i-1}$ e G_i/G_{i-1} é abeliano, $\forall i \in \{1, \cdots, n\}$.

Seja $H \leq G$ um subgrupo qualquer e defina, para cada $i \in \{0, 1, \cdots\}$, $H_i = H \cap G_i$. Assim, por construção, segue-se que:

$$H_0 = \{id\} \leq H_1 \leq \cdots \leq H_{n-1} \leq H_n = H \cap G = H$$

Provaremos primeiro que $H_{i-1} \lhd H_i$, para cada i. De fato, fixado $i \in \{1, \cdots, 0\}$, tome $x \in H_{i-1} = G_{i-1} \cap H$ e $g \in H_i = G_i \cap H$ arbitrários e fixados. Temos então que: $x \in G_{i-1}$ e $x \in H$, $g \in G_i$ e $g \in H$. Assim, $g^{-1}xg \in H$ e como $G_{i-1} \lhd G_i$, temos que $g^{-1}xg \in G_{i-1}$, ou seja, $g^{-1}xg \in H_{i-1} = G_{i-1} \cap H$. Isso prova que $H_{i-1} \lhd H_i$.

Resta provarmos agora que H_i/H_{i-1} é abeliano. Para isso, para cada i defina a função:

$$\begin{array}{rccc} \psi_i\colon & H_i & \longrightarrow & G_i/G_{i-1} \\ & x & \longmapsto & x \cdot G_{i-1} \end{array}$$

Afirmamos que ψ_i é um homomorfismo de grupos. De fato, dados $x, y \in H_i$, e pela normalidade de H_{i-1} em H_i, segue-se que:

$$\begin{array}{rcl} \psi_i(xy) & = & xy \cdot G_{i-1} \\ & = & x \cdot G_{i-1}y \cdot G_{i-1} \\ & = & \psi_i(x)\psi_i(y) \end{array}$$

Afirmamos também que $Ker(\psi_i) = H_{i-1}$. Ora, por definição:

$$Ker(\psi_i) = \{x \in H_i; \psi_i(x) = G_{i-1}\}$$

Para mostrarmos que $Ker(\psi_i) \subset H_{i-1}$, tomemos $x \in Ker(\psi_i)$, o que nos garante $\psi_i(x) = G_{i-1}$, isto é, $x \in G_{i-1}$, e consequentemente, $x \in G_i$. Além disso, como $x \in H_i$, tem-se também que $x \in H$. Logo, $x \in H_{i-1} = H \cap G_{i-1}$. Para mostrarmos a inclusão contrária, isto é, que $H_{i-1} \subset Ker(\psi_i)$, tomemos $x \in H_{i-1}$. Consequentemente, $x \in H$ e $x \in G_{i-1}$. Logo, $\psi_i(x) = G_{i-1}$, e portanto, $x \in Ker(\psi_i)$. Isto prova nossa segunda afirmação de que $Ker(\psi_i) = H_{i-1}$.

Agora, pelo teorema dos Isomorfismos, segue-se que

$$H_i/H_{i-1} \simeq \psi_i(H_i) \leq G_i/G_{i-1}.$$

Isso demonstra o primeiro item, uma vez que G_i/G_{i-1} é um grupo abeliano.

Provaremos agora o item (2): Para isso, considere $N \lhd G$, e

$$\begin{array}{rccc} \pi\colon & G & \longrightarrow & G/N \\ & x & \longmapsto & N \cdot x \end{array}$$

a projeção canônica, a qual é claramente um homomorfismo sobrejetor.

Suponha que G seja solúvel. Provaremos que G/N é solúvel. Para isso, considere a cadeia de solubilidade de G, dada por:

$$\{id\} = G_0 \leq G_1 \leq \cdots \leq G_{i-1} \leq G_i \leq \cdots \leq G_{n-1} \leq G_n = G$$

Note que, se $G_i/N = \pi(G_i) = \{\overline{g_i} = \pi(g_i); g_i \in G_i\}$, então:

$$\{\overline{id}\} = G_0/N \leq G_1/N \leq \cdots \leq G_{i-1}/N \leq G_i/N \leq \cdots \leq G_{n-1}/N \leq G_n/N = G/N$$

Devemos mostrar que:

$$G_{i-1}/N \lhd G_i/N$$

e que:

$$\frac{G_i/N}{G_{i-1}/N}$$

é abeliano, $\forall i \in \{1, \cdots, n\}$.

Fixado $i \in \{1, \ldots n\}$, se considerarmos a restrição $\pi_i = \pi|_{G_i}$, então pelo Teorema da Correspondência, temos que $\pi(G_{i-1}) = G_{i-1}/N \lhd G_i/N$, pois $G_{i-1} \lhd G_i$. E isso prova a normalidade da cadeia que exibimos acima.

Para provarmos que cada grupo quociente é abeliano, considere:

$$x, y \in \frac{G_i/N}{G_{i-1}/N} = \frac{\pi(G_i)}{\pi(G_{i-1})}$$

Assim, temos que:

- Existe $\pi(g_i) \in \pi(G_i)$, tal que $x = \pi(G_{i-1})\pi(g_i)$
- Existe $\pi(h_i) \in \pi(G_i)$, tal que $y = \pi(G_{i-1})\pi(h_i)$

Como G_i/G_{i-1} é abeliano, então:

$$(G_{i-1}g_i)(G_{i-1}h_i) = (G_{i-1}h_i)(G_{i-1}g_i)$$

ou seja:

$$G_{i-1}g_ih_i = G_{i-1}h_ig_i$$

Daí, existe $u_{i-1} \in G_{i-1}$ tal que $g_i h_i = (h_i g_i)u_{i-1}$. Basta notar agora que

$$\begin{aligned} xy &= \pi(G_{i-1})\pi(g_i)\pi(h_i) \\ &= \pi(G_{i-1})\pi(g_i h_i) \\ &= \pi(G_{i-1})\pi((h_i g_i)u_{i-1}) \\ &= \pi(G_{i-1})\pi(h_i g_i)\pi(u_{i-1}) \end{aligned}$$

Mas como $\pi(u_{i-1}) \in \pi(G_{i-1})$, segue-se finalmente que

$$xy = \pi(G_{i-1})\pi(h_i)\pi(g_i) = yx$$

o que prova que $\dfrac{G_i/N}{G_{i-1}/N}$ é abeliano, como queríamos.

Finalmente, provaremos o item (3): Suponha que G/N e N sejam grupos solúveis. Provaremos que G é solúvel. Primeiro, consideremos novamente a projeção canônica definida conforme abaixo:

$$\begin{aligned} \pi\colon\ G &\longrightarrow G/N \\ x &\longmapsto N \cdot x \end{aligned}$$

Por hipótese, existem duas cadeias de subgrupos normais a saber:

1. $id = N_0 \lhd N_1 \lhd \cdots N_r = N$
2. $N/N = G_0/N \lhd G_1/N \lhd \cdots G_s/N = G/N$

Em cada cadeia acima, cada subgrupo quocientado pelo seu "antecessor"é um grupo abeliano. Considerando-se a projeção canônica, pelo Teorema da Correspondência, temos que $G_{i-1} \lhd G_i$, $\forall i \in \{1, \cdots, n\}$. A partir disto, obtemos a seguinte cadeia:

$$id = N_0 \lhd N_1 \lhd \cdots N_r = N = G_0 \lhd G_1 \lhd \cdots \lhd G_s = G$$

Temos por hipótese que N_{i-1}/N_i é um grupo abeliano. Além disso, pelo corolário do Teorema dos Isomorfismos, temos também que

$$G_i/G_{i-1} \simeq \frac{G_i/N}{G_{i-1}/N}$$

Consequentemente,

$$id = N_0 \lhd N_1 \lhd \cdots N_r = N = G_0 \lhd G_1 \lhd \cdots \lhd G_s = G$$

é uma cadeia de solubilidade para G, e portanto, G é solúvel, como queríamos.

■

5.2 Grupos Simples

Agora iremos abordar o importante conceito de grupo simples.

Definição 5.2.1. Um grupo G diz-se simples se é não trivial e se seus únicos subgrupos normais são $\{id\}$ e G.

Observação 5.2.1. *Todo grupo cíclico $\mathbb{Z}_p$ (p primo) é simples, pois não possui subgrupos além de $\{id\}$ e $\mathbb{Z}_p$. Consequentemente, estes são os únicos subgrupos normais. Além disso, estes são os únicos grupos simples que são solúveis.*

O teorema abaixo estabelece uma condição necessária e suficiente para que um grupo solúvel seja simples, o que explica porque a observação feita acima é verdadeira.

Teorema 5.2.2. *Um grupo solúvel é simples se, e somente se, for cíclico de ordem prima.*

Demonstração: Seja G um grupo solúvel. Então G possui a cadeia

$$\{id\} = G_0 \lhd G_1 \lhd ... \lhd G_n = G$$

onde G_{i+1}/G_i abeliano $\forall i \in \{0, 1, ..., n-1\}$. Assumiremos que $G_{i+1} \neq G_i$. Daí, podemos afirmar que $G_{n-1} \lhd G$. Mas G é simples, então $G_{n-1} = \{id\}$ e $G \simeq G_n/G_{n-1}$ que é abeliano (G solúvel). Como todo subgrupo de um grupo abeliano é um subgrupo normal e todo elemento de G gera um subgrupo cíclico, G deverá ser cíclico sem subgrupos não triviais. Consequentemente, G tem ordem prima.

Reciprocamente, suponha que G seja cíclico de ordem prima. Isto implica que G é abeliano. Além disso, seus únicos subgrupos são $\{id\}$ e G, e como sabemos, $\{id\} \lhd G$. Logo, como G é abeliano, segue-se que $G/\{id\}$ é abeliano, e portanto, G é solúvel e simples.

■

5.3 A simplicidade do grupo A_n, e a não solubilidade de S_n para $n \geq 5$

Para mostrarmos a não solubilidade do grupo S_n para $n \geq 5$, iremos enunciar um lema, que será fundamental para concluir tal resultado. E logo adiante, o teorema principal, seguido de seu corolário.

Lema 5.3.1. *Se $n \geq 3$, então todo elemento de A_n é um produto de 3-ciclos.*

Demonstração: Primeiro, note que para provar o lema, é suficiente considerarmos elementos de A_n da forma $(kl)(ij)$. De fato, se $\{k, l\} \cap \{i, j\} = \emptyset$, os ciclos comutam. Logo, teremos

que $(kl)(ij) = (kl)(ki)(ik)(ij) = (kil)(ijk)$. Além disso, se $k = i$, e $l \neq j$, teremos $\{k, l\} \cap \{i, j\} \neq \emptyset$. Logo, $(kl)(kj) = (kjl)$, como queríamos.

■

Teorema 5.3.1. *Se $n \geq 5$, então o grupo das permutações pares A_n é simples.*

Demonstração: Suponha que exista $N \lhd A_n$, tal que $id \neq N$. Vamos mostrar que $N = A_n$. Dividiremos a demonstração em casos. Primeiro, suponha que N contenha um 3-ciclo. E suponha sem perda de generalidade que $(123) \in N$. Logo, para qualquer $k \geq 3$, o ciclo $(32k) = (3k)(32)$ é uma permutação par e consequentemente, $(32k) \in A_n$. Além disso, como $N \lhd A_n$, temos que $(32k)(123)(32k)^{-1} = (32k)(123)(k23) = (1k2) \in N$. E ainda $(1k2)^2 = (1k2)(1k2) = (12k) \in N$, $\forall k \geq 3$.

Afirmamos que: N é gerado por todos os 3-ciclos da forma $(12k)$. De fato, se $n = 3$, então $N = A_3 = \{(123), (132), (1)\} = \langle(123)\rangle$, pois $(123)(123) = (132)$ e $(123)(123)(123) = (1)$. Agora, se $n > 3$, então para quaisquer $a, b > 2$, a permutação $(1a)(2b)$ é par e logo, pertence a A_n, o que implica que A_n contém

$$\begin{aligned}(1a)(2b)(12k)((1a)(2b))^{-1} &= (1a)(2b)(12k)(b2)(a1)\\ &= (abk)\end{aligned}$$

onde $k \neq a$ e $k \neq b$. Agora, como $(12k) = (1k2)^{-1} \in N$, $(1a)(2a) \in A_n$, e $N \lhd A_n$, temos que $(1a)(2b)(12k)((1a)(2b))^{-1} = (1a)(2b)(12k)(b2)(a1) = (abk) \in N$, se $k \neq a$, b e a, $b > 2$. Pelo Lema 5.3.1, como A_n é gerado por todos os 3-ciclos, concluímos que $N = A_n$.

Agora, resta mostrar que N contém pelo menos um 3-ciclo. Para isso, considere $\sigma \in N$, tal que $\sigma \neq 1$. Podemos decompor

$$\sigma = \pi_1\pi_2 \cdots \pi_k$$

onde π_j são ciclos disjuntos $\forall j \in \{1, \cdots, k\}$ e nenhum deles é 1-ciclo. Logo, todos os π_j comutam. Agora, analisaremos os possíveis casos.

1. Suponha que existe algum π_i que tem comprimento $c \geq 4$. Podemos então escrever $\pi_1 = (12 \cdots r)$ onde $r \geq 4$. Seja $\varphi = (123)$. Como $\sigma \in N$, $\varphi \in A_n$ e $N \lhd A_n$, temos que:

$$\begin{aligned}\varphi\sigma\varphi^{-1} &= \varphi\pi_1\pi_2 \cdots \pi_k\varphi^{-1}\\ &= \varphi\pi_1\varphi^{-1}\pi_2 \cdots \pi_k\end{aligned}$$

pois ciclos disjuntos comutam. Basta notar agora que $\pi_1^{-1}\sigma = \pi_2 \cdots \pi_k$. Então, substituindo na igualdade acima, obtemos:

$$\varphi\sigma\varphi^{-1} = \varphi\pi_1\varphi^{-1}\pi_1^{-1}\sigma.$$

Daí segue-se que:

$$\varphi\sigma\varphi^{-1} = (123)(123\cdots r)(321)(r\cdots 21)\sigma = (124)\sigma.$$

Portanto,

$$(124)\sigma = \varphi\sigma\varphi^{-1} \Rightarrow (124) = \varphi\sigma\varphi^{-1}\sigma^{-1} \in N.$$

Logo, basta aplicar o que provamos anteriormente.

2. Suponha que todo π_i tem comprimento $c \leq 3$ e no mínimo dois tem comprimento $c = 3$. Neste caso, considere sem perda de generalidade, que $\pi_1 = (123)$ e $\pi_2 = (456)$. Seja $\varphi = (124)$. Então:

$$\varphi\sigma\varphi^{-1} = \varphi\pi_1\pi_2\cdots\pi_k\varphi^{-1} = \varphi\pi_1\pi_2\varphi^{-1}\pi_3\cdots\pi_k.$$

Com um raciocínio análogo ao feito no caso anterior, temos que $\pi_3\cdots\pi_k = \pi_2^{-1}\pi_1^{-1}\sigma$.Assim,

$$\varphi\sigma\varphi^{-1} = \varphi\pi_1\pi_2\varphi^{-1}\pi_2^{-1}\pi_1^{-1}\sigma.$$

Ou seja,

$$\varphi\sigma\varphi^{-1} = (124)(123)(456)(421)(654)(321)\sigma = (12534)\sigma.$$

Portanto, $\varphi\sigma\varphi^{-1} = (12534)\sigma$. Logo,

$$\varphi\sigma\varphi^{-1}\sigma^{-1} = (12534) \in N.$$

Daí, pelo caso anterior, podemos encontrar um 3-ciclo a partir deste 5-ciclo.

3. Suponha que exatamente um π_i tem comprimento 3 e os outros têm comprimento $c \leq 2$. Neste caso, sem perda de generalidade, suponha que $\pi_1(123)$ e que todo π_i sejam $2 - ciclos$. Daí, usando o fato de que os ciclos comutam, obtemos que $\sigma^2 = \pi_1^2 \in N$, ou seja, $(123) \in N$, como queríamos.

4. Suponha que todo π_i seja um $2 - ciclo$. Note que este caso ocorre exclusivamente em $n = 4$. De fato, o grupo de Klein, dado por $\mathbb{V} = \{(1), (12)(34), (13)(24), (14)(32)\}$ conforme sabemos é normal em A_4. Agora, admitindo-se $n \geq 5$, suponha sem perda de generalidade que $x = (12)(34)p \in N$, tal que p fixa 1, 2, 3 e 4. Seja $t = (234)$. Daí, pela normalidade de N e fazendo uma substituição análoga a que foi feita nos casos anteriores, obtemos:

$$(txt^{-1})x^{-1} = (14)(23).$$

Considere ainda $u = (145) \in A_n$. Daí, temos que N contém $u(txt^{-1}x^{-1})u^{-1} = (23)(45)$. Isto é, N contém $(23)(45)(14)(23) = (145)$. Mas isso contradiz a hipótese inicial de que $\sigma = \pi_1\pi_2\ldots\pi_k$ são ciclos disjuntos. Basta notar que em todos os casos anteriores mostramos a existência de um $3 - ciclo$ em N a partir de produtos de ciclos disjuntos, diferentemente deste caso.

Portanto, o grupo A_n para $n \geq 5$ é simples, como queríamos.

■

Corolário 5.3.1. *O grupo S_n, com $n \geq 5$ não é solúvel.*

Demonstração: De fato, se S_n fosse solúvel, então A_n também seria. Pelo teorema anterior A_n é um subgrupo simples de S_n. E pelo Teorema 5.2.2, A_n teria ordem prima. Mas isso é uma contradição, pois para $n \geq 5$, o número $\frac{n!}{2}$ não é primo. Portanto, S_n não é solúvel.

■

5.4 Subgrupos maximais, cadeias subnormais e cadeias de composição

Agora, nesta última de seção deste capítulo, iremos enunciar e demonstrar certos conceitos e resultados que serão usados fortemente na demonstração do resultado principal deste trabalho.

Definição 5.4.1. Seja G um grupo não trivial, e consideremos a família de subgrupos normais próprios em G, denotada por $N(G) = \{H; H \lhd G, H \neq G\}$. Dizemos que H é um subgrupo normal maximal de G, se H é um elemento maximal em $N(G)$. Isto é, quando existir um subgrupo I normal em G, tal que $H \subset I$, então ou $I = H$ ou $I = G$.

Observação 5.4.1. *Note que quando $G = \{id\}$, então $N(G) = \emptyset$.*

Logo abaixo, provaremos que é possível estabelecer uma relação entre grupos simples e subgrupos normais maximais.

Proposição 5.4.1. *Sejam G um grupo e $H \lhd G$, tal que $H \neq G$. Os seguintes itens são equivalentes:*

1. *$H \lhd G$ é maximal.*
2. *Sendo $H \lhd G$ maximal, então os únicos subgrupos normais intermediários entre H e G são eles mesmos. Isto é, $\{I; H \lhd I \lhd G\} = \{H, G\}$*
3. *G/H é um grupo simples.*

Demonstração: (1) $\Longrightarrow$ (2): Esta implicação é imediada pela Definição 5.4.1.

(2) $\Longrightarrow$ (3): Suponha que os únicos subgrupos normais em G, diferentes de $\{id\}$ são H e G, onde $H \neq G$. Isto implica diretamente que o $G/H \neq \{eH\}$. Vamos mostrar

que G/H é um grupo simples, para isso, suponha por absurdo que G/H não é simples. Isto é, existe subgrupo $K/H \lhd G/H$, com $H \subset K \lhd G$. Mas isto implica que H não é maximal em G, o que é uma contradição, portanto G/H é simples.

(3) $\Longrightarrow$ (1): Suponha por absurdo que H não é maximal em G. Então existe $K \lhd G$ tal que $H \subset K \lhd G$. Mas sendo $H \lhd G$, então por uma consequência do Teorema dos Isomorfismos, temos que $\frac{K}{H} \lhd \frac{G}{H}$, o que implica que G/H não é um grupo simples, pois K/H é um subgrupo próprio normal de G/H, o que é uma contradição.

