UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

TAÍS RIBEIRO DRABIK DE ALMEIDA

EQUAÇÕES POLINOMIAIS: AS FÓRMULAS CLÁSSICAS E A RESOLUBILIDADE POR MEIO DE RADICAIS

DISSERTAÇÃO

CURITIBA

2014

TAÍS RIBEIRO DRABIK DE ALMEIDA

EQUAÇÕES POLINOMIAIS: AS FÓRMULAS CLÁSSICAS E A RESOLUBILIDADE POR MEIO DE RADICAIS

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do grau de "Mestre em Matemática".

Orientador: Ronie Peterson Dario, Dr.

CURITIBA

2014

Dados Internacionais de Catalogação na Publicação

A447 Almeida, Taís Ribeiro Drabik de
Equações polinomiais : as fórmulas clássicas e a resolubilidade por meio de radicais / Taís Ribeiro Drabik de Almeida. –2014.
46 f. : il. ; 30 cm

Orientador: Ronie Peterson Dario.
Dissertação (Mestrado) – Universidade Tecnológica Federal do Paraná. Programa de Mestrado Profissional em Matemática em Rede Nacional. Curitiba, 2014.
Bibliografia: f. 46.

1. Equações – Soluções numéricas. 2. Polinômios. 3. Galois, Teoria de. 4. Teoria dos grupos. 5. Álgebra. 6. Matemática – Estudo e ensino. 7. Matemática – Dissertações. I. Dario, Ronie Peterson, orient. II. Universidade Tecnológica Federal do Paraná. Programa de Mestrado Profissional em Matemática em Rede Nacional. III. Título.

CDD (22. ed.) 510

Biblioteca Central da UTFPR, Campus Curitiba

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
Câmpus Curitiba

Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Título da Dissertação No. 015

"Equações polinomiais: as fórmulas clássicas e a resolubilidade por meio de radicais