■

Corolário 5.4.1. *Suponha que G seja um grupo, então G é simples se, e somente se, $\{id\}$ é um subgrupo normal maximal em G.*

Demonstração: Sendo G um grupo simples, então pela Proposição 5.4.1, o subgrupo normal $\{id\}$ é maximal em G. Reciprocamente, se $\{id\}$ é maximal em G, então novamente pela Proposição 5.4.1 $G/\{id\}$ é simples. Mas como $G/\{id\} \simeq G$, então G é simples, como queríamos.

■

Note que na Definição 5.4.1 não nos preocupamos em estabelecer se tal subgrupo normal maximal de G sempre existirá, ou não. O próximo teorema garante que este subgrupo sempre existirá, sob determinadas condições. Entretanto, na demonstração deste teorema, usaremos fortemente o famoso Lema de Zorn, cuja demonstração iremos omitir, pois ela envolve conceitos que fogem do objetivo deste trabalho.

Lema 5.4.1 (Lema de Zorn)**.** *Seja X um conjunto não vazio, parcialmente ordenado, tal que cada cadeia em X é limitada superiormente. Então X possui pelo menos um elemento maximal.*

Teorema 5.4.2. *Seja G um grupo finito tal que $G \neq \{e\}$. Então G possui um subgrupo normal maximal.*

Demonstração: Vamos considerar a mesma notação estabelecida na Definição 5.4.1, isto é, o conjunto $N(G) = \{H; H \lhd G, H \neq G\}$. Primeiro, observe que $N(G) \neq \emptyset$, pois $\{id\} \in N(G)$. Seja $\mathcal{H} \subset N(G)$ uma cadeia não vazia de subgrupos. Aqui estamos considerando que $N(G)$ é parcialmente ordenado pela inclusão. A ideia é mostrarmos que existe uma cota superior (ou elemento maximal) em $N(G)$ para a cadeia $\mathcal{H}$. Note que:

$$\mathcal{H} \subset N(G) \subset \mathcal{P}(G)$$

onde $\mathcal{P}$ é o conjunto das partes de G. Como G é finito, então $\mathcal{P}(G)$ é finito. Logo, $\mathcal{H}$ é finito.

Iremos denotar como $t = |\mathcal{H}|$ e $\mathcal{H} = \{H_1, \cdots, H_t\}$. Isto é, garantimos que $\mathcal{H}$ é finito e totalmente ordenado. E todo conjunto com estas propriedades possui um máximo no próprio conjunto. Isto é, existe $s \in \{1, \cdots, t\}$ tal que $H_i \subset H_s$, $\forall i \in \{1, \cdots, t\}$. Logo, $H_s \in N(G)$ é uma cota superior de $\mathcal{H}$. Pelo Lema de Zorn, $N(G)$ admite um elemento maximal, o que prova o que queríamos.

■

Teorema 5.4.3. *Seja G um grupo tal que $G \neq \{e\}$. São equivalentes:*

1. *G é simples e abeliano.*
2. *$\{e\}$ e G são os únicos subgrupos de G.*
3. *G é cíclico de ordem prima.*

Demonstração: (1) $\Longrightarrow$ (2): Como G é abeliano, então todo subgrupo é normal em G. E sendo G um grupo simples, então seus únicos subgrupos normais são $\{e\}$ e G. Portanto, segue que $\{e\}$ e G s]ao os únicos subgrupos de G.

(2) $\Longrightarrow$ (3): Primeiro, provaremos que G é cíclico. Por hipótese, $G \neq \{e\}$, então existe $x \in G$ tal que $x \neq e$. Logo, $\{e\} \subset \langle x \rangle$, com $\{e\} \neq \langle x \rangle$. Logo, nos resta que $\langle x \rangle = G$. Portanto G é cíclico.

Agora, provaremos que G tem ordem prima, mas antes, vamos mostrar que $|G|$ é um número finito. De fato, se $|G|$ não é finito, então $G \simeq \mathbb{Z}$, uma vez que $\mathbb{Z}$ é o único grupo cíclico infinito a menos de isomorfismo. Defina,

$$\begin{array}{rccc} \phi\colon & \mathbb{Z} & \longrightarrow & G \\ & t & \longmapsto & x^t \end{array}$$

Esta função é um isomorfismo de grupos. De fato, $\phi(s+t) = x^{(s+t)} = x^s x^t = \phi(s)\phi(t)$. Além disso, se $t \in Ker(\phi)$ é tal que $x^t = e$, então $t = 0$, uma vez que estamos supondo que G é infinito. Logo, $Ker(\phi) = \{0\}$. Além disso, a sobrejetividade de ϕ é óbvia. Assim, ϕ de fato é um isomorfismo de grupos.

Mas sabemos que $\{0\} \leq 2\mathbb{Z} \leq \mathbb{Z}$, e daí, como ϕ é isomorfismo, então

$$\{e\} \leq \phi(2\mathbb{Z}) \leq G$$

com $\phi(2\mathbb{Z})$ um subgrupo próprio de G, o que contradiz a hipótese. Logo, $|G|$ é um finito.

Agora, resta mostrar que $|G|$ é um número primo. Suponha por absurdo que $p = |G|$ não seja primo, então existe $d \in \mathbb{N}$ com $1 < d < p$ tal que d divide p. Neste caso, temos que $\langle x^{p/d} \rangle$ é um subgrupo de G de ordem d. Logo, $|\langle x^{p/d} \rangle| < |G|$, o que implica que $\langle x^{p/d} \rangle$

é um subgrupo próprio de G, o que contradiz a hipótese novamente. Portanto, G tem ordem prima.

(3) $\Longrightarrow$ (1): Como G é cíclico, então G é abeliano. E o fato de G ser simples decorre imediatamente do Teorema 5.2.2.

■

Definição 5.4.4. Seja G um grupo. Uma série subnormal de G é:

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_m = G$$

onde $G_0, G_1, \cdots, G_m$ são subgrupos de G com $G_i \lhd G_{i+1}$, $\forall i \in \{0, \cdots, m-1\}$.

Definição 5.4.5. Dizemos que $\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_m = G$ é uma série de composição, se $\dfrac{G_{i+1}}{G_i}$ for um grupo simples, $\forall i \in \{0, \cdots, m-1\}$.

Observação 5.4.2. *É interessante notarmos que, de forma prática, entre dois subgrupos intermediários de G, não existe nenhum outro subgrupo. Isto é, uma série de composição é um refinamento de uma série subnormal.*

Lema 5.4.2. *Seja $f\colon G \longrightarrow H$ um homomorfismo sobrejetor de grupos. Se G é abeliano, então H também é.*

Demonstração: Sejam $h_1, h_2 \in H$. Como f é sobrejetivo, então existem $g_1, g_2 \in G$ tal que $h_i = f(g_i)$, $\forall i \in \{1, 2\}$. Logo,

$$\begin{aligned} h_1 h_2 &= f(g_1) f(g_2) \\ &= f(g_1 g_2) \\ &= f(g_2 g_1) \\ &= f(g_2) f(g_1) \\ &= h_2 h_1 \end{aligned}$$

Portanto, H é abeliano.

■

Teorema 5.4.6. *Seja G um grupo finito tal que $G \neq \{e\}$. Então G admite uma série de composição. Além disso, se G é solúvel, então G admite uma série de composição cujos quocientes são cíclicos de ordem prima.*

Demonstração: Vamos provar este resultado usando indução sobre $n = |G|$. Primeiro, como $G \neq \{e\}$, então $|G| \geq 2$. Assim, provaremos primeiro que o resultado vale para $n = 2$. De fato, se $|G| = n = 2$, então G é claramente cíclico de ordem prima, e além

disso, podemos obter: $\{e\} = G_0 \lhd G_1 = G$, que é uma série de composição de G, onde $G_1/G_0 \simeq G$ é cíclico de ordem prima 2. Isto prova o caso trivial.

Agora, suponha que $|G| > 2$ e que ambos os resultados são válidos para todo grupo finito com ordem menor do que $|G|$. Como G é grupo finito, então pelo Teorema 5.4.2 existe $G_m \lhd G$ maximal de G. Em particular, $|G_m| < |G|$ e pela hipótese de indução, G_m admite uma série de composição $G_1 = \{e\} \lhd \cdots \lhd G_{m-1} \lhd G_m$, com $\dfrac{G_i}{G_{i+1}}$ simples $\forall i \in \{1, \cdots, m-1\}$. Como G_m é subgrupo normal maximal de G, então pela Proposição 5.4.1 $\dfrac{G}{G_m}$ é um grupo simples. Logo,

$$\{id\} = G_1 \lhd \cdots \lhd G_{m-1} \lhd G_m \lhd G$$

é uma série de composição de G, o que prova a primeira afirmação.

Agora provaremos a segunda afirmação em que G é um grupo solúvel por hipótese. Assim, exite a cadeia

$$\{id\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n \lhd G$$

com $\dfrac{G_{i+1}}{G_i}$ abeliano $\forall i \in \{0, \cdots, m-1\}$. Observe que G/G_n é finito e $G/G_n \neq \{eG_n\}$. Assim, pelo Teorema 5.4.2, isto implica que existe um subgrupo $\overline{H_n} \lhd G/G_n$ normal maximal. Consideremos o homomorfismo sobrejetivo de grupos definido por:

$$\begin{array}{rccc} \pi_n\colon & G & \longrightarrow & G/G_n \\ & x & \longmapsto & xG_n \end{array}$$

Sabemos que $\pi_n^{-1}(\overline{H_n}) = H_n \lhd G$, onde $G_n \subset H_n$.

Afirmamos que H_n é um subgrupo normal maximal de G. De fato, se existe subgrupo J de G tal que $J \lhd G$ com $H_n \subset J \subset G$, temos que $G_n \subset H_n \subset J \subset G$. Aplicando-se π_n nessa cadeia e usando o fato de que π_n é sobrejetivo, obtemos:

$$\{eG_n\} \subset \overline{H_n} \subset \pi_n(J) \subset G/G_n$$

Mas lembre-se de que $\overline{H_n}$ é maximal em G/G_n e $\pi_n(J) \lhd G/G_n$. Logo, $\overline{H_n} = \pi_n(J)$ ou $\pi_n(L) = G/G_n$. Isto implica que $J = H_n$ ou $L = G$, o que prova a afirmação. Logo, pela Proposição 5.4.1, G/H_n é um grupo simples.

Sendo $G_n \subset H_n$, defina:

$$\begin{array}{rccc} \sigma\colon & G/G_n & \longrightarrow & G/H_n \\ & xG_n & \longmapsto & xH_n \end{array}$$

Observe que σ está bem definida, pois se xG_n, $yG_n \in G/G_n$ são tais que $xG_n = yG_n$, então $\sigma(xG_n) = xH_n$ e $\sigma(yG_n) = yH_n$, mas como $G_n \subset H_n$, segue-se que $xH_n = yH_n$.

Note que σ é homomorfismo de grupos. De fato, dados quaisquer xG_n, $yG_n \in G/G_n$ temos que $\sigma(xG_nyG_n) = \sigma(xyG_n) = xyH_n = xH_nyH_n = \sigma(xG_n)\sigma(yH_n)$. Além disso, σ é claramente sobrejetiva.

Como G/G_n é um grupo abeliano, então pelo Lema 5.4.2, G/H_n também é. Ora, já mostramos também que G/H_n é simples. Assim, pelo Teorema 5.4.3, G/H é cíclico de ordem prima. Além disso, H_n é solúvel, pois é subgrupo de um grupo solúvel (G), e $|H_n| < |G|$. Agora, basta usarmos a hipótese de indução em H_n para concluirmos o resultado. Isto é, H_n admite uma série de composição:

$$\{e\} = H_0 \lhd H_1 \lhd H_1 \lhd \cdots \lhd H_n$$

com H_{i+1}/H_i cíclico de ordem prima, $\forall i \in \{0, \cdots, n\}$. Agora, basta acrescentarmos G nesta série para obtermos o resultado desejado:

$$\{e\} = H_0 \lhd H_1 \lhd H_1 \lhd \cdots \lhd H_n \lhd G$$

que é uma série de decomposição com H_{i+1}/H_i cíclico de ordem prima, $\forall i \in \{0, \cdots, n-1\}$.

■

6 Solubilidade de polinômios por Radicais

Considere K um corpo tal que $\mathbb{Q} \subset K \subset \mathbb{C}$. Neste capítulo, temos o objetivo de estudar uma aplicação direta e muito importante do Teorema Fundamental da Teoria de Galois. Esta aplicação é fundamental para o estudo da não resolubilidade das equações algébricas de grau $n \geq 5$.

Definiremos o que significa um polinômio ser ou não ser resolúvel por radicais e operações algébricas como soma, multiplicação, subtração e divisão. Para isso, introduziremos um novo tipo de extensões de corpos, denominada Extensão Radical.

Finalmente, relacionaremos a propriedade de solubilidade do grupo de Galois de um polinômio com o fato deste ser ou não ser resolúvel por radicais. Isto é, utilizaremos o Teorema Fundamental da Teoria de Galois para estabelecer uma condição suficiente para solubilidade do grupo de Galois do referido polinômio. As definições e exemplos foram retirados da referência [1], e os resultados deste capítulo foram baseados na referência [4].

6.1 Extensões Radicais

Definição 6.1.1. Uma extensão $M \supset K$ finita é uma extensão radical sobre K se existem $a_1, a_2, \cdots, a_r \in M$ tais que as seguintes condições sejam satisfeitas:

1. $K = K_0 \subset K_1 = K[a_1] \subset K_2 = K_1[a_2] \subset \cdots \subset K_i = K_{i-1}[a_i] \subset \cdots \subset K_r = M$
2. Para cada $i \in \{1, 2, \cdots, r\}$ existe $n_i \in \mathbb{N}$ tal que $a_i^{n_i} \in K_{i-1}$

Devemos observar que a definição acima pode ser reformulada. De fato, considerando-se as notações que estamos utilizando, note que, podemos escrever:

$$a_i^{n_i} = b_{i-1} \in K_{i-1}$$

A partir disso, poderíamos reescrever a construção da cadeia de corpos como

$$K_i = K_{i-1}[\sqrt[n_i]{b_{i-1}}]$$

O que significa que K_i é obtido adjuntando-se uma raiz do polinômio $x^{n_i} - b_{i-1} \in K_{i-1}[x]$ ao corpo K_{i-1}.

Para ilustrar melhor o conceito de extensões radicais, considere os exemplos abaixo:

Exemplo 6.1.1. *Suponha que a seja uma raiz de $f \in \mathbb{Q}[x]$ tal que a possa ser obtida por meio dos seguintes radicais:*

$$a = \frac{\sqrt[5]{2 - \sqrt[3]{2}} + \sqrt{2}}{\sqrt[7]{1 - \sqrt[4]{5}}}$$

Podemos denotar separadamente $a_1 = \sqrt[4]{5}$, $a_2 = \sqrt[7]{1-a_1}$, $a_3 = \sqrt[3]{2}$, $a_4 = \sqrt[5]{2-a_3}$, $a_5 = \sqrt{2}$.

Note que, estamos usando o processo de adjunção de raízes para obtermos a seguinte cadeia de corpos:

$$\mathbb{Q} = K_0 \subset K_0[a_1] = K_1 \subset K_1[a_2] = K_2 \subset K_2[a_3] = K_3 \subset K_3[a_4] = K_4 \subset K_4[a_5] = K_5$$

Portanto:

$$K_5 = \mathbb{Q}[a_1, a_2, a_3, a_4, a_5]$$

Do exemplo anterior, note que:

1. $a_1^4 = (\sqrt[4]{5})^4 = 5 \in K_0$;
2. $a_2^7 = (\sqrt[7]{1-\sqrt[4]{5}})^7 = 1 - \sqrt[4]{5} \in K_1$;
3. $a_3^3 = (\sqrt[3]{2})^3 = 2 \in K_2$;
4. $a_4^5 = (\sqrt[5]{2-\sqrt[3]{2}})^5 = 2 - \sqrt[3]{2} \in K_3$;
5. $a_5^2 = (\sqrt{3})^2 = 5 \in K_4$;
6. E finalmente, $a \in K_5$.

Exemplo 6.1.2. *Considere* $f(x) = x^2 - 2 \in \mathbb{Q}$. *A extensão* $\mathbb{Q}[\sqrt{2}] \supset \mathbb{Q}$ *é radical. De fato,* $\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ *e* $(\sqrt{2})^2 = 2 \in \mathbb{Q}$.

Exemplo 6.1.3. *Seja* $p(x) = x^6 - 6x^3 + 7 \in \mathbb{Q}$. *Uma de suas raízes é o número real* $a = \sqrt[3]{3+\sqrt{2}}$. *Logo, pelo processo de adjunção de raízes, podemos obter uma extensão de* $\mathbb{Q}$ *contendo a da seguinte forma: basta tomarmos* $a_1 = \sqrt{2}$ *e* $a_2 = \sqrt[3]{3+a_1}$. *Assim, a cadeia de corpos será dada por*

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}\left[\sqrt{2}, \sqrt[3]{3+\sqrt{2}}\right]$$

Assim, obtivemos uma extensão radical. De fato, $a_2^3 = 3 + \sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ *e* $a_1^2 = (\sqrt{2})^2 = 2 \in \mathbb{Q}$.

Note ainda que, podemos generalizar os exemplos anteriores. De fato, considere $f \in K[x]$ e suponha que α seja raiz de f, tal que $\alpha \in M = K[a_1, \cdots, a_r]$ e M seja uma extensão radical. A partir do raciocínio desenvolvido anteriormente, podemos escrever α como uma expressão polinomial p que depende de $a_1, \cdots, a_r$ com coeficientes em K. Isto é,

$$\alpha = p(a_1, \cdots, a_r)$$

Observe que $a_1 = \sqrt[n_1]{b_0}$, $a_2 = \sqrt[n_2]{b_1}, \cdots, a_r = \sqrt[n_r]{b_{r-1}}$, com $b_j \in K_j$, $\forall j \in \{0, 1, \cdots, r-1\}$. Podemos então reescrever:

$$\alpha = p(\sqrt[n_1]{b_0}, \sqrt[n_2]{b_1}, \cdots, \sqrt[n_r]{b_{r-1}})$$

que é uma expressão polinomial radical. Note que, de forma geral temos:

1. $a_1 = \sqrt[n_1]{b_0}$
2. $a_2 = \sqrt[n_2]{q_1(\sqrt[n_1]{b_0})}$
3. $a_3 = \sqrt[n_3]{q_2(\sqrt[n_2]{q_1(\sqrt[n_1]{b_0})})}$
4. $a_r = \sqrt[n_r]{q_{r-1}(\sqrt[n_{r-1}]{\cdots \sqrt[n_2]{(q_1 \sqrt[n_1]{b_0})}})}$

Onde $q_1, q_2, \cdots q_r$ são polinômios em K, e dessa forma, a raiz α pode ser obtida como uma expressão radical que envolve polinômios e raízes de $b_0 \in K$.

Pelo que vimos até aqui, é intuitivo pensar que um polinômio ser solúvel por radicais, significa que é possível obter uma extensão radical de $\mathbb{Q}$ que contenha todas as raízes do polinômio. Isto nos permite enunciar a próxima definição.

Definição 6.1.2. Seja $f(x) \in K[x]$ e L seu corpo de decomposição ($L = Gal(f, K)$). Diz-se que $f(x)$ é um polinômio solúvel por meio de radicais sobre K se existe uma extensão radical $M \supset K$ tal que $M \supset L \supset K$.

Observação 6.1.1. *É importante notar que:*

1. *Não é necessário que a extensão $Gal(f, K) \supset K$ seja radical. Isto é, se $M \supset K$ é extensão radical e L é um corpo intermediário, então não necessariamente $L \supset K$ será extensão radical. Veremos um exemplo disso um pouco mais adiante.*
2. *Se $f(x) \in K[x]$ é irredutível e tem uma raiz expressa por radicais então todas as outras também serão.*

Os próximos lemas são de extrema importância para o objetivo deste capítulo.

Lema 6.1.1. *Seja $M \supset K$ uma extensão radical. Então existe uma extensão radical e normal $N \supset K$ tal que $M \subset N$.*

Demonstração: Por hipótese, $M \supset K$ é extensão radical. Então, existe a cadeia radical:

$$K = K_0 \subset K_1 \subset \cdots \subset K_s = M$$

onde $\forall j \in I = \{1, \cdots, s\}$, $\exists \alpha_j \in K_j, n_j \in \mathbb{N}$ tal que $\alpha_j^{n_j} \in K_{j-1}$ e $K_j = K_{j-1}[\alpha_j]$. Defina

$$N = Gal\left(\prod_{j \in I} p_j(x), K\right)$$

onde $p_j(x) = irr(\alpha_j, K)$.

Primeiro vamos mostrar que $N \supset K$ é extensão radical. Mostraremos para o caso em que $s = 2$ e a demonstração segue por indução sobre s.

Suponha que $M \supset K$ seja radical, com $M = K[\beta, \gamma]$, onde $\beta^n \in K$ e $\gamma^m \in K[\beta]$. Assim temos a seguinte cadeia:

$$K \subset K[\beta] \subset K[\beta, \gamma] = M$$

Sejam $p(x) = irr(\beta, K)$ e $q(x) = irr(\gamma, K)$ e suponha que $\beta = \beta_1, \cdots, \beta_r$ e $\gamma = \gamma_1, \cdots, \gamma_k$ sejam as raízes de $p(x)$ e $q(x)$ respectivamente.

Mostraremos que $N \supset K$ é extensão radical, onde

$$N = K[\beta_1, \cdots, \beta_r, \gamma_1, \cdots, \gamma_k] = Gal(p(x)q(x), K)$$

Observe que a cadeia radical é $K \subset K[\beta_1] \subset \cdots \subset K[\beta_1, \cdots, \beta_r] = L$ completada com $L \subset K[\gamma_1] \subset \cdots \subset L[\gamma_1, \cdots, \gamma_k] = N$. A partir disto, fica evidente que:

1. $M \subset N$.
2. $L = Gal(p(x), K)$.
3. $L[\gamma_1, \cdots \gamma_r] = Gal(q(x), L)$.
4. $N \supset K$ é extensão normal.

Finalmente, observe que para cada $j \in \{1, \cdots, r\}$, existe K-automorfismo $\tau\colon N \longrightarrow N$ tal que $\tau(\beta) = \beta_j$. Mas $\beta^n = a \in K$. Logo:

$$\begin{aligned} \beta_j^n &= \tau(\beta)^n \\ &= \tau(\beta^n) \\ &= \tau(a) \\ &= a \end{aligned}$$

onde $a \in K \subset K[\beta_1, \cdots, \beta_{j-1}]$, $\forall j \geq 2$.

Além disso, pelo Corolário 3.1.1, para cada $j \in \{1, \cdots, k\}$, existe K-automorfismo $\sigma\colon N \longrightarrow N$ tal que $\sigma(\gamma) = \gamma_j$ e $\sigma|_L$ é um K-automorfismo de L, uma vez que

$L \supset K$ é normal. Devemos lembrar que $\gamma^m = f(\beta) \in K[\beta]$, para algum $f(x) \in K[x]$. Então $\sigma(\beta) \in L$ e

$$\begin{aligned} \gamma_j^m &= \sigma(\gamma)^m \\ &= \sigma(\gamma^m) \\ &= \sigma(f(\beta)) \\ &= f(\sigma(\beta)) \end{aligned}$$

onde $f(\sigma(\beta)) \in L \subset L[\gamma_1, \cdots, \gamma_{j-1}]$, $\forall j \geq 2$, como queríamos. O resultado segue indutivamente para todo $s \geq 2$.

■

Lema 6.1.2. *Seja K um corpo tal que K contém uma raiz primitiva n-ésima da unidade. Sejam $a \in K \setminus \{0\}$, $f(x) = x^n - a \in K[x]$ e $L = Gal(f, K)$. Então são verdadeiras as afirmações:*

1. *$L = K[b]$, onde b é qualquer raiz de f.*
2. *$Aut_K L$ é um grupo abeliano.*

Demonstração: Primeiro, provaremos (1). Suponha que ω seja uma raiz primitiva n-ésima da unidade. Então, $1, \omega \cdots, \omega^{n-1}$ são as n raízes da unidade. Tomemos $b^n = a$. Assim, $b\omega^j$ são as n raízes de $x^n - a$, com $b \in \{0, \cdots, n-1\}$. Isto é:

$$x^n - a = (x - b)(x - b\omega)(x - b\omega^2) \cdots (x - b\omega^{n-1})$$

Como $\omega \in K$, então $1, \omega, \ldots, \omega^{n-1} \in K$. Portanto, $L = K[b] = Gal(f, K)$ e isto prova (1).

Resta provar (2), isto é, que $Aut_K L$ é um grupo abeliano. Para isso, sejam $\sigma, \tau \in Aut_K L$. Temos que $\sigma(b) = b\omega^i$ e $\tau(b) = b\omega^j$, com $i, j \in \{0, \cdots, n-1\}$.Assim,

$$\begin{aligned} (\sigma \circ \tau)(b) &= \sigma(\tau(b)) \\ &= \sigma(b\omega^j) \\ &= \omega^j \sigma(b) \\ &= \omega^j \omega^i b \\ &= \omega^{j+i} b \end{aligned}$$

Por outro lado,

$$\begin{aligned} (\tau \circ \sigma)(b) &= \tau(\sigma(b)) \\ &= \tau(b\omega^i) \\ &= \omega^i \tau(b) \\ &= \omega^i \omega^j b \\ &= \omega^{i+j} b \end{aligned}$$

Logo, $(\sigma \circ \tau)(b) = (\tau \circ \sigma)(b)$. E como $L = K[b]$, então

$$\sigma \circ \tau = \tau \circ \sigma$$

como queríamos.

■

Teorema 6.1.3. *Sejam $K \supset \mathbb{Q}$, $f(x) \in K[x]$ e L seu corpo de decomposição ($L = Gal(f, K)$). Se f é solúvel por meio de radicais sobre K, então o grupo de Galois $G = Aut_K L$ é solúvel.*

Demonstração: Seja $f(x) \in K[x]$ solúvel por radicais. Pela definição que temos:

- Existe $N \supset K$ tal que:

$$K_1 = K \subset K_2 \subset \cdots \subset K_s = N$$

- Para cada $j \in \{2, \cdots, s\}$, existem $\alpha_j \in K_j$, $n_j \in \mathbb{N}$, tais que $K_j = K_{j-1}[\alpha_j]$.
- $L = Gal(f, K) \subset N$.

Pelo Lema 6.1.1, podemos admitir $N \supset K$ normal.

Sejam $n = mmc(n_2, \cdots, n_s)$ e ω uma raiz primitiva n-ésima da unidade. A partir disso, consideremos $K_{s+1} = K_s[\omega]$. Construiremos uma cadeia auxiliar de corpos para termos controle sobre seu grupo de Galois. Para isso, definimos: $L_0 = K_1 = K$, $L_1 = K[\omega]$ e $L_j = L_{j-1}[\alpha_j]$ para cada $j \geq 2$. Note que $\omega^{\frac{n}{n_j}} \in L_{j-1}$ é uma raiz primitiva n_j-ésima da unidade. Por indução, temos $L_j = K_j[\omega]$. De modo que, $L_s = K_s[\omega] = K_{s+1} = N[\omega]$. Com esse raciocínio indutivo, obtemos o seguinte diagrama:

Para cada $j \in \{2, \cdots, s\}$ tem-se $L_j = L_{j-1}[\alpha_j]$ e $L_j = Gal(x^{n_j} - \alpha_j^{n_j}, L_{j-1})$, pois L_{j-1} possui raiz n_j-ésima da unidade. Logo, $L_j \supset L_{j-1}$ é extensão normal. Observe ainda que pelo Lema 6.1.2 , $Aut_{L_{j-1}} L_j$ é abeliano para $j = 2, \cdots, s$. Além disso,$L_1 \supset L_0$ é normal, pois $Aut_{L_0} L_1 = Aut_K K[\omega]$ é abeliano. De fato, cada $\sigma \in Aut_K K[\omega]$ está bem determinada por $\sigma(\omega)$, onde $\sigma(\omega)$ é uma raiz primitiva n-ésima da unidade. Portanto, existe único $i \in \{1, \cdots, n-1\}$, com $mdc(i, n) = 1$, tal que $\sigma(\omega) = \omega^i$.

Defina:

$$\begin{array}{rccc} \varphi\colon & Aut_K K[\omega] & \longrightarrow & \mathbb{Z}_n^* \\ & \sigma & \longmapsto & \overline{i} \end{array}$$

Pelo Lema 6.1.1, existe $M \supset L \supset K$ tal que M seja extensão radical sobre K e $M = Gal(f, K)$ para algum $f(x) \in K[x]$.

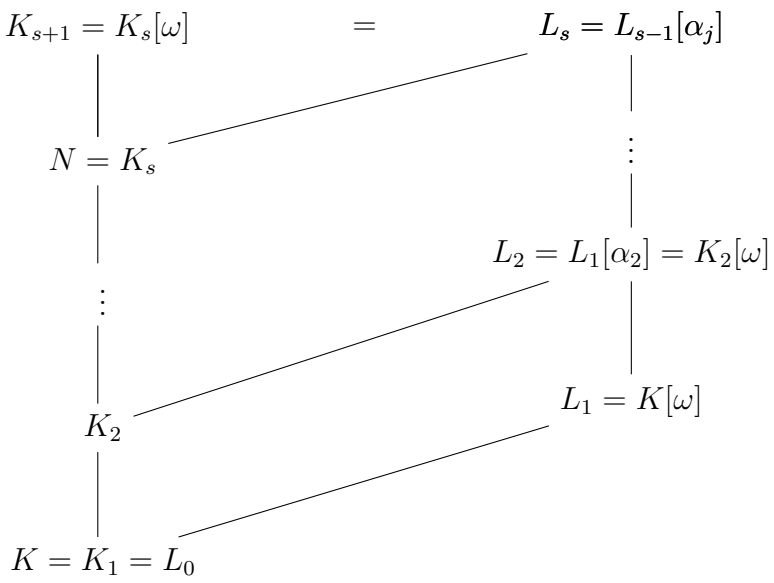

Figura 11 – Cadeia de corpos auxiliar comparada com a da hipótese

Como $L \supset K$ é extensão normal, o Teorema 5.2.2 garante que:

$$G = Aut_K L \simeq \frac{Aut_K M}{Aut_L M}$$

Considerando-se o Teorema 5.1.2 item 2, é suficiente mostrarmos que o grupo $Aut_K M$ é solúvel. Suponha que ζ seja uma raiz primitiva n-ésima da unidade, em que $n = n_1 n_2 \cdots n_r$, $M = K[a_1, a_2, \cdots, a_r]$, $a_i^{n_i} \in K_{i-1}$, e $K_i = K_{i-1} = K_I[a_i]$.

Denotando-se $M^* = M[\zeta]$, $K^* = K[\zeta]$, podemos admitir que se $\sigma \in Aut_K M$, então $\sigma^* \in Aut_{K^*} M^*$. Onde $\sigma^*|_M = \sigma$ e $\sigma^*(\zeta) = \zeta$.

Note que se $\phi \in Aut_K M$ é tal que $\sigma \neq \phi$ então $\sigma^* \neq \phi^*$ e portanto a aplicação abaixo estará bem definida:

$$\Phi : Aut_K M \longrightarrow Aut_{K^*} M^*$$

Sendo $\Phi(\sigma) = \sigma^*$, esta aplicação é um homomorfismo injetivo. Isto nos garante que

$$Aut_K M \simeq \Phi(Aut_K M) \leq Aut_{K^*} M^*$$

E daí, o grupo $Aut_K M$ é solúvel quando $Aut_{K^*} M^*$ for solúvel.

Por simplicidade de notação, assumiremos a partir de agora, que $K = K^* = K[\zeta]$, assim, K possui uma raiz primitiva n-ésima, ζ, da unidade.

Agora, sendo $M = K[a_1, a_2, ..., a_r]$ uma extensão radical sobre K, $n = n_1 \cdots n_r$, onde $a_i^{n_i} \in K_{i-1}$, e K contém uma raiz primitiva n-ésima da unidade, vamos provar por indução sobre o índice r que $Aut_K M$ é um grupo solúvel. Primeiro, se $r = 1$, então

$M = K[a_1]$, $a_1^{n_1} = b_0 \in K$ e como K contém uma raiz primitiva n_1-ésima da unidade, temos que $M = Gal(x^{n_1} - b_0, K)$ e pela Lema 6.1.2, $Aut_K M$ é abeliano, e portanto, solúvel.

Considere como hipótese de indução que $Aut_{K_1} M$ é solúvel, onde $M = K_1[a_2, a_3, ..., a_r]$.

Defina a função:

$$\Theta : Aut_K M \longrightarrow Aut_K K_1$$

dada por $\Theta(\sigma) = \sigma|_{K_1} = \sigma_1$. Sendo $K_1 = Gal(x^{n_1} - b_0, K)$ normal sobre K, provaremos que Θ é um homomorfismo.

Afirmamos que o núcleo $Ker(\Theta) = Aut_{K_1} M$.

De fato, $Ker(\Theta) \subset Aut_{K_1} M$ trivialmente, pois como $Ker(\Theta) = \{\sigma \in Aut_{K_1} M; \Theta(\sigma) = Id\}$, temos que todos elementos de $Ker(\Theta)$ fixam elementos de K_1.

Agora, suponha que $\sigma \in Aut_{K_1} M$, temos:

$$\Theta(\sigma) = \sigma|_{K_1} = \sigma_1$$

onde $\sigma_1 : K_1 \longrightarrow K_1$ é dada por $\sigma_1(x) = x$. Agora, veja que $\sigma_1(x) = id(x) \Rightarrow \sigma_1 \in Kerf(\Theta)$

Assim, pelo Teorema do Isomorfismo, segue-se:

$$\frac{Aut_K M}{Aut_{K_1} M} \simeq \Theta(Aut_K M) \leq Aut_K K_1$$

Como $Aut_K K_1$ é abeliano, e pela hipótese de indução, $Aut_{K_1} M$ é solúvel, obtemos que $Aut_K M$ é solúvel, como queríamos.

■

Veremos mais adiante que a recíproca do Teorema 6.1.3 é verdadeira, e de fato, ela é o resultado principal deste trabalho. Entretanto, ainda precisamos de alguns conceitos fundamentais para provarmos sua validade. Tais conceitos serão abordados nos capítulos seguintes.

7 Aplicações em Polinômios

7.1 Polinômios Simétricos

Nesta seção, iremos introduzir um conceito fundamental para o estudo do Grupo de Galois de um polinômio de grau n qualquer, denominado polinômios simétricos. Provaremos o chamado Teorema Fundamental dos Polinômios Simétricos, conforme a referência [5], o qual é de extrema importância para o nosso objetivo.

Primeiro, relembremos a definição de extensão finitamente gerada:

Definição 7.1.1. Considere os corpos L, K. A extensão $L \supset K$ é dita finitamente gerada se $L = K[a_1, \cdots, a_n]$, onde $n \in \mathbb{N}$.

Até aqui, consideramos apenas extensões algébricas. Mas nada impede que $a_j \in L$ seja transcendente sobre K. Como exemplos clássicos de números transcendentes sobre $\mathbb{Q}$, podemos considerar a constante de Euler e e o número π.

Definição 7.1.2. Sejam $t_1, \cdots, t_n \in L$ elementos transcendentes sobre K. Tais elementos são independentes se não existe polinômio f não trivial sobre K, em n indeterminadas tal que $f(t_1, \cdots, t_n) = 0$ em L.

Exemplo 7.1.1. *Se x é transcendente sobre K e y é transcendente sobre $K[x]$, então $K[x, y]$ é uma extensão transcendente finitamente gerada e x, y são independentes. Entretanto, se tivéssemos x e $y = x^2 + 1$, então x e y seriam dependentes, pois ambos se relacionariam pela equação $x^2 + 1 - y = 0$.*

Portanto, indeterminadas sobre K são definidas como elementos transcendentes sobre K sem relações algébricas entre eles. E neste caso, são chamados de variáveis algebricamente independentes.

Agora, para dar continuidade ao estudo sobre a Teoria de Galois, precisamos introduzir um novo assunto que possui uma importância bastante relevante para a generalização do grupo de Galois de um polinômio de grau n. O objetivo aqui é definir, e exemplificar os polinômios simétricos, e posteriormente, demonstrar o Teorema Fundamental dos Polinômios Simétricos.

Para ilustrar melhor a ideia de polinômios simétricos, considere K um corpo qualquer, e seja $h \in K[x]$ um polinômio, digamos, de terceiro grau, dado por $h(x) = ax^3 + bx^2 + cx + d$. Sendo L uma extensão qualquer de K onde h se fatora e t_1, t_2 e t_3 suas

raízes, sabemos que:

$$h(x) = ax^3 + bx^2 + cx + d = a(x - t_1)(x - t_2)(x - t_3)$$

Ao desenvolver o lado direito da igualdade acima, obtemos:

$$\begin{aligned} h(x) &= a(x^3 - x^2t_3 - x^2t_2 - x^2t_1 + xt_1t_2 + xt_2t_3 + xt_1t_3 - t_1t_2t_3) \\ &= a(x^3 - (t_1 + t_2 + t_3)x^2 + (t_1t_2 + t_2t_3 + t_1t_3)x - t_1t_2t_3) \end{aligned}$$

Como $a \neq 0$, segue-se das igualdades acima que:

$$x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a} = x^3 - (t_1 + t_2 + t_3)x^2 + (t_1t_2 + t_2t_3 + t_1t_3)x - t_1t_2t_2$$

E daí comparando-se termo a termo, obtemos que:

$$\begin{aligned} \frac{b}{a} &= -(t_1 + t_2 + t_3); \\ \\ \frac{c}{a} &= t_1t_2 + t_2t_3 + t_1t_3; \\ \\ \frac{d}{a} &= -t_1t_2t_3 \end{aligned}$$

Essas igualdades que foram deduzidas acima são conhecidas como Relações de Girard. Elas estabelecem uma relação entre os coeficientes de um polinômio e suas raízes. Ou seja, os coeficientes de um polinômio são funções de suas raízes. A generalização deste fato para um polinômio de grau n qualquer, também é verdadeira.

Considerando-se ainda o corpo K, seja $f \in K[x]$, de grau n, dado por:

$$f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0.$$

Suponha que f se fatore completamente em uma certa extensão $L \supset K$. Isto nos dá:

$$f(x) = (x - r_1)(x - r_2)\cdots(x - r_n).$$

Como vimos, os coeficientes a_j do polinômio são funções de suas raízes, então, podemos ainda escrever:

$$f(x) = x^n - s_1(r_1, r_2, \cdots, r_n)x^{n-1} + s_2(r_1, r_2, \cdots, r_n)x^{n-2} - \cdots + (-1)^n s_n(r_1, r_2, \cdots, r_n)$$

onde as expressões s_j são funções de $r_1, \cdots r_n$, dadas por:

$$\begin{aligned} s_1(r_1, \cdots, r_n) &= \sum_{i=1}^{n} r_i; \\ s_2(r_1, \cdots, r_n) &= \sum_{i<j}^{n} r_ir_j; \\ &\vdots \\ s_k(r_1, \cdots, r_n) &= \sum_{i_1<\cdots<i_k}^{n} r_{i_1}\cdots r_{i_k}; \\ &\vdots \\ s_n(r_1, \cdots, r_n) &= \prod_{i=1}^{n} r_i \end{aligned}$$

As funções $s_k = s_k(r_1, \cdots, r_n)$, $\forall k \in \{1, \cdots, n\}$ possuem a propriedade de serem invariantes por qualquer permutação das raízes r_j (independente da multiplicidade m da mesma. Caso $m \geq 2$, elas são consideradas como distintas). É claro que aqui estamos considerando s_j como um polinômio de n variáveis, onde r_i é a i-ésima variável. Em outras palavras, estas funções polinomiais são fixadas pela ação do grupo S_n no conjunto $\{r_1, \cdots, r_n\}$. Isto é:

$$\sigma \cdot s(r_1, \cdots r_n) = s(r_{\sigma(1)}, \cdots, r_{\sigma(n)}) = s(r_1, \cdots, r_n), \forall \sigma \in S_n$$

Tudo que foi explicitado acima, nos permite fazer as seguintes definições:

Definição 7.1.3. Um polinômio $f \in K[r_1, \cdots, r_n]$ diz-se simétrico em $r_1, \cdots, r_n$ se for fixado pela ação de S_n conforme explicitado acima. Isto é, se $\sigma \cdot f(r_1, \cdots r_n) = f(r_{\sigma(1)}, \cdots, r_{\sigma(n)}) = f(r_1, \cdots, r_n)$, $\forall \sigma \in S_n$.

Aqui estamos supondo que $r_1, \cdots r_n$ são variáveis algebricamente independentes. De maneira informal, isto significa que todas as variáveis do polinômio f "desempenham o mesmo papel", e trocá-las de lugar com outras, não faz nenhuma diferença em termos numéricos.

Proposição 7.1.1. *O conjunto dos polinômios simétricos $K[r_1, \cdots, r_n]$ em n variáveis é um subanel do conjunto dos polinômios em n variáveis.*

Demonstração: Primeiro, note que $K[r_1, \cdots r_n]$ é não vazio, pois o polinômio nulo de fato pertence a $K[r_1, \cdots, r_n]$. Agora, sejam $f, g \in K[r_1, \cdots, r_n]$ e $\sigma \in S_n$ uma permutação qualquer. Note que:

$$\begin{aligned}
\sigma \cdot (f(r_1, \cdots, r_n) - g(r_1, \cdots, r_n)) &= \sigma \cdot ((f-g)(r_1, \cdots, r_n)) \\
&= (f-g)(r_{\sigma(1)}, \cdots r_{\sigma(n)}) \\
&= f(r_{\sigma(1)}, \cdots, r_{\sigma(n)}) - g(r_{\sigma(1)}, \cdots, r_{\sigma(n)}) \\
&= f(r_1, \cdots, r_n) - g(r_1, \cdots, r_n)
\end{aligned}$$

$$\begin{aligned}
\sigma \cdot (f(r_1, \cdots, r_n) g(r_1, \cdots, r_n)) &= \sigma \cdot ((fg)(r_1, \cdots, r_n)) \\
&= (fg)(r_{\sigma(1)}, \cdots r_{\sigma(n)}) \\
&= f(r_{\sigma(1)}, \cdots, r_{\sigma(n)}) g(r_{\sigma(1)}, \cdots, r_{\sigma(n)}) \\
&= f(r_1, \cdots, r_n) g(r_1, \cdots, r_n)
\end{aligned}$$

$\forall \sigma \in S_n$. Ou seja, $f - g, fg \in K[r_1, \cdots, r_n]$. Isso mostra o que queríamos.

■

Definição 7.1.4. As funções polinomiais s_k deduzidas anteriormente são chamadas de Polinômios Simétricos Elementares.

Considere os exemplos abaixo:

Exemplo 7.1.2. *Considere o polinômio $f \in \mathbb{Q}[x]$ dado por $f(x) = x^3 - 2x^2 - x + 2$. Suas raízes são $r_1 = -1, r_2 = 1$ e $r_3 = 2$. É claro que $f(x) = (x+1)(x-1)(x-2)$. Temos que:*

1. $s_1(-1, 1, 2) = 2$;
2. $s_2(-1, 1, 2) = -1$;
3. $s_3(-1, 1, 2) = -2$;

Considere, por exemplo a permutação $\sigma = (132) \in S_3$ agindo no conjunto de índices $\{1, 2, 3\}$. Veja que:

1. $\sigma \cdot s_1(r_1, r_2, r_3) = s_1(r_{\sigma(1)}, r_{\sigma(2)}, r_{\sigma(3)}) = s_1(r_3, r_1, r_2) = 2$
2. $\sigma \cdot s_2(r_1, r_2, r_3) = s_2(r_{\sigma(1)}, r_{\sigma(2)}, r_{\sigma(3)}) = s_2(r_3, r_1, r_2) = -1$
3. $\sigma \cdot s_3(r_1, r_2, r_3) = s_3(r_{\sigma(1)}, r_{\sigma(2)}, r_{\sigma(3)}) = s_3(r_3, r_1, r_2) = -2$

Exemplo 7.1.3. *Os polinômios seguintes são exemplos de funções polinomiais simétricas:*

1. $f(x, y) = x + y$
2. $h(x, y, z) = x^5 + y^5 + z^5 + x^3yz + y^3xz + z^3xy + xyz$
3. $i(x, y, z) = x^3 + y^3 + z^3 - 3xyz$

Observe, por exemplo, o polinômio simétrico dado por $i(x, y) = x^2 + y^2$. Note que i pode ser obtido como

$$\begin{aligned} i(x,y) &= x^2 + y^2 \\ &= (x+y)^2 - 2xy \\ &= s_1^2(x,y) - 2s_2(x,y) \end{aligned}$$

onde s_1 e s_2 são Polinômios Simétricos Elementares conforme a Definição 7.1.4. É claro que é possível generalizar. Considere, por exemplo:

$$\begin{aligned} r(x_1, \cdots, x_n) &= x_1^2 + \cdots + x_n^2 \\ &= (x_1 + \cdots + x_n)^2 - 2(x_1x_2 + \cdots + x_{n-1}x_n) \\ &= s_1^2(x_1, \cdots, x_n) - 2s_2(x_1, \cdots, x_n) \end{aligned}$$

onde $s_1(x_1, \cdots, x_n)$ e $s_2(x_1, \cdots, x_n)$ são as mesmas relações acima, para o caso de n variáveis. A pergunta que devemos fazer é: "É possível reescrever todos os polinômios simétricos em função de polinômios simétricos elementares?"

Definição 7.1.5. Define-se como o grau do monômio $r_1^{i_1} r_2^{i_2} \cdots r_n^{i_n}$ a n-upla $(i_1, \cdots, i_n)$.

A partir disso, consideraremos a ordem lexicográfica: diremos que $(i_1, \cdots, i_n) > (j_1, \cdots, j_n)$ se o primeiro elemento não nulo (caso exista) na sequência $i_1 - j_1$, $i_2 - j_2$, $\cdots$, $i_n - j_n$ for positivo.

Definição 7.1.6. Seja $f \in K[x_1, \cdots, x_n]$. Define-se como o grau de f como o máximo dos graus dos seus monômios. A notação utilizada é a usual: $\partial(f)$.

Observação 7.1.1. *Novamente, considere as funções simétricas elementares s_k, com $k \in \{1, \cdots, n\}$. Considerando a definição anterior e a ordem lexicográfica, podemos determinar o grau de cada uma destas funções. Seguindo um raciocínio indutivo, temos que:*

- $\partial(s_1) = (1, 0, 0, \cdots, 0)$.
- $\partial(s_2) = (1, 1, 0, \cdots, 0)$.
- $\partial(s_3) = (1, 1, 1, \cdots, 0)$
- $\partial(s_k) = (1, 1, 1, 1, \cdots, 1, 0, \cdots 0)$ *para algum* $k \in \{4, \cdots, n\}$
- $\partial(s_n)(1, 1, 1, \cdots, 1)$

O objetivo aqui neste capítulo é provar que qualquer função polinomial simétrica em $r_1, \cdots, r_n$ pode ser escrita como uma expressão de polinômios simétricos elementares $s_1, \cdots, s_n$ como foi exemplificado após o Exemplo 7.1.3.

Teorema 7.1.7. *(Teorema Fundamental dos Polinômios Simétricos) Todo polinômio simétrico em $r_1, \cdots, r_n$ pode ser obtido como uma expressão de polinômios simétricos elementares $s_1, \cdots, s_n$.*

Demonstração: Seja $f \in K[r_1, \cdots, r_n]$ um polinômio simétrico. Suponha, considerando a ordem lexicográfica que $Ar_1^{i_1} r_2^{i_2} \cdots r_n^{i_n}$ seja o monômio de maior grau de f. É claro que $Ar_1^{i_1} r_2^{i_2} \cdots r_n^{i_n}$ também é um polinômio simétrico, e qualquer monômio obtido a partir deste pela permutação das variáveis, também será um monômio de f. Defina:

$$f_1 = As_1^{(i_1 - i_2)} s_2^{(i_2 - i_3)} \cdots s_{n-1}^{(i_{n-1} - i_n)} s_n^{i_n}$$

e levando em conta a Observação 7.1.1, note que $\partial(f_1) = (i_1 - i_2)\partial(s_1)(i_2 - i_3)\partial(s_2) \cdots i_n \partial(s_n) = i_1(1, 0, 0, \cdots, 0) - i_2(1, 0, 0, \cdots, 0) + i_2(1, 1, 0, \cdots, 0) - i_3(1, 1, 0, \cdots, 0) + i_3(1, 1, 1, \cdots, 0) + \cdots + i_n(1, 1, 1, \cdots, 1) = (i_1, i_2, i_3, \cdots, i_n)$, que é o grau do monômio $Ar_1^{i_1} r_2^{i_2} \cdots r_n^{i_n}$.

Além disso,

$$\begin{aligned} f_1 &= As_1^{(i_1-i_2)}s_2^{(i_2-i_3)}\cdots s_{n-1}^{(i_{n-1}-i_n)}s_n^{i_n} \\ &= A\left[\left(\sum_{k=1}^{n} r_k\right)^{(i_1-i_2)}\left(\sum_{k<l} r_k r_l\right)^{(i_2-i_3)}\cdots\left(\sum_{k_1<\cdots<k_{n-1}}^{n} r_{k_1}\cdots r_{k_{n-1}}\right)^{(i_{n-1}-i_n)}\left(\prod_{k=1}^{n} r_k\right)^{i_n}\right] \end{aligned}$$

Considerando-se a ordem lexicográfica e novamente a Observação 7.1.1, não é necessário expandir os termos de f_1. Pelo mesmo raciocínio indutivo já empregado, conclui-se que o monômio de maior grau da expressão acima é dado por:

$$A(r_1^{(i_1-i_2)}r_2^{(i_2-i_3)}r_2^{(i_2-i_3)}\cdots(r_1^{i_n}\cdots r_n^{i_n})) = A(r_1^{i_1}r_2^{i_2}\cdots r_{n-1}^{i_{n-1}}r_n^{i_n})$$

que é exatamente igual ao monômio de maior grau do polinômio f.

Assim, $f - f_1$ também é um polinômio simétrico cujo monômio de maior grau, digamos, $Br_1^{j_1}r_2^{j_2}\cdots r_n^{j_n}$ possui grau menor do que o monômio $Ar_1^{i_1}r_2^{i_2}\cdots r_n^{i_n}$ em f. É claro que $j_1 \geq j_2 \geq \cdots \geq i_n$. Agora, defina:

$$f_2 = Bs_1^{(j_1-j_2)}s_2^{(j_2-j_3)}\cdots s_{n-1}^{(j_{n-1}-j_n)}s_n^{j_n}$$

De forma análoga a que fizemos anteriormente, note que o monômio de maior grau do polinômio $f - f_1$ é o mesmo que o monômio definido f_2. Novamente, o polinômio simétrico dado pela diferença $f - f_1 - f_2$ possui um monômio de maior grau, cujo o grau é menor do que $\partial(f_2)$. Repetindo-se o processo indutivamente, obteremos o polinômio nulo dado por $f - f_1 - f_2 - \cdots - f_p = 0$, onde f_i é definido em função dos polinômios simétricos elementares, $\forall i \in \{1, \cdots, p\}$. Portanto,

$$f = f_1 + f_2 + \cdots + f_p$$

como queríamos.

■

Com esse Teorema, mostramos que $K[r_1, \cdots, r_n] \subset K[s_1, \cdots, s_n]$. Observe que a inclusão contrária é imediata. Em outras palavras, o teorema acima é equivalente a afirmar que, se $K[r_1, \cdots, r_n]$ é o anel dos polinômios simétricos, então $K[r_1, \cdots, r_n] = K[s_1, \cdots, s_n]$.

Exemplo 7.1.4. *Considere o polinômio* $f = x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2$. *Note que* $\partial(f) = (2, 2, 0)$. *De acordo com o teorema anterior, devemos tomar* $f_1 = s_1^0s_2^2s_3^0 = s_2^2 = (x_1x_2 + x_1x_3 + x_2x_3)^2$. *Daí, segue-se que*

$$\begin{aligned} f - f_1 &= x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 - (x_1x_2 + x_1x_3 + x_2x_3)^2 \\ &= x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 - x_1^2x_2^2 - x_1^2x_3^2 - x_2^2x_3^2 - 2x_1^2x_2x_3 - 2x_1x_2^2x_3 - 2x_1x_2x_3^2 \\ &= -2(x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2) \end{aligned}$$

E que $\partial(f - f_1) = (2, 1, 1)$.

Novamente pelo teorema anterior, tome

$$\begin{aligned} f_2 &= -2s_1 s_2^0 s_3 \\ &= -2(x_1 + x_2 + x_3)(x_1 x_2 x_3) \\ &= -2(x_1^2 x_2 x_3 + x_1 x_2^2 x_3 + x_1 x_2 x_3^2) \\ &= -2x_1^2 x_2 x_3 - 2x_1 x_2^2 x_3 - 2x_1 x_2 x_3^2 \end{aligned}$$

Assim

$$\begin{aligned} f - f_1 - f_2 &= -2x_1^2 x_2 x_3 - 2x_1 x_2^2 x_3 - 2x_1 x_2 x_3^2 + 2x_1^2 x_2 x_3 + 2x_1 x_2^2 x_3 + 2x_1 x_2 x_3^2 \\ &= 0 \end{aligned}$$

Logo, $f = f_1 + f_2$ *e portanto,* $f = s_2^2 - 2s_1 s_3$

Definição 7.1.8. Uma função f em n variáveis é uma função racional, se f pode ser escrita como uma fração de funções polinomiais. Em outras palavras, se $f(r_1, \cdots, r_n)$ é uma função racional, então existem $p(r_1, \cdots, r_n) \in K[r_1, \cdots, r_n]$, $q(r_1, \cdots, r_n) \in K[r_1, \cdots, r_n] - \{0\}$ tais que $f(r_1, \cdots, r_n) = \dfrac{p(r_1, \cdots, r_n)}{q(r_1, \cdots, r_n)}$.

Para facilitar, denotaremos o anel das funções racionais com coeficientes no corpo K por $K(r_1, \cdots, r_n)$.

O grupo simétrico S_n também age naturalmente em $K(r_1, \cdots, r_n)$. Assim, a fração $\dfrac{p}{q}$ diz-se fixa por essa ação, se:

$$\frac{p(r_{\sigma(1)}, \cdots, r_{\sigma(n)})}{q(r_{\sigma(1)}, \cdots, r_{\sigma(n)})} = \frac{p(r_1, \cdots, r_n)}{q(r_1, \cdots, r_n)}, \forall \sigma \in S_n$$

.

Teorema 7.1.9. *Um elemento de* $K(r_1, \cdots, r_n)$ *é fixo pela ação do grupo simétrico* S_n *se, e somente se, este elemento pertencer a* $K(s_1, \cdots, s_n)$.

Demonstração: Seja $f/g \in K(r_1, \cdots, r_n)$ um elemento fixo pela ação do grupo simétrico S_n. Veja que, se f ou g for um polinômio simétrico, ou seja, se f ou g for fixo pela ação, então é claro que o outro também será fixo. Basta observar que se, digamos g não fosse fixado, teríamos:

$$\frac{f(r_{\sigma(1)}, \cdots, r_{\sigma(n)})}{g(r_{\sigma(1)}, \cdots, r_{\sigma(n)})} \neq \frac{f(r_1, \cdots, r_n)}{g(r_1, \cdots, r_n)}$$

uma vez que $g(r_{\sigma(1)}, \cdots, r_{\sigma(n)}) \neq g(r_1, \cdots, r_n)$. E isso contrariaria a hipótese. Sendo assim, para concluir o resultado, basta aplicar o Teorema Fundamental dos Polinômios Simétricos e o teorema está provado.

Agora, suponha que nem f e nem g sejam fixos pela ação de S_n. Neste caso, considere a órbita, digamos de g sob a ação de S_n dada pelo conjunto $o(g) = \{g, g_2, \cdots, g_k\}$. Note que o produto $gg_2 \cdots g_k$ é fixado por S_n. Basta ver que:

$$\begin{aligned}\sigma(gg_2 \cdots g_k) &= \sigma(g)\sigma(g_2) \cdots \sigma(g_k) \\ &= g(r_{\sigma(1)}, \cdots, r_{\sigma(n)})g_2(r_{\sigma(1)}, \cdots, r_{\sigma(n)}) \cdots g_k(r_{\sigma(1)}, \cdots, r_{\sigma(n)})\end{aligned}$$

$\forall \sigma \in S_n$. Assim, é claro que toda imagem de σ aplicado em um elemento de $o(g)$ ainda será um elemento de $o(g)$. E independente da ordem dos índices $\{1, \cdots, k\}$, teremos o mesmo resultado, uma vez que aqui vale a comutatividade.

Agora, basta notar que $\dfrac{f}{g} = \dfrac{fg_2 \cdots g_l}{gg_2 \cdots g_k}$ e que o denominador $gg_2 \cdots g_k$ é um polinômio é simétrico. Daí, voltamos para o primeiro caso analisado, e o resultado está demonstrado, uma vez que a recíproca é imediata.

■

Uma fato importante é que a representação de um polinômio simétrico nas variáveis $r_1, \cdots, r_n$ como um elemento do anel $K[r_1, \cdots, r_n]$, conforme afirma o Teorema 7.1.7, é única. Além disso, sendo $r_1, \cdots, r_n$ variáveis algebricamente independentes, então $s_1, \cdots, s_n$ também são. De fato, existe um isomorfismo entre os anéis $K[y_1, \cdots, y_n]$ e $K[s_1, \cdots, s_n]$, que é o que provaremos no próximo teorema. Primeiro, considerando $y_1, \cdots, y_n$ variáveis algebricamente independentes, defina a função:

$$\begin{array}{rccc}\varphi\colon & K[y_1, \cdots, y_n] & \longrightarrow & K[s_1, \cdots, s_2] \\ & y_j & \longmapsto & \varphi(y_j) = s_j\end{array}$$

Esta função é um homomorfismo de anéis. De fato, sejam $f, g \in K[y_1, \cdots, y_n]$. Isto é:

$$f(y_1, \cdots, y_n) = \sum_{j=1}^{k} A_j y_1^{i_{1,j}} \cdots y_n^{i_{n,j}}$$

$$g(y_1, \cdots, y_n) = \sum_{p=1}^{m} B_p y_1^{q_{1,p}} \cdots y_n^{q_{n,p}}$$

Assim, temos que:

$$\begin{aligned}\varphi(f+g) &= \varphi\left(\sum_{j=1}^{k} A_j y_1^{i_{1,j}} \cdots y_n^{i_{n,j}} + \sum_{p=1}^{m} B_p y_1^{q_{1,p}} \cdots y_n^{q_{n,p}}\right) \\ &= \sum_{j=1}^{k} \varphi(A_j y_1^{i_{1,j}} \cdots y_n^{i_{n,j}}) + \sum_{p=1}^{m} \varphi(B_p y_1^{q_{1,p}} \cdots y_n^{q_{n,p}}) \\ &= \sum_{j=1}^{k} A_j s_1^{i_{1,j}} \cdots s_n^{i_{n,j}} + \sum_{p=1}^{m} B_p s_1^{q_{1,p}} \cdots s_n^{q_{n,p}} \\ &= \varphi(f) + \varphi(g)\end{aligned}$$

E também:

$$\begin{aligned}
\varphi(fg) &= \varphi\left[\left(\sum_{j=1}^{k} A_j y_1^{i_{1,j}} \cdots y_n^{i_{n,j}}\right)\left(\sum_{p=1}^{m} B_p y_1^{q_{1,p}} \cdots y_n^{q_{n,p}}\right)\right] \\
&= \varphi\left(\sum_{j=1}^{k}\sum_{p=1}^{m} A_j B_p y_1^{i_{1,j}+q_{1,p}} \cdots y_n^{i_{n,j}+q_{n,p}}\right) \\
&= \sum_{j=1}^{k}\sum_{p=1}^{m} \varphi(A_j B_p y_1^{i_{1,j}+q_{1,p}} \cdots y_n^{i_{n,j}+q_{n,p}}) \\
&= \sum_{j=1}^{k}\sum_{p=1}^{m} A_j B_p s_1^{i_{1,j}+q_{1,p}} \cdots s_n^{i_{n,j}+q_{n,p}} \\
&= \left(\sum_{j=1}^{k} A_j s_1^{i_{1,j}} \cdots s_n^{i_{n,j}}\right)\left(\sum_{p=1}^{m} B_p s_1^{q_{1,p}} \cdots s_n^{q_{n,p}}\right) \\
&= \varphi(f)\varphi(g)
\end{aligned}$$

Isto mostra que φ é um homomorfismo de anéis. O teorema a seguir garante que se trata de um homomorfismo bijetor.

Teorema 7.1.10. *Com as condições e notações estabelecidas acima, o homomorfismo φ é um isomorfismo entre os anéis $K[y_1, \cdots, y_n]$ e $K[s_1, \cdots, s_n]$*

Demonstração: Para mostrar a injetividade de φ, considere $\varphi(f), \varphi(g) \in K[s_1, \cdots, s_n]$ tais que $\varphi(f) = \varphi(g)$. Suponha que $u = Ay_1^{i_1} \cdots y_n^{i_n}$ seja o monômio de maior grau de f (pela ordem lexicográfica). De maneira idêntica a que foi feita na demonstração do Teorema Fundamental dos Polinômios Simétricos (Teorema 7.1.7), observe que o grau de $\varphi(u) = As_1^{i_1} \cdots s_n^{i_n}$ é dado por

$$\partial(\varphi(u)) = (i_1 + \cdots + i_n, i_2 + \cdots + i_n, \cdots, i_{n-1} + i_n, i_n).$$

Considere a função:

$$\begin{array}{rccc}
\tau: & \mathbb{N}^n & \longrightarrow & \mathbb{N}^n \\
& (i_1, \cdots, i_n) & \longmapsto & (i_1 + \cdots + i_n, i_2 + \cdots + i_n, \cdots, i_{n-1} + i_n, i_n)
\end{array}$$

Afirmamos que a função τ é injetiva. De fato, se considerarmos a igualdade entre as n-uplas abaixo, teremos que:

$$(i_1 + \cdots + i_n, i_2 + \cdots + i_n, \cdots, i_{n-1} + i_n, i_n) = (j_1 + \cdots + j_n, j_2 + \cdots + j_n, \cdots, j_{n-1} + j_n, j_n)$$

implicará em $i_n = j_n$, e consequentemente, teremos também $i_{n-1} = j_{n-1}, \cdots i_2 = j_2$ e $i_1 = j_1$. E portanto, $(i_1, \cdots, i_n) = (j_1, \cdots, j_n)$, o que garante a injetividade de τ.

Com o fato provado acima, temos que o termo de maior grau de g tem que coincidir com o termo de maior grau de f. Prosseguindo com este raciocínio com os demais monômios

de f e g, conclui-se que $f = g$. Além disso, a função φ é claramente sobrejetiva devido sua construção, uma vez que dado $s_j \in K[s_1, \cdots, s_n]$, existe $y_j \in K[y_1, \cdots, y_n]$ tal que $\varphi(y_j) = s_j$. Portanto, φ é um isomorfismo.

■

Este teorema garante que a representação de um polinômio simétrico como um elemento de $K[s_1, \cdots, s_n]$ é única, uma vez que existe uma correspondência bijetiva entre os anéis.

Teorema 7.1.11. *Suponha que $y_1, \cdots, y_n$ sejam variáveis algebricamente independentes sobre um corpo F e $K = F(y_1, \cdots, y_n)$ seja o corpo das funções racionais nestas variáveis. Então, as n raízes $\alpha_1, \cdots, \alpha_n$ em alguma extensão $L \supset K$ do polinômio $f(T) = T^n - y_1T^{n-1} + y_2T^{n-2} - \cdots + (-1)^n y_n$ são algebricamente independentes sobre F, ou seja, o anel $F[\alpha_1, \cdots, \alpha_n]$ é isomorfo a um anel de polinômios em n variáveis independentes.*

Demonstração: Considere as funções:

$$\begin{array}{rccc} \sigma\colon & F[r_1, \cdots, r_n] & \longrightarrow & F[\alpha_1, \cdots, \alpha_n] \\ & r_j & \longmapsto & \sigma(r_j) = \alpha_j \end{array}$$

e

$$\begin{array}{rccc} \theta\colon & F[y_1, \cdots, y_n] & \longrightarrow & F[s_1, \cdots, s_n] \\ & y_j & \longmapsto & \theta(y_j) = s_j \end{array}$$

Esquematicamente, temos o seguinte diagrama:

$$\begin{array}{ccc} F[r_1, \cdots, r_n] & \xrightarrow{\sigma} & F[\alpha_1, \cdots, \alpha_n] \\ \Big| & & \Big| \\ F[s_1, \cdots, s_n] & \xleftarrow{\theta} & F[y_1, \cdots, y_n] \end{array}$$

Note ainda que $\sigma|_{F[s_1,\cdots,s_n]} = \theta^{-1}$. De fato, pelo teorema anterior, θ é um isomorfismo. Assim, fixado $h \in F[s_1, \cdots, s_n]$, temos:

$$\begin{aligned} \sigma(h(s_1, \cdots, s_n)) &= h(s_1(\alpha_1, \cdots, \alpha_n), \cdots, s_n(\alpha_1, \cdots, \alpha_n)) \\ &= h(y_1, \cdots, y_n) \\ &= \theta^{-1}(h(s_1, \cdots, s_n)) \end{aligned}$$

Provaremos que a função σ é um isomorfismo de anéis. A demonstração de que é um homomorfismo é idêntica a que fizemos para o Teorema 1.3. Para provarmos a injetividade, suponha por absurdo que não seja. Isto é, suponha $ker(\sigma) \neq \{0\}$, ou seja, que exista $f \in F[r_1, \cdots, r_n] \backslash \{0\}$ tal que $f(\alpha_1, \cdots, \alpha_n) = 0$. Defina $g(r_1, \cdots, r_n) = \prod_{\tau \in S_n} f(r_{\tau(1)}, \cdots, r_{\tau(n)})$.

Uma vez que g é definido como o produto de polinômios não nulos, então $g \neq 0$. Além disso, se considerarmos uma enumeração do conjunto S_n como $S_n = \{\tau_1, \tau_2, \cdots, \tau_n\}$, note que:

$$\begin{aligned} g(r_1, \cdots, r_n) &= \prod_{\tau \in S_n} f(r_{\tau(1)}, \cdots, r_{\tau(n)}) \\ &= f(r_{\tau_1(1)}, \cdots, r_{\tau_1(n)}) f(r_{\tau_2(1)}, \cdots, r_{\tau_2(n)}) \cdots f(r_{\tau_n(1)}, \cdots, r_{\tau_n(n)}) \end{aligned}$$

Assim, considerando a comutatividade do produto de polinômios, temos que g é um polinômio simétrico. é um polinômio simétrico. Logo, pelo Teorema Fundamental dos Polinômios Simétricos, existe $h \in F[s_1, \cdots, s_n]$ tal que $g(r_1, \cdots, r_n) = h(s_1, \cdots, s_n)$.

Agora, observe que, nessas condições:

$$\sigma(g) = \prod_{\tau \in S_n} f(\alpha_{\tau(1)}, \cdots, \alpha_{\tau(n)}) = 0$$

Como $\sigma(v) = \theta^{-1}(v)$ para $v \in F[s_1, \cdots, s_n]$ e θ é isomorfismo, então $h = 0$, o que implicaria que $f = 0$. Mas isso é uma contradição. Logo, f é injetora.

Pelo menos raciocínio utilizado na demonstração do teorema anterior, segue-se que σ também é sobrejetora. Portanto, σ é um isomorfismo, como queríamos.

■

Dessa forma, o polinômio $f(T) = T^n - y_1 T^{n-1} + y_2 T^{n-2} - \cdots + (-1)^n y_n$ é um polinômio mônico genérico de grau n com coeficientes no corpo $F(y_1, \cdots, y_n)$, onde $y_1, \cdots, y_n$ são variáveis algebricamente independentes sobre F.

7.2 O polinômio geral de grau n

Suponha que K seja um corpo de característica zero ($char(K) = 0$), e $x_1, \cdots, x_n$ sejam variáveis algebricamente independentes sobre K e $L = K(x_1, \cdots, x_n)$ o corpo das funções racionais nestas variáveis.

Vimos anteriormente que o grupo simétrico age, de forma natural, sobre o corpo L. Isto é, dado $r \in L$, existem $f, g \in K[x_1, \cdots, x_n]$, com $g \neq 0$, tais que:

$$r(x_1, \cdots, x_n) = \frac{f(x_1, \cdots, x_n)}{g(x_1, \cdots, x_n)},$$

e

$$\sigma(r(x_1, \cdots, x_n)) = r(x_{\sigma(1)}, \cdots, x_{\sigma(n)}) = \frac{f(x_{\sigma(1)}, \cdots, x_{\sigma(n)})}{g(x_{\sigma(1)}, \cdots, x_{\sigma(n)})}$$

$\forall \sigma \in S_n$.

A essência da Teoria de Galois está no fato de que elementos distintos do grupo S_n induzem distintos automorfismos sobre as extensões de corpos consideradas. De fato,

para mostrarmos isso, fixe uma permutação $\sigma \in S_n$, considere o grupo simétrico S_n agindo sobre o conjunto das n variáveis $\{x_1, \cdots, x_n\}$ e defina:

$$\begin{array}{rccc} \hat{\sigma}: & L & \longrightarrow & L \\ & r(x_1, \cdots, x_n) & \longmapsto & r(x_{\sigma(1)}, \cdots, x_{\sigma(n)}) \end{array}$$

Por definição, se $r_1(x_1, \cdots, x_n), r_2(x_1, \cdots, x_n) \in L$, então existem $f_1(x_1, \cdots, x_n)$, $g_1(x_1, \cdots, x_n)$, $f_2(x_1, \cdots, x_n)$, $g_2(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n]$, com $g_1, g_2 \neq 0$, tais que:

$$r_1(x_1, \cdots, x_n) = \frac{f_1(x_1, \cdots, x_n)}{g_1(x_1, \cdots x_n)}$$

$$r_2(x_1, \cdots, x_n) = \frac{f_2(x_1, \cdots, x_n)}{g_2(x_1, \cdots, x_n)}$$

Mostraremos primeiro que $\hat{\sigma}$ é homomorfismo de corpos:

$$\begin{array}{rcc} \hat{\sigma}(r_1 + r_2) & = & \hat{\sigma}\left(\dfrac{f_1(x_1, \cdots, x_n)}{g_1(x_1, \cdots x_n)} + \dfrac{f_2(x_1, \cdots, x_n)}{g_2(x_1, \cdots, x_n)}\right) \\ & = & \hat{\sigma}\left(\dfrac{f_1(x_1, \cdots, x_n)g_2(x_1, \cdots, x_n) + f_2(x_1, \cdots, x_n)g_1(x_1, \cdots, x_n)}{g_1(x_1, \cdots x_n)g_2(x_1, \cdots, x_n)}\right) \\ & = & \dfrac{f_1(x_{\sigma(1)}, \cdots, x_{\sigma(n)})g_2(x_{\sigma(1)}, \cdots, x_{\sigma(n)}) + f_2(x_{\sigma(1)}, \cdots, x_{\sigma(n)})g_1(x_{\sigma(1)}, \cdots, x_{\sigma(n)})}{g_1(x_{\sigma(1)}, \cdots x_{\sigma(n)})g_2(x_{\sigma(1)}, \cdots, x_{\sigma(n)})} \\ & = & \dfrac{f_1(x_{\sigma(1)}, \cdots, x_{\sigma(n)})}{g_1(x_{\sigma(1)}, \cdots, x_{\sigma(n)})} + \dfrac{f_2(x_{\sigma(1)}, \cdots, x_{\sigma(n)})}{g_2(x_{\sigma(1)}, \cdots, x_{\sigma(n)})} \\ & = & \hat{\sigma}(r_1) + \hat{\sigma(r_2)} \end{array}$$

Em relação ao produto, temos:

$$\begin{array}{rcc} \hat{\sigma}(r_1 \cdot r_2) & = & \hat{\sigma}\left(\dfrac{f_1(x_1, \cdots, x_n)}{g_1(x_1, \cdots x_n)} \cdot \dfrac{f_2(x_1, \cdots, x_n)}{g_2(x_1, \cdots, x_n)}\right) \\ & = & \dfrac{f_1(x_{\sigma(1)}, \cdots, x_{\sigma(n)}) \cdot f_2(x_{\sigma(1)}, \cdots, x_{\sigma(n)})}{g_1(x_{\sigma(1)}, \cdots, x_{\sigma(n)}) \cdot g_2(x_{\sigma(1)}, \cdots, x_{\sigma(n)})} \\ & = & \dfrac{f_1(x_{\sigma(1)}, \cdots, x_{\sigma(n)})}{g_1(x_{\sigma(1)}, \cdots, x_{\sigma(n)})} \cdot \dfrac{f_2(x_{\sigma(1)}, \cdots, x_{\sigma(n)})}{g_2(x_{\sigma(1)}, \cdots, x_{\sigma(n)})} \\ & = & \hat{\sigma}(r_1) \cdot \hat{\sigma}(r_2) \end{array}$$

Para mostrarmos a injetividade de $\hat{\sigma}$, suponha que $r_1(x_1, \cdots, x_n) \in Ker(\hat{\sigma})$. Mostraremos que $r_1(x_1, \cdots, x_n)$ é a função racional nula. De fato, por definição, existem $f_1(x_1, \cdots, x_n), g_1(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n]$, com $g_1 \neq 0$. Note que:

$$\begin{array}{rcc} \hat{\sigma}(r_1(x_1, \cdots, x_n)) & = & \hat{\sigma}\left(\dfrac{f_1(x_1, \cdots, x_n)}{g_1(x_1, \cdots, x_n)}\right) \\ & = & \dfrac{f_1(x_{\sigma(1)}, \cdots, x_{\sigma(n)})}{g_1(x_{\sigma(1)}, \cdots, x_{\sigma(n)})} \\ & = & 0 \end{array}$$

Ora, como $g_1(x_{\sigma(1)}, \cdots, x_{\sigma(n)}) \neq 0$, então nos resta que $f_1(x_{\sigma(1)}, \cdots, x_{\sigma(n)}) = 0$, $\forall x_{\sigma(1)}, \cdots, x_{\sigma(n)} \in L$. Logo, $f_1(x_1, \cdots, x_n) = 0$, $\forall x_1, \cdots, x_n \in L$. Portanto, r_1 é a função racional nula, e $Ker(\hat{\sigma}) = \{0\}$, o que prova a injetividade.

Para verificarmos a sobrejetividade, basta notarmos que, dado $r(x_{\sigma(1)}, \cdots, x_{\sigma(n)}) \in L$, é claro que existe $r(x_1, \cdots x_n) \in L$, tal que $\hat{\sigma}(r(x_1, \cdots, x_n)) = r(x_{\sigma(1)}, \cdots, x_{\sigma(n)})$, $\forall \sigma \in S_n$.

Com tudo que mostramos assim, fica demonstrado que distintas permutações de S_n induzem distintos automorfismos sobre as extensões de corpos consideradas. Podemos considerar o seguinte exemplo:

Exemplo 7.2.1. *Suponha que $\sigma \in S_n$ seja tal que $\sigma = (1234)$. Se $r(x_1, x_2, x_3, x_4) = \dfrac{5x_1^6 x_4}{x_2^5 + x_3}$, então*

$$\begin{aligned} \hat{\sigma}(r(x_1, x_2, x_3, x_4)) &= \frac{5x_{\sigma(1)}^6 x_{\sigma(4)}}{x_{\sigma(2)}^5 + x_{\sigma(3)}} \\ &= \frac{5x_2^6 x_1}{x_3^5 + x_4} \end{aligned}$$

Além disso, como já vimos, sendo $s_j(x_1, \cdots, x_n)$ um polinômio simétrico elementar qualquer, temos que $\sigma(s_j(x_1, \cdots x_n)) = s_j(x_{\sigma(x_1)}, \cdots, x_{\sigma(x)}) = s_j(x_1, \cdots, x_n)$, $\forall j \in \{1, \cdots, n\}$ e $\forall \sigma \in S_n$. Isto significa que o grupo simétrico S_n é um grupo de automorfismos.

Concluiremos com o Lema e com o Teorema abaixo que S_n é o grupo de automorfismos do corpo L.

Lema 7.2.1. *Seja $f \in K[x]$ com $\partial(f) = n \geq 1$. Então, existe uma extensão L de K tal que $[L : K] \leq n!$ em que f tem n raízes, isto é, L contém todas as raízes de f.*

Demonstração: Provaremos este Lema utilizando indução sobre o grau n de $f \in K[x]$.

Veja que se $\partial(f) = 1$, então neste caso, é óbvio que L contém todas as raízes de f e mais ainda, $[L : K] = 1 \leq 1!$. Agora, suponha que o resultado seja válido para polinômios com coeficientes em K e de grau p, onde $1 \leq p < n$. Mostraremos que se, $f \in K[x]$ é tal que $\partial(f) = n$, então o resultado também é verdadeiro.

Como $\partial(f) \geq 1$, então existe uma extensão finita $F \supset K$ tal que f tem uma raiz α_1 e $[F : K]] \leq \partial(f) = n$. Considerando-se $F[x]$, temos que

$$f(x) = (x - \alpha_1)q(x)$$

onde $q \in F[x]$ e $\partial(q) = n - 1$. Pela hipótese de indução, existe extensao $L \supset K$ tal que q tem $n - 1$ raízes com $[L : F] \leq (n - 1)!$. É claro que as raízes de f são α_1 e as mesmas de

q. Isto significa que em L, o polinômio f tem n raízes e, finalmente, pela Lei da Torre, segue-se que:

$$\begin{aligned} [L:K] &= [F:K][L:F] \\ &\leq n(n-1)! \\ &= n! \end{aligned}$$

■

Observação 7.2.1. *É importante ressaltar que o lema anterior garante, implicitamente, a existência de uma extensão normal K. E de forma equivalente, em corpos de característica zero, é sempre possível obtermos um corpo de decomposição.*

Teorema 7.2.1. *Sejam K um corpo com característica zero, $x_1, \cdots, x_n$ indeterminadas sobre K, $F = K(s_1, \cdots, s_n)$ onde s_i são os polinômios simétricos elementares em $x_1, \cdots, x_n$, e $f(x) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n \in F[x]$. Então $L = K(x_1, \cdots x_n) = Gal(f, F)$ e $S_n = Aut_F L$ a menos de isomorfismo.*

Demonstração: A demonstração pode ser encontrada em [4].

Para darmos continuidade ao trabalho e demonstrarmos a recíproca do Teorema 6.1.3, ainda precisamos de alguns conceitos fundamentais que veremos no capítulo seguinte.

8 Grupos de Galois de polinômios irredutíveis

Este capítulo é baseado nas referências [6] e [7]. Começaremos com um estudo a respeito de Discriminantes, e em seguida iremos generalizar os grupos de Galois para polinômios irredutíveis de grau $n \leq 4$.

8.1 Discriminantes

A partir de agora, trataremos de uma importante ferramenta para determinarmos características fundamentais sobre o grupo de Galois de um certo polinômio. Estamos familiarizados com o conceito de discriminantes de um polinômio quadrático, o qual é comumente denotado como Δ. Isto é, sendo $f(x) = ax^2 + bx + c \in K[x]$, com $K \subset \mathbb{Q}$, onde $a \neq 0$, então:

$$\Delta = b^2 - 4ac$$

O conceito que veremos a seguir, basicamente, trata-se de uma generalização do discriminante de um polinômio quadrático para um polinômio de grau arbitrário. Veremos mais adiante também que o discriminante permite determinarmos quando que o grupo de Galois consiste apenas de permutações pares.

É importante mencionar que, novamente, trataremos de corpos com característica zero, isto é, subcorpos de $\mathbb{C}$. Assim, considere $K = F[a]$ uma extensão normal do corpo F, e $f(x) = irr(F, a)$. Como vimos, o grupo de Galois $Aut_K F$ é isomorfo a algum subgrupo do grupo de permutações do conjunto de raízes de $f(x)$.

Como ressaltamos acima, iremos generalizar a noção de discriminante de um polinômio quadrático. Para isso, suponha que $f(x) = x^2+bx+c$. Sabemos que $\Delta = b^2-4ac$, e além disso, sendo r_1 e r_2 raízes de $f(x)$, então;

$$r_1 = \frac{1}{2}(-b + \sqrt{b^2 - 4c})$$

e

$$r_2 = \frac{1}{2}(-b - \sqrt{b^2 - 4c})$$

Agora, note que:

$$\begin{aligned} r_1 - r_2 &= \frac{1}{2}(-b + \sqrt{b^2 - 4c}) - \frac{1}{2}(-b - \sqrt{b^2 - 4c}) \\ &= \frac{1}{2}(\sqrt{b^2 - 4c}) + \frac{1}{2}(\sqrt{b^2 - 4c}) \\ &= \sqrt{b^2 - 4c} \end{aligned}$$

E portanto,

$$b^2 - 4c = (r_1 - r_2)^2$$

Definição 8.1.1. Sejam F um corpo e $f(x) \in F[x]$ um polinômio mônico. Sejam $r_1, \cdots, r_n$ as distintas raízes de f em algum corpo de decomposição K de f sobre F, e seja $\Delta = \prod_{i<j}(r_i - r_j) \in K$. Então, definimos como o discriminante de f ou apenas $disc(f)$ o elemento

$$D = \Delta^2 = \prod_{i<j}(r_i - r_j)^2$$

Definição 8.1.2. Sejam K uma extensão algébrica de F e $\alpha \in K$. Então definimos como $disc(\alpha) = disc(irr(F, \alpha))$.

Observação 8.1.1. *Devemos observar que:*

- *Embora $\alpha \in K$, o elemento $disc(\alpha)$ depende do corpo base F. Porque $disc(\alpha)$ é função das raízes de $irr(\alpha, F)$, o qual tem coeficientes em F.*
- *O elemento Δ depende da indexação das raízes de $f(x)$. Sendo assim, com uma indexação diferente obteríamos $-\Delta$.*
- *Se $f(x) \in F[x]$, então $D = disc(f) = 0$ se, e somente se, $r_i = r_j$, para $i \neq j$.*

Pelo último item da observação anterior, notemos também que este possui certa limitação, uma vez que precisamos que não haja raízes repetidas em $f(x)$. O lema a seguir estabelece uma relação importante entre o grupo de Galois de $f(x)$ e seu discriminante.

Lema 8.1.1. *Sejam $f(x) \in F[x]$ um polinômio irredutível e $K = Gal(f, F)$. Então, $\sigma \in Aut_F K$ é uma permutação par se, e somente se, $\sigma(\Delta) = \Delta$ e σ é impar se, e somente se, $\sigma(\Delta) = -\Delta$. Além disso, $disc(f) \in F$.*

Demonstração: Primeiro, lembre que toda permutação de S_n pode ser obtida como produto de transposições. Agora, considere $h(x) = \prod_{i<j}(x_i - x_j)$ e suponha, sem perda de generalidade, que $\sigma \in S_n$ seja a transposição (ij), com $i < j$. Neste caso, σ permuta apenas os fatores que dependem dos índices i e j e os demais são mantidos fixos. Dada a construção de $h(x)$ e os índices i e j fixados, são possíveis os seguintes fatores no produtório:

1. $(x_i - x_j)$;
2. $(x_k - x_i)$, $(x_k - x_j)$ para $k < i$.
3. $(x_i - x_l)$, $(x_j - x_l)$ para $j < l$.
4. $(x_i - x_m)$, $(x_m - x_j)$ para $i < m < j$

Vamos analisar cada caso:

1. Note que $\sigma(x_i - x_j) = x_j - x_i = -(x_i - x_j)$

2. $\sigma(x_k - x_i) = (x_k - x_j)$ e $\sigma(x_k - x_j) = (x_k - x_i)$. Além disso, $\sigma(x_i - x_l) = (x_j - x_l)$ e por fim, $\sigma(x_j - x_l) = (x_j - x_l)$.

3. Análogo ao caso anterior.

4. E, $\sigma(x_i - x_m) = x_j - x_m = -(x_m - x_j)$. E finalmente, $(x_m - x_j) = x_m - x_i = -(x_i - x_m)$.

Multiplicando-se todos os termos acima, obtemos $\sigma(h) = -h$. Logo, da arbitrariedade de $\sigma \in S_n$, temos que $\sigma(h) = h$ se, e somente se, σ for o produto de uma quantidade par de transposições. Analogamente, $\sigma(h) = -h$ se, e somente se, σ for o produto de uma quantidade impar de transposições. Portanto, para concluirmos o resultado, basta substituirmos x_i, x_j por r_i e r_j respectivamente.

Finalmente, observe que $disc(f) \in F$, o que sai por uma conta simples. Observe que, dado $\sigma \in Aut_F K$, temos:

$$\begin{aligned} \sigma(\Delta^2) &= \sigma(\Delta\Delta) \\ &= \sigma(\Delta)\sigma(\Delta) \\ &= \Delta^2 \end{aligned}$$

Isto mostra que $disc(f)$ é fixado por $\sigma \in S_n$, e portanto, $disc(f) \in F$.

■

Corolário 8.1.1. *Sejam F, K e $f(x)$ seguindo as mesmas hipóteses do lema anterior, e $GG = Aut_F K$ o grupo de Galois de $f(x)$. Então, $G \subset A_n$ se, e somente se, $disc(f) = a^2$, para algum $a \in F$. Além disso, o corpo $F[\Delta] \subset K$ corresponde ao subgrupo $G \cap A_n$ de G.*

Demonstração: A demonstração pode ser consultada em [6].

Como vimos até aqui, precisamos conhecer as raízes do polinômio para calcularmos seu discriminante. Entretanto, calcular as raízes de um polinômio é algo relativamente complicado. Contornaremos esse problema com as próximas definições.

Definição 8.1.3. Sejam K um corpo e $\alpha_1, \alpha_2, \cdots, \alpha_n \in K$. Definimos a chamada Matriz de Vandermonde como sendo a matriz quadrada de ordem n dada por:

$$V(\alpha_1, \cdots, \alpha_n) = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{bmatrix}$$

Lema 8.1.2. *Sejam K um corpo e $\alpha_1, \alpha_2, \cdots, \alpha_n \in K$. Então o determinante da Matriz de Vandermonde é $\prod_{i<j}(\alpha_j - \alpha_i)$. Além disso, se $f(x) \in F[x]$ tem raízes $\alpha_1, \alpha_2, \cdots, \alpha_n \in K$, onde $K \supset F$, então o discriminante de $f(x)$ é dado por $det(V(\alpha_1, \cdots, \alpha_n))^2$.*

Demonstração: Consideremos por comodidade $A = V(\alpha_1, \cdots, \alpha_n)$. Primeiro, observe que se $\alpha_i = \alpha_j$ com $i \neq j$, então $det(A) = 0$ e a fórmula é verdadeira neste caso. Assim, assumiremos que α_i são distintos e provaremos o resultado por indução sobre n.

Note que se $n = 1$, não há o que provar. Admitiremos como hipótese de indução que o resultado seja válido para $n - 1$ e provaremos que vale para n.

Suponha que $n > 1$ e considere $h(x) = det(V(\alpha_1, \alpha_2, \cdots, \alpha_{n-1}, x))$. Por construção, $h(x)$ é um polinômio de grau igual a $n - 1$. Temos que:

$$h(x) = \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \\ 1 & x & x^2 & \cdots & x^{n-1} \end{vmatrix}$$

Ao expandirmos o cálculo deste determinante pela última linha, fica fácil perceber que o coeficiente do termo de maior grau é dado por $det(V(\alpha_1, \cdots, \alpha_{n-1}))$. Além disso, fixado $i \in \{1, \cdots, n-1\}$, pelas propriedades básicas de determinante, temos que:

$$h(\alpha_i) = det(V(\alpha_1, \cdots, \alpha_{n-1}, \alpha_i)) = 0$$

Isto significa que $h(x)$ é divisível por cada $x - \alpha_i$, ou seja, α_i é raiz de $h(x)$, para todo $i \in \{1, \cdot, n-1\}$. Como estamos supondo α_i distintos, então $h(x)$ tem $n - 1$ fatores lineares distintos. Isto é:

$$h(x) = c(x - \alpha_1) \cdots (x - \alpha_{n-1})$$

onde $c = det(V(\alpha_1, \cdots, \alpha_{n-1}))$.

Agora, avaliando-se $h(x)$ em α_n e usando a hipótese de indução, temos que:

$$\begin{aligned} h(\alpha_n) &= det(V(\alpha_1, \cdots, \alpha_n)) \\ &= \prod_{i<j\leq n-1} (\alpha_j - \alpha_i) \prod_{i<n} (\alpha_n - \alpha_i) \\ &= \prod_{i<j} (\alpha_j - \alpha_i) \end{aligned}$$

Isto prova que $det(V(\alpha_1, \cdots, \alpha_n)) = \prod_{i<j} (\alpha_j - \alpha_i)$. E consequentemente, a segunda afirmação, segue diretamente da própria definição de discriminante.

■

Agora, veremos que o cálculo do discriminante de um polinômio pode ser realizado sem a necessidade de obter suas raízes. Seja $A = V(\alpha_1, \cdots, \alpha_n)$. Temos que:

$$det(A)^2 = det(A)det(A) = det(A)det(A^t) = det(AA^t)$$

Veja que:

$$A^tA = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \alpha_3^{n-1} & \cdots & \alpha_n^{n-1} \end{bmatrix} \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{bmatrix}$$

$$= \begin{bmatrix} t_0 & t_1 & t_2 & \cdots & t_{n-1} \\ t_1 & t_2 & t_3 & \cdots & t_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ t_{n-1} & t_n & t_{n+1} & \cdots & t_{2n-2} \end{bmatrix}$$

onde $t_i = \sum_j \alpha_j^i$, para $i \geq 1$ e $t_0 = n$. Todo esse cálculo é interessante, pois, sendo $\alpha_1, \cdots, \alpha_n$ as raízes de um polinômio $f(x)$, existem relações recursivas entre t_i e os coeficientes de $f(x)$. Tais relações são chamadas identidades de Newton e auxiliam bastante no cálculo do discriminante, conforme veremos mais adiante. O próximo resultado relaciona as entradas da matriz A^tA com os coeficientes do polinômio $f(x)$, e auxiliará nos cálculos de discriminantes.

Teorema 8.1.4 (Identidades de Newton)**.** *Seja $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$ um polinômio mônico sobre F com as raízes $\alpha_1, \cdots, \alpha_n$. Se $t_i = \sum_j \alpha_j^i$, então $t_m + a_{n-1}t_{m-1} + \cdots a_{n-m+1}t_1 + ma_{n-m} = 0$ para $m \leq n$ e $t_m + a_{n-1}t_{m-1} + \cdots + a_0t_{m-n} = 0$ para $m > n$.*

Demonstração: A demonstração pode ser encontrada em [6].

Exemplo 8.1.1. *Seja $f(x) = x^2 + bx + c$. Observe que $t_0 = 2$. A identidade de Newton nos diz $t_1 + b = 0$, então $t_1 = -b$. Para t_2, temos $t_2 + bt_1 + 2c = 0$, daí $t_2 = -bt_1 - 2c = b^2 - 2c$. Portanto, conforme deduzimos, obtemos:*

$$disc(f) = \begin{vmatrix} t_0 & t_1 \\ t_1 & t_2 \end{vmatrix} = \begin{vmatrix} 2 & -b \\ -b & b^2 - 2c \end{vmatrix} = 2b^2 - 4c - b^2 = b^2 - 4c$$

Exemplo 8.1.2. *Seja $f(x) = x^3 + px + q$. Pelas identidades de Newton, temos $t_1 = 0$, $t_2 = -2p$, $t_3 = -3q$, $t_4 = 2p^2$.*

$$disc(f) = \begin{vmatrix} t_0 & t_1 & t_2 \\ t_1 & t_2 & t_3 \\ t_2 & t_3 & t_4 \end{vmatrix} = \begin{vmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{vmatrix} = -12p^3 - (-8p^3 + 27q^2) = -4p^3 - 27q^2$$

Exemplo 8.1.3. *Consideremos agora o caso geral de um polinômio de grau 3. Seja $f(x) = x^3 + bx^2 + cx + d \in \mathbb{Q}[x]$. Pelas identidades de Newton, temos: $t_0 = 3$ e $t_1 = -b$. Utilizando-se novamente a identidades de Newton, encontramos: $t_2 = b^2 - 2c$, $t_3 = -b^3 + 3bc - 3d$ e*

$t_4 = b^4 - 4b^2c + 4bd + 2c^2$. *Agora, calculando o determinante, temos:*

$$disc(f) = \begin{vmatrix} t_0 & t_1 & t_2 \\ t_1 & t_2 & t_3 \\ t_2 & t_3 & t_4 \end{vmatrix} = t_0t_2t_4 + t_1t_2t_3 + t_1t_2t_3 - t_2^3 - t_0t_3^2 - t_4t_1^2$$
$$= b^2c^2 + 18bcd - 27d^2 - 4b^3d - 4c^3$$

8.2 Grupos de Galois

Anteriormente, vimos que o grupo de Galois nada mais é do que um grupo de automorfismos sobre a operação composição de funções. Dada uma extensão $L \supset K$ finitamente gerada, através do estudo da ação do Grupo de Galois $Aut_K L$ sobre sua base, vimos que diferentes automorfismos induzem diferentes permutações no grupo simétrico S_n, onde $n = [L : K]$. Aqui será visto que grupos de Galois de polinômios irredutíveis possuem uma característica importante, e portanto, nosso objetivo aqui será caracterizar os grupos de Galois para tais tipos de polinômios.

Logo abaixo, provaremos que o grupo de Galois de um certo polinômio $f(x) \in K[x]$ com $L = Gal(f, K)$ é isomorfo a algum subgrupo de S_n. Isto é, a proposição abaixo prova que para cada indexação escolhida no conjunto de raízes $\{r_1, \cdots, r_n\}$ de um certo polinômio separável, conseguimos um homomorfismo injetor de $Aut_K L$ em S_n.

Mas antes de enunciarmos o próximo resultado, relembremos que a definição de um polinômio separável foi enunciada na Definição 3.2.1.

Proposição 8.2.1. *Sejam $f \in K[x]$ um polinômio separável de grau $n \geq 1$, $L = Gal(f, K)$, e $r_1, \cdots r_n$ as raízes de f. Então existe um homomorfismo injetor entre $Aut_K L$ e S_n.*

Demonstração: Fixado um índice $j \in \{1, \cdots n\}$ e $\sigma \in Aut_K L$ arbitrários, defina:

$$\begin{array}{rccc} \Phi\colon & Aut_K L & \longrightarrow & S_n \\ & \sigma(r_j) & \longmapsto & \Phi(\sigma(r_j)) \end{array}$$

onde $\Phi(\sigma(r_j)) = \Phi(r_{\sigma(j)}) = \sigma(j)$.

Provaremos primeiro que Φ é homomorfismo. Sejam σ, $\tau \in Aut_K L$, com $j \in \{1, \cdots, n\}$ fixado, suponha que $\pi(r_j) = \sigma(r_j) \circ \tau(r_j)$. Então temos que:

$$\begin{aligned} \Phi(\sigma(r_j) \circ \tau(r_j)) &= \Phi(\pi(r_j)) \\ &= \Phi(r_{\pi(j)}) \\ &= \pi(j) \\ &= \sigma(j) \circ \tau(j) \\ &= \Phi(r_{\sigma(j)}) \circ \Phi(r_{\tau(j)}) \\ &= \Phi(\sigma(r_j)) \circ \Phi(\tau(r_j)) \end{aligned}$$

Agora mostraremos que vale a injetividade para Φ. De fato, suponha que $\Phi(\sigma(r_j)) = \Phi(\tau(r_j))$. Usando a definição de Φ, temos: $\Phi(\sigma(r_j)) = \sigma(j)$ e $\Phi(\tau(r_j)) = \tau(j)$. Pela hipótese, segue-se que $\sigma(j) = \tau(j)$, $\forall j \in \{1, \cdots, n\}$. Portanto, $\sigma = \tau$, como queríamos.

■

Corolário 8.2.1. *Admitindo-se as hipóteses da proposição anterior, $Aut_K L$ é isomorfo a algum subgrupo de S_n.*

Demonstração: Como Φ é um homomorfismo injetor de $Aut_K L$ em S_n. Então, o Teorema dos Isomorfismos garante que

$$\frac{Aut_K L}{Ker\Phi} \simeq \Phi(Aut_K L) \leq S_n$$

Além disso, como $Ker\Phi = \{id\}$, segue-se o resultado que queríamos.

■

Como dissemos no início deste capítulo, existe uma característica do grupo de Galois de polinômios irredutíveis, a qual mencionaremos no teorema a seguir.

Teorema 8.2.1. *Seja $f(x) \in K[x]$ um polinômio irredutível de grau n, tal que $L = Gal(f, K)$. Então n divide $|Aut_K L|$. Além disso, $f(x)$ é irredutível em $K[x]$ se, e somente se, $Aut_K L$ é um subgrupo transitivo de S_n.*

Observação 8.2.1. *Neste enunciado, estamos considerando fortemente o fato de que $Aut_K L$ é isomorfo a algum subgrupo de S_n.*

Demonstração do Teorema 8.2.1: Seja r uma raiz de f em K. Considere $f(x) = irr(r, K)$. Pela Lei da Torre, $[K[r] : K] = n$ será um fator do grau da extensão $L \supset K$. Como tal extensão é normal, então $[L : K] = |Aut_K L|$. Logo, $|Aut_K L| = [L : K] = [Gal(f, K) : K][K[r] : K] = k \cdot n$, para algum $k \in \mathbb{Z}$. Portanto, n divide $|Aut_K L|$.

Agora, suponhamos que r_i e r_j sejam duas raízes de $f(x)$. Sabemos que $r_j = \sigma(r_i)$ para algum $\sigma \in Aut_K L$. Consequentemente, a menos de isomorfismo, $Aut_K L$ como subgrupo de S_n permuta i com j. Da arbitrariedade de i e j, segue-se que $Aut_K L$ é um grupo transitivo.

Reciprocamente, suponha por absurdo que $f(x)$ seja redutível. Como estamos supondo que $f(x)$ é separável, então existem $g_1(x), \cdots g_n(x) \in K[x]$ tais que $g_i(r_i) = 0$, $\forall i \in \{1, \cdots, n\}$ e com

$$f(x) = \prod_{i=1}^{n} g_i(x)$$

Além disso, $g_i(x) = irr(r_i, K)$ e $g_j(x) = irr(r_j, K)$. Para cada $\sigma \in Aut_K L$, $\sigma(r_i)$ tem o mesmo polinômio minimal sobre K que r_i. Logo $\sigma(r_i) \neq r_j$, e por isso, $Aut_K L$ não é transitivo, o que é uma contradição.

■

Iremos agora caracterizar os grupos de Galois dos polinômios irredutíveis de grau $n \leq 4$, considerando-se sempre coeficientes racionais.

8.2.1 Polinômio de grau 1

Considere $f(x) \in K[x]$ tal que $\partial(f(x)) = 1$. É claro que $f(x)$ é irredutível sobre K. Observe que, como $\partial(f(x)) = 1$, então se α é raiz de $f(x)$, então $\alpha \in K$. Logo $L = K$, e $[L : K] = 1$.

Pelo Teorema Fundamental da Teoria de Galois, $[L : K] = |G| = 1$. Portanto, $Aut_K L \simeq S_1 = \{id\}$.

8.2.2 Polinômio de grau 2

Suponhamos que $f(x)$ seja um polinômio irredutível sobre $K[x]$, tal que $f(x) = x^2 + bx + c \in K[x]$. Note que $L = K[\alpha]$, onde $\alpha = \dfrac{-b \pm \sqrt{b^2 - 4c}}{2}$. Como $\alpha \notin K$ é uma raiz de $f(x)$, temos que $f(x) = irr(\alpha, K)$. Daí, $[L : K] = |G| = 2$. Logo, nos resta que $Aut_K L \simeq S_2$, pois S_2 é o único subgrupo a menos de isomorfismo de ordem 2.

8.2.3 Polinômios de grau 3

Considere $f(x) \in K[x]$ um polinômio irredutível de grau 3, onde $K \supset \mathbb{Q}$. Nosso objetivo aqui é caracterizar o grupo de Galois destes polinômios. Para isso, precisamos de alguns resultados importantes.

Teorema 8.2.2. *Sejam $K \supset \mathbb{Q}$ e $f(x) \in K[x]$ irredutível. Se r_1, r_2, r_3 são as distintas raízes de $f(x)$, então $Gal(f, K) = K[r_1, r_2, r_3] = K[r_1, \sqrt{D}]$, onde D é o discriminante de $f(x)$.*

Demonstração: Podemos assumir sem perda de generalidade que $f(x) = x^3 - s_1 x^2 + s_2 x - s_3$. Denotando-se $L = Gal(f, K)$, temos em L:

$$f(x) = (x - r_1)(x - r_2)(x - r_3)$$

onde $s_1 = r_1 + r_2 + r_3$, $s_2 = r_2 r_1 + r_1 r_3 + r_2 r_3$, e $s_3 = r_1 r_2 r_3$. Agora, observe que, como $s_1 \in K$ e $s_1 = r_1 + r_2 + r_3$, então $r_3 = s_1 - r_1 - r_2 \in K[r_1, r_2]$. Logo, $L = K[r_1, r_2, r_3] = K[r_1, r_2]$,

donde:

$$K \subset K[r_1] \subset K[r_1, r_2] = L$$

Como $f(x)$ é irredutível em K, então $f(x) = irr(r_1, K)$, o que nos garante que $[K[r_1] : K] = 3$.

Observe que em $K[r_1]$, tem-se:

$$f(x) = (x - r_1)q(x)$$

Se $q(x)$ for irredutível sobre K, então, $q(x) = irr(r_2, K[r_1])$. E portanto,

$$\begin{aligned} [L : K] &= [L : K[r_1]][K[r_1] : K] \\ &= 2 \cdot 3 \\ &= 6 \end{aligned}$$

Agora, se $q(x)$ for redutível sobre K, teremos que $r_2, r_3 \in K[r_1]$, donde $L = K[r_1]$ e consequentemente,

$$[L : K] = [K[r_1] : K] = 3$$

Logo, as possibilidades para $|Aut_K L|$ são 3 ou 6.

Por definição, $D = (r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2$, e por comodidade, consideremos $D = \Delta^2$. Note que $\Delta \in L$ sempre, mas não necessariamente $\Delta \in K$, embora seja sempre verdade que $\Delta^2 \in K$, uma vez que o discriminante também é obtido como função dos coeficientes de $f(x)$.

Se $\Delta \in K$, então não há o que provar. Assim, suponha que $\Delta = \sqrt{D} \notin K$. e considere o polinômio $g(x) = x - \delta^2 \in K[r_1]$. É claro que $g(x) = irr(\Delta, K[r_1])$, e assim, $[K[r_1, \Delta] : K[r_1]] = 2$, e portanto,

$$\begin{aligned} [K[r_1, \Delta] : K] &= [K[r_1, \Delta] : K[r_1]][K[r_1] : K] \\ &= 2 \cdot 3 \\ &= 6 \end{aligned}$$

Pela unicidade do corpo de decomposição, segue-se portanto, que $L = K[r_1, \Delta]$, como queríamos.

■

O próximo teorema estabelece todos os critérios para determinarmos o grupo de Galois de um polinômio irredutível de grau 3.

Teorema 8.2.3. *Seja $f(x) \in K[x]$ um polinômio irredutível de grau $n = 3$ com $L = Gal(f, K)$. Considerando-se a notação já estabelecida para o discriminante de $f(x)$:*

1. *$\sqrt{D} = \Delta \in K$ se, e somente se, $Aut_K L \simeq A_3$.*

2. $\sqrt{D} = \Delta \notin K$ *se, e somente se,* $Aut_K L \simeq S_3$.

Demonstração: Suponha que $f(x) = f(x) = x^3 + bx^2 + cx + d$ e r_1, r_2, r_3 sejam suas raízes. Como f é separável (pois é irredutível), então temos $\Delta \neq 0$. Conforme já calculamos no Exemplo 8.1.3, temos:

$$D = \Delta^2 = b^2c^2 + 18bcd - 27d^2 - 4b^3d - 4c^3 \in K$$

1. Suponha que $\Delta \in K$. Como f é irredutível sobre K, então, digamos, $r_1 \notin K$. Logo, $[K[r_1] : K] = 3$, pois $f(x) = irr(r_1, K)$. Pelo Teorema anterior, temos que $L = K[r_1, \Delta]$. Mas como $\Delta \in K$, então $L = K[r_1]$, e assim, $[L : K] = |Aut_K L| = 3$. Como $Aut_K L$ é isomorfo a algum subgrupo de S_3, e o único subgrupo de S_3 de ordem 3 é A_3, segue-se o resultado.

2. Suponha que $\Delta \notin K$. Como f é irredutível então, novamente, suponha que $r_1 \notin K$. Como $\Delta^2 \in K$, podemos considerar o polinômio minimal $irr(\Delta, K[r_1]) = x^2 - \Delta^2$, de forma que $[K[r_1, \Delta] : K] = [[Kr_1, \Delta] : K[r_1]][K[r_1] : K] = 2 \cdot 3 = 6$. Como o único subgrupo de S_3 que possui ordem 6 é o próprio S_3, segue-se o resultado que queríamos.

■

A figura abaixo representa o diagrama do grupo S_3 com seus subgrupos, onde A_3 é o grupo das permutações pares e C_2 o grupo cíclico de ordem 2. O segmento destacado de vermelho representa a cadeia de solubilidade do grupo.

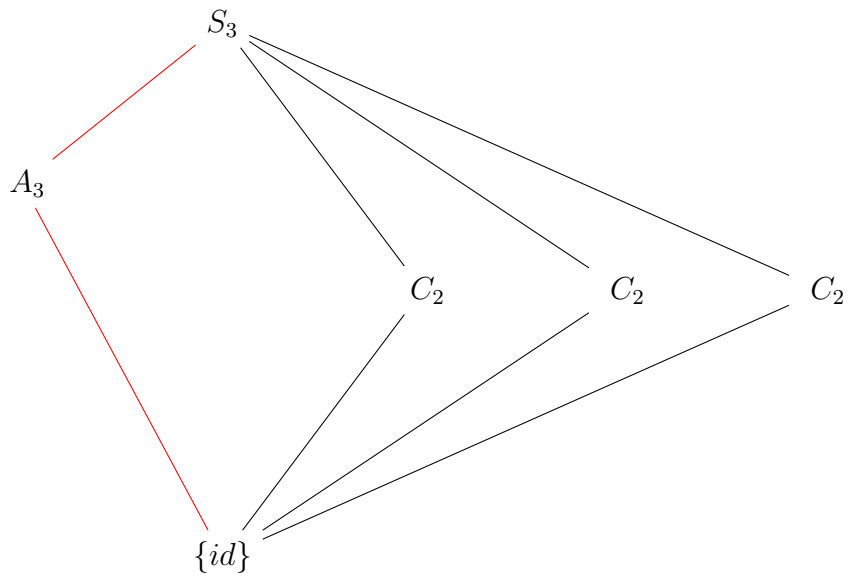

Figura 12 – Diagrama do grupo simétrico S_3.

Exemplo 8.2.1. *Seja $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Note que $f(x)$ é irredutível sobre $\mathbb{Q}$. Vamos calcular $disc(f)$ a partir da fórmula desenvolvida no Exemplo 8.1.3. Temos que*

$$disc(f) = 0 + 18.0 - 27(-2)^2 - 4(0)^3 2 - 4.0 = -108$$

Logo, $\sqrt{disc(f)} = 6\sqrt{-3} \notin \mathbb{Q}$. Como $disc(f)$ não é um quadrado perfeito, pelo Teorema 8.2.3, seu grupo de Galois G é tal que $G \simeq S_3$.

Exemplo 8.2.2. *Seja $g(x) = x^3 - 3x - 1 \in \mathbb{Q}[x]$. Pelo Critério de Eisenstein, temos que g é irredutível sobre $\mathbb{Q}$. Calculando-se o discriminante de $g(x)$, temos:*

$$disc(g) = 0(-3)^2 + 18.0.(-3)(-1) - 27(-1)^2 - 4(0)^3(-1) - 4(-3)^3 = -27 + 108 = 81$$

Como 81 é um quadrado perfeito, então pelo Teorema 8.2.3, o grupo de Galois de $g(x)$ é G tal que $G \simeq A_3$.

Exemplo 8.2.3. *Seja $h(x) = x^3 - 4x + 2 \in \mathbb{Q}[x]$. Pelo Critério de Eisenstein, temos que h é irredutível sobre $\mathbb{Q}$. Calculando-se o discriminante de $h(x)$, temos:*

$$disc(h) = 0(-4)^2 + 18(0)(-4)(2) - 27(2)^2 - 4(0)^3(2) - 4(-4)^3 = -108 + 256 = 148$$

Logo, $\sqrt{disc(h)} = 2\sqrt{37} \notin \mathbb{Q}$, e portanto, o grupo de Galois de $h(x)$ é isomorfo a S_3.

8.2.4 Polinômios de grau 4

A figura abaixo representa o diagrama do grupo S_4 com todos os seus subgrupos. Observe que a complexidade deste grupo é bem maior do que a do grupo S_3.

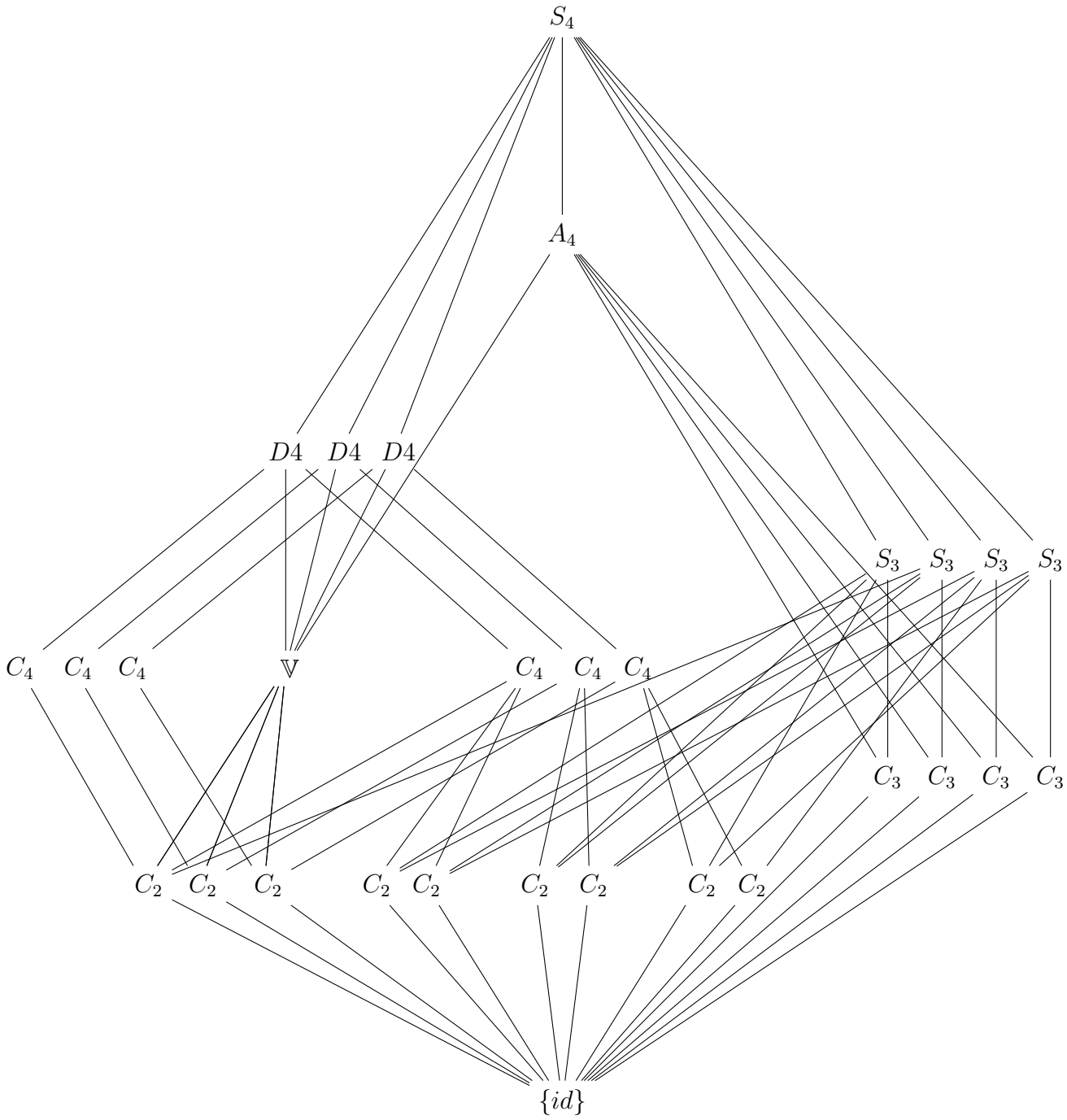

Figura 13 – Diagrama do grupo Simétrico S_4.

Seja $f(x) = x^4 + ax^3 + bx^2 + cx + d \in F[x]$ um polinômio irredutível de grau 4, e suponha que suas raízes sejam r_1, r_2, r_3 e r_4. Para estudarmos o grupo de Galois deste polinômio, precisamos definir um polinômio de grau 3 associado. Para isso, considere: $\beta_1 = r_1r_2 + r_3r_4$, $\beta_2 = r_1r_3 + r_2r_4$ e $\beta_3 = r_1r_4 + r_2r_3$.

Definição 8.2.4. O polinômio de grau 3 associado ao polinômio $f(x)$, definido como $r(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3)$ é chamado de cúbica resolvente de $f(x)$.

Observe que embora $r(x)$ tenha sido definido em termos de $\beta_1, \beta_2, \beta_3$, $r(x)$ pode ser escrito em função dos coeficientes de $f(x)$, isto é, $r(x) \in F[x]$. De fato, temos que: $r(x) = (x-\beta_1)(x-\beta_2)(x-\beta_3) = (x - r_1r_2 - r_3r_4)(x - r_1r_3 - r_2r_4)(x - r_1r_4 - r_2r_3) = (x^2 - r_1r_3x - r_2r4x + r_1^2r_2r_3 + r_1r_2^2r_4 - r_3r_4x + r_1r_3^2r_4 + r_2r_3r_4^2)(x - r_1r_4 - r_2r_3) = x^3 - r_1r_4x^2 - r_2r_3x^2 - r_1r_3x^2 + r_1^2r_3r_4x + r_1r_2r_3^2x - r_2r_4x^2 + r_1r_2r_4^2x + r_2^2r_3r_4x - r_1r_2x^2 + r_1^2r_2r_4x + r_1r_2^2r_3x + r_1^2r_2r_3x - r1_3r_2r_3r_4^2 - r_1^2r_2^2r_3^2 + r_1r_2^2r_4x - r_1^2r_2^2r_4^2 - r_1r_2^3r_3r_4 - r_3r_4x^2 + r_1r_3r_4^2x + r_2r_3^2r_4x + r_1r_3^2r_4x - r_1^2r_3^2r_4^2 - r_1r_2r_3^3r_4 + r_2r_3r_4^2x - r_1r_2r_3r_4^3 - r_2^2r_3^2r_4^2 = x^3 - (r_1r_4 + r_2r_3 + r_1r_3 + r_2r_4 + r_1r_2 + r_3r_4)x^2 + (r_1^2r_3r_4 + r_1r_2r_3^2 + r_1r_2r_4^2 + r_2^2r_3r_4 + r_1^2r_2r_4 + r_1r_2^2r_3 + r_1^2r_2r_3 + r_1r_2^2r_4 + r_1r_3r_4^2 + r_2r_3^2r_4 + r_1r_3^2r_4 + r_2r_3r_4^2)x - r_1^3r_2r_3r_4 - r_1^2r_2r_3^2 - r_1^2r_2^2r_4^2 - r_1r_2^3r_3r_4 - r_1^2r_3^2r_4^2 - r_1r_2r_3^3r_4 - r_1r_2r_3r_4^3 - r_2^2r_3^2r_4^2 = x^3 - bx^2 + (ac - 4d)x + 4bd - a^2d - c^2$. Portanto, $r(x) = x^3 - bx^2 + (ac-4d)x + 4bd - a^2d - c^2 \in F[x]$.

Uma outra observação importante também é que a cúbica resolvente $r(x)$ possui o mesmo discriminante de $f(x)$. De fato,

$$\begin{aligned}
disc(r) &= (\beta_1-\beta_2)^2(\beta_1-\beta_3)^2(\beta_2-\beta_3)^2 \\
&= (r_1r_2 + r_3r_4 - r_1r_3 - r_2r_4)^2(r_1r_2 + r_3r_4 - r_1r_4 - r_2r_3)^2(r_1r_3 + r_2r_4 - r_1r_4 - r_2r_3)^2 \\
&= (r_1(r_2-r_3) - r_4(r_2-r_3))^2(r_1(r_2-r_4) - r_3(r_2-r_4))^2(r_1(r_3-r_4) - r_2(r_3-r_4))^2 \\
&= (r_1-r_2)^2(r_1-r_3)^2(r_1-r_4)^2(r_2-r_3)^2(r_2-r_4)^2(r_3-r_4)^2 \\
&= disc(f)
\end{aligned}$$

Vimos anteriormente pelo Teorema 8.2.1 que como $f(x)$ é um polinômio irredutível, então seu grupo de Galois age transitivamente sobre o conjunto de suas raízes. Assim, pelo Corolário 8.2.1, basta encontrarmos os subgrupos transitivos de S_4 e estabelecer as condições para determinarmos o grupo de Galois de $f(x)$.

O teorema seguinte estabelece parâmetros para determinarmos o grupo de Galois de um polinômio irredutível $f(x) \in F[x]$ de grau 4 em termos de seu discriminante e de sua cúbica resolvente $r(x)$.

Teorema 8.2.5. *Suponha que $[L:F] = m$. Então as seguintes equivalências são verdadeiras:*

1. *$G \simeq S_4$ se, e somente se, $r(x)$ for irredutível sobre F e $\sqrt{D} \notin F$.*
2. *$G \simeq A_4$ se, e somente se, $r(x)$ for irredutível sobre F e $\sqrt{D} \in F$.*
3. *$G \simeq \mathbb{V}$ se, e somente se, $r(x)$ se fatorar linearmente sobre F*
4. *$G \simeq C_4$ (o grupo cíclico de ordem 4) se, e somente se, $r(x)$ possuir uma única raiz $t \in F$ e $h(x) = (x^2 - tx + d)(x^2 + ax + (b-t))$ se fatorar linearmente sobre L, se e somente se, $m = 2$ e $f(x)$ for redutível sobre L.*

5. $G \simeq D_4$ *(o grupo diedral) se, e somente se,* $r(x)$ *possuir uma única raiz* $t \in F$ *e* $h(x)$ *não se fatorar linearmente em* L*, se e somente se,* $m = 2$ *e* $f(x)$ *for irredutível sobre* L*.*

Demonstração: A demonstração pode ser encontrada em [6].

Exemplo 8.2.4. *Considere o polinômio* $f(x) = x^4 - 4x^3 + 4x^2 + 6 \in \mathbb{Q}[x]$*. Aqui temos os coeficientes* $a = -4$*,* $b = 4$*,* $c = 0$ *e* $d = 6$*. E a cúbica resolvente associada é dada por* $r(x) = x^3 - 4x^2 + (-4 \cdot 0 - 4 \cdot 6)x + 4(4)6 - 16 \cdot 6 = x^3 - 4x^2 - 24x = x(x^2 - 4x - 24)$*. As raízes de* $r(x)$ *são* $\beta_1 = 0$*,* $\beta_2 = 2 + 2\sqrt{7}$ *e* $\beta_3 = 2 - 2\sqrt{7}$*. Assim, temos que* $Gal(r(x), \mathbb{Q}) = \mathbb{Q}[\sqrt{7}]$*. Agora, de acordo com o Teorema 8.2.5, temos que* $t = 0 \in \mathbb{Q}$ *e:*

$$h(x) = (x^2 - tx + d)(x^2 + ax + (b - t)) = (x^2 + 6)(x^2 - 4x + 4)(x^2 + 6)(x - 2)^2$$

Note que $h(x)$ *não se fatora linearmente sobre* $\mathbb{Q}$*, portanto, pelo Teorema 8.2.5, temos que o grupo de Galois de* $f(x)$ *é isomorfo a* D_4*.*

Exemplo 8.2.5. *Seja* $f(x) = x^4 - t \in \mathbb{Q}[x]$*. Temos os coeficientes* $a = 1$*,* $b = c = 0$ *e* $d = t$*. Assim, a cúbica resolvente associada é dada por* $r(x) = x^3 + 4tx = x(x^2 + 4t)$*. Observe que se* $\sqrt{-t} \notin Q$*, então* $r(x)$ *tem exatamente uma raíz em* $\mathbb{Q}$*. Além disso, o polinômio associado* $h(x) = x^2(x^2 + l)$ *não se fatora linearmente sobre* $\mathbb{Q}$*, e pelo Teorema 8.2.5, segue que o grupo de Galois de* $f(x)$ *é isomorfo a* D_4*. Agora se* $\sqrt{-t} \in \mathbb{Q}$*, então ainda pelo Teorema 8.2.5, o grupo de Galois de* $f(x)$ *será isomorfo ao grupo de Klein,* $\mathbb{V}$*.*

Exemplo 8.2.6. *Seja* $p \in \mathbb{N}$ *um número primo e considere* $f(x) = x^4 + px + p$*. Temos os coeficientes:* $a = b = 0$*,* $c = d = p$*. Assim, a cúbica resolvente associada é dada por* $r(x) = x^3 - 4px - p^2$*. Vamos analisar as possibilidades para as raízes de* $r(x)$*. Observe que em* $\mathbb{Q}$ *é suficiente testarmos para os números* ± 1*,* $\pm p$ *e* $\pm p^2$*. Donde* $r(\pm 1) \neq 0$ *e* $r(\pm p^2) \neq 0$*. Assim, temos que:*

1. $r(p) = p^3 - 4p^2 - p^2 = p^3 - 5p^2 = p^2(p - 5)$
2. $r(-p) = -p^3 + 4p^2 - p^2 = -p^3 + 3p^2 = p^2(3 - p)$

Assim, fica evidente que para $p \neq 3$ *e* $p \neq 5$*, a cúbica resolvente* $r(x)$ *não possui raízes em* $\mathbb{Q}$ *e portanto será irredutível sobre* $\mathbb{Q}$*. Em relação ao discriminante* D *de* $r(x)$*, observe ainda que* $D = p^3(256 - 27p)$ *conforme o Exemplo 8.1.3. Assim,* $\sqrt{D} \notin \mathbb{Q}$*. De fato, se* p *é impar, então* p *não divide* $256 - 27p$ *e se* $p = 2$*, então* $D = 256 \cdot 8 - 27 \cdot 16 = 1616$ *é tal quee* $\sqrt{1616} \notin \mathbb{Q}$*. Vamos supor que o grupo de Galois de* $f(x)$ *seja* G*. Então, se considerarmos* $p \neq 3$ *e* $p \neq 5$*, teremos que* $r(x)$ *não se fatora linearmente sobre* $\mathbb{Q}$ *e pelo Teorema 8.2.5,* $G \simeq S_4$*. Agora, se supormos que* $p = 3$*, podemos considerar* $\beta_1 = -3$ *e teremos que* $r(x) = x^3 - 12x - 9 = (x + 3)(x^2 - 3x - 3)$ *cujas raízes serão* $\beta_1 = -3$*,* $\beta_2 = \dfrac{3 + \sqrt{21}}{2}$

e $\beta_3 = \dfrac{3-\sqrt{21}}{2}$. *Assim,* $Gal(r(x), \mathbb{Q}) = \mathbb{Q}[\sqrt{21}]$, *e teremos* $h(x) = (x^2+3x+3)(x^2+3)$ *que claramente não se fatora linearmente sobre* $\mathbb{Q}$. *Portanto,* $G \simeq D_4$. *Finalmente, se tivermos* $p = 5$, *a cúbica resolvente será dada por* $r(x) = (x-5)(x^2+5x+5)$, *onde as raízes serão* $\beta_1 = 5$, $\beta_2 = \dfrac{-5+\sqrt{5}}{2}$ *e* $\beta_3 = \dfrac{-5-\sqrt{5}}{2}$. *Logo,* $Gal(r(x), \mathbb{Q}) = \mathbb{Q}[\sqrt{5}]$ *e* $h(x) = (x^2-5x+5)(x^2-5)$ *se fatora em* $\mathbb{Q}[\sqrt{5}]$. *Portanto, neste caso, teremos novamente pelo Teorema 8.2.5 que* $G = C_4$.

9 Não solubilidade por radicais

Finalmente temos quase todo o conhecimento necessário para estabelercemos uma condição suficiente para a solubilidade por radicais de um certo polinômio. As definições e resultados que restam serão dados no decorrer deste capítulo.

9.1 Uma condição necessária e sufuciente para a não solubilidade de polinômios por radicais.

Definição 9.1.1. Uma extensão $L \supset K$ é cíclica se tal extensão for normal e seu grupo de Galois $Aut_K L$ for cíclico.

Definição 9.1.2. Seja $L \supset K$ uma extensão normal finita com seu grupo de Galois G. A norma N de um elemento $x \in L$ é definida como

$$N(x) = \sigma_1(x)\sigma_2(x)\cdots\sigma_n(x)$$

em que $\sigma_i \in G$, $\forall i \in \{1, \cdots, n\}$.

Os dois seguintes teoremas são de extrema importância para a demonstração do teorema principal:

Teorema 9.1.3. *Seja $L \supset K$ uma extensão finita e normal com grupo de Galois G cíclico gerado por τ. Então $a \in L$ tem norma $N(a) = 1$ se, e somente se, $a = \dfrac{b}{\tau(b)}$, para algum $b \in L$, com $b \neq 0$.*

Demonstração: A demonstração pode ser encontrada em [2].

Teorema 9.1.4. *Seja $L \supset K$ uma extensão finita e normal, com grupo de Galois G cíclico de ordem prima p e gerado por τ. Se $x^p - 1$ se fatora linearmente em K, então $L = K[\alpha]$, onde α é raiz de um polinômio irredutível $x^p - a$ sobre K.*

Demonstração: A demonstração pode ser encontrada em [2].

Agora, finalmente chegamos ao principal resultado deste trabalho:

Teorema 9.1.5. *Seja $L \supset K$ uma extensão de corpos normal e finita, com grupo de Galois $Aut_K L$ solúvel. Então existe uma extensão R de L tal que $R \supset K$ é radical.*

Demonstração: A demonstração é por indução sobre $n = |Aut_K L|$. Primeiro, observe que se $n = 1$, então pelo Teorema 4.2.3, $|Aut_K L| = [L : K] = 1$, e $Aut_K L = \{id\}$. Assim, $L = K$ e portanto, não há o que demonstrar. Logo, segue-se o resultado.

Consideremos como hipótese de indução que o teorema seja verdadeiro para qualquer grupo G tal que $|G| < n$ e suponhamos agora que $|Aut_L K| > 1$. Como o grupo é finito, então, pelo Teorema 5.4.2, podemos escolher $H \lhd Aut_K L$ como o subgrupo maximal próprio. Isto é, se existe I tal que $H \leq I \leq Aut_K L$, então $H = I$, ou $I = Aut_K L$.

Consequentemente, pela Proposição 5.4.1, $\frac{Aut_K L}{H}$ é um grupo simples, pois H é maximal. Além disso, $\frac{Aut_K L}{H}$ é solúvel (pelo Teorema 5.1.2) e pelo Teorema 5.2.2, tem ordem prima p. Agora, suponhamos que ζ seja uma raiz p-ésima primitiva da unidade e tomemos $L[\zeta]$ como o corpo de decomposição do polinômio $x^p - 1$ sobre L.

Afirmamos que $L[\zeta] \supset K$ é extensão normal. De fato, como $L \supset K$ é normal (por hipótese), então pelo Teorema 3.1.2 existe $f(x) \in K[x]$ tal que $L = Gal(f, K)$. Então $L[\zeta] = Gal((x^p - 1)f, L)$, e portanto, novamente pelo Teorema 3.1.2, $L[\zeta] \supset K$ é extensão normal. Considere também o corpo $K[\zeta]$. Então temos o seguinte diagrama:

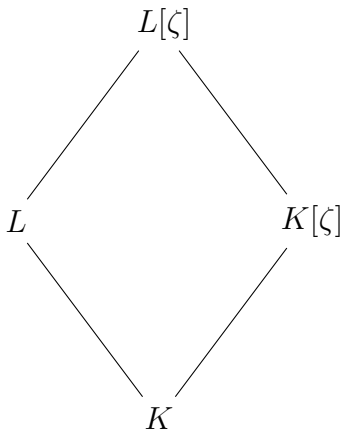

Figura 14 – Diagrama de corpos

Ou ainda:

Figura 15 – Cadeia de corpos auxiliar comparada com a da hipótese

Agora, pelo Lema 6.1.2, temos que $Aut_L L[\zeta]$ é abeliano, pois é o grupo de Galois do polinômio $x^p - 1$ sobre L. E novamente pelo Teorema 4.2.3, temos que:

$$Aut_K L \simeq \frac{Aut_K L[\zeta]}{Aut_L L[\zeta]}$$

Isto nos permite concluir que: $\dfrac{Aut_K L[\zeta]}{Aut_L L[\zeta]}$ é um grupo solúvel. Além disso, como $L[\zeta] \supset L$ é normal, então $Aut_L L[\zeta] \lhd Aut_K L[\zeta]$. Logo, pelo Teorema 5.1.2, $Aut_K L[\zeta]$ é solúvel.

Observe ainda que $K[\zeta] \supset K$ é extensão normal, pois $K[\zeta]$ é o corpo de decomposição de $x^p - 1$ sobre K. Além disso, esta extensão também é radical, pois $\zeta^p \in K$, e $L[\zeta] \supset K[\zeta]$ é extensão normal.

Agora que concluímos certos fatos, note que na Figura 15, construímos a direita uma extensão auxiliar de corpos. A partir disso, a ideia da demonstração é construir um isomorfismo de grupos entre $Aut_K L$ e $Aut_{K[\zeta]} L[\zeta]$, concluir o resultado nesta extensão auxiliar, e a partir do isomorfismo, concluir o que precisamos na extensão original (da esquerda).

Afirmamos agora que $Aut_{K[\zeta]} L[\zeta] \simeq J \leq Aut_K L$, onde J é um subgrupo de $Aut_K L$. Vamos provar essa afirmação definindo a função:

$$\begin{array}{rccc} \Phi\colon & Aut_{K[\zeta]} L[\zeta] & \longrightarrow & Aut_K L \\ & \sigma & \longmapsto & \sigma|_L \end{array}$$

Observe que Φ é homomorfismo de grupos, pois dados $\sigma, \tau \in Aut_{K[\zeta]} L[\zeta]$, temos que:

$$\begin{array}{rcl} \Phi((\sigma \circ \tau) & = & (\sigma \circ \tau)|_L \\ & = & \sigma|_L \circ \tau|_L \\ & = & \Phi(\sigma) \circ \Phi(\tau) \end{array}$$

Precisamos mostrar agora que $Ker(\Phi) = \{id\}$. De fato, pela definição, temos que $Ker(\Phi) = \{\sigma \in Aut_{K[\zeta]} L[\zeta]; \Phi(\sigma) = \sigma|_L = id_L\}$. Assim, se tomarmos $\sigma \in Ker(\Phi)$, então

$\Phi(\sigma) = id|_L$. Isto é, $\Phi(\sigma)$ fixa L. Assim, a única possibilidade é que $\Phi(\sigma) = id_L$. Logo, $Ker(\Phi) = \{id\}$. Portanto, pelo Teorema dos Isomorfismos, tem-se:

$$Aut_{K[\zeta]}L[\zeta] \simeq J \leq Aut_K L$$

onde $J = \Phi(Aut_{K[\zeta]}L[\zeta])$.

Temos então dois possíveis casos:

1. $J = \Phi(Aut_{K[\zeta]}L[\zeta]) \leq Aut_K L$ um subgrupo próprio.
2. $J = Aut_K L$

Vamos analisar o primeiro caso: observe que $|J| \leq |Aut_K L|$. Pela hipótese de indução, existe extensão R de $L[\zeta]$, tal que $R \supset K[\zeta]$ é radical. Logo, o isomorfismo garante que R é extensão de L tal que $R \supset K$ é extensão radical e acaba a demonstração.

Agora, iremos analisar o segundo caso: como $J = Aut_K L$, então podemos encontrar um subgrupo $I \lhd Aut_{K[\zeta]}L[\zeta]$ de índice p, ou seja, $[Aut_{K[\zeta]}L[\zeta] : I] = p$. Suponha que $I = \Phi^{-1}(H)$ e considere o corpo fixo de I: $\theta(I) = P$. Pelo Teorema 4.2.3, temos que $[P : K[\zeta]] = p$, e $P \supset K[\zeta]$ é normal.

Além disso, é claro que $x^p - 1$ se fatora linearmente em $K[\zeta]$. Assim, pelo Teorema 9.1.4, existe $\alpha \in P$, tal que $P = K[\zeta][\alpha]$, onde $\alpha^p = a \in K[\zeta]$. Isto é, mostramos que $P \supset K[\zeta]$ é uma extensão radical.

Podemos representar no diagrama abaixo o que temos até o momento:

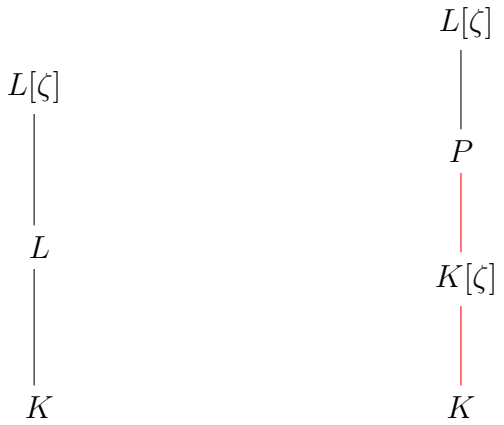

Figura 16 – Cadeia de corpos auxiliar.

Os traços destacados com a cor vermelha representam as extensões radicais que já temos até o momento.

Agora, usaremos a hipótese de indução para concluir o resultado para este segundo caso. Primeiro, note que, como $L[\zeta] \supset K$ é extensão normal, então $L[\zeta] \supset P$ também é.

Além disso, como $Aut_K L[\zeta]$ é um grupo solúvel e $Aut_P L[\zeta] \leq Aut_K L[\zeta]$, então $Aut_P L[\zeta]$ também é solúvel e mais ainda $|Aut_P L[\zeta]| < |Aut_K L[\zeta]|$. Assim, pela hipótese de indução, existe extensão R de $L[\zeta]$ tal que $R \supset P$ é radical. Mas $R \supset K[\zeta]$ também é extensão radical, então $L[\zeta] \supset K$ é extensão radical, que é exatamente o que precisávamos concluir. Pois como neste caso $Aut_K L[\zeta] \simeq Aut_K L$, então provamos que existe extensão R de L tal que $R \supset K$ é radical, como queríamos.

■

Corolário 9.1.1. *Seja $f(x) \in K[x]$. Se o grupo de Galois de $f(x)$ é solúvel, então $f(x)$ é solúvel por radicais.*

Demonstração: Sendo $f(x) \in K[x]$, suponha que $L = Gal(f, K)$. Por hipótese, o grupo de Galois $Aut_K L$ é solúvel. Pelo Teorema anterior, isto implica que L está contido em uma extensão radical. Portanto, $f(x)$ é solúvel por radicais.

■

E finalmente, temos o resultado desejado:

Teorema 9.1.6. *Um polinômio $f(x) \in K[x]$ é solúvel por radicais se, e somente se, seu grupo de Galois for solúvel.*

Demonstração: A demonstração é imediata pelo Teorema 6.1.3 e pelo Corolário 9.1.1.

■

Corolário 9.1.2. *Todo polinômio de grau $n \leq 4$ é solúvel por radicais.*

Demonstração: Todo polinômio de grau $n \leq 4$ tem grupo de Galois isomorfo a algum subgrupo de S_4, o qual, conforme já mostramos, é solúvel. Isto prova este corolário.

■

Corolário 9.1.3. *O polinômio geral $f(x) = x^n + s_1 x^{n-1} + \cdots + s_n \in K[s_1, \cdots, s_n]$ de grau $n \geq 5$ não é solúvel.*

Demonstração: Já mostramos que o grupo de Galois de $f(x)$ é o grupo das permutações S_n, o qual mostramos que não é solúvel para $n \geq 5$. Logo, pelo Teorema 9.1.6, o corpo de decomposição de $f(x)$ não está contido numa extensão radical, e portanto, não é solúvel por radicais.

■

10 Considerações finais

Ao término deste trabalho, foi possível estabelecer uma sólida relação entre dois ramos importantíssimos da Álgebra Abstrata, que são: Teoria de Corpos e Teoria de Grupos. Tal relação é consolidada pela belíssima Teoria de Galois. Vimos ainda que, para polinômios irredutíveis, existem determinadas condições para estabelecermos as propriedades de seus grupos de Galois, e que a complexidade do grupo aumenta conforme o grau do polinômio aumenta. E finalmente, mostramos uma das principais aplicações de toda a teoria desenvolvida: usamos a Teoria de Galois para mostrar que polinômios de grau $n \geq 5$ não são solúveis por radicais. Isto é, existem polinômios de grau $n \geq 5$ que não conseguimos calcular suas raízes em função de seus coeficientes através de operações algébricas e extração de radicais. Isto significa que suas raízes podem ser calculadas apenas por aproximações numéricas. Além disso, o Corolário 9.1.3 nos mostra a existência de uma classe de polinômios que não podem ser solúveis por radicais. Este resultado que provamos possui uma ampla importância não somente dentro da Álgebra, mas dentro de toda a Matemática, pois diversos problemas do mundo real são modelados por expressões polinomiais, e encontrar as raízes dessas expressões é algo fundamental para a resolução de tais problemas. Portanto, podemos concluir que todo este trabalho focado em uma área totalmente da Matemática Pura, possui aplicações no que diz respeito à Matemática Aplicada.

Referências

1 GONÇALVES, A. *Introdução à Álgebra*. Rio de Janeiro: IMPA, 2017. Citado 7 vezes nas páginas 3, 5, 6, 7, 8, 9 e 56.

2 STEWART, I. *Galois Theory*. Coventry: Chapman and Hall/CRC, 2004. Citado 4 vezes nas páginas 3, 10, 16 e 93.

3 CANAL MATEMATHIAGO. *Teoria de Corpos*. Disponível em: <https://www.youtube.com/watch?v=PWMHEhW0kcc&list=PL2xox8ncv81W0HbBtma7QQMeyVllJMk0m&index=2>. Acesso em: 15 março. 2021. Citado na página 3.

4 UNIVERSIDADE FEDERAL FLUMINENSE. *Extensões de Corpos*. Disponível em: <http://www.professores.uff.br/marco/wp-content/uploads/sites/37/2017/07/corpos-mod1.pdf>. Acesso em: 11 dez. 2020. Citado 2 vezes nas páginas 56 e 77.

5 MARTIN, P. A. *Grupos, Corpos e Teoria de Galois*. São Paulo: Livraria da Física, 2010. Citado na página 64.

6 MORANDI, P. A. *Field and Galois Theory*. New York: Springer, 1996. Citado 4 vezes nas páginas 78, 80, 82 e 91.

7 SELBY'S MATHS CAPSULE. *Galois Theory Lecture 18: Galois Group of Irreducible Cubic Polynomials*. Disponível em: <https://www.youtube.com/watch?v=Rr3tFb6i2n4&t=933s>. Acesso em: 1 março. 2021. Citado na página 78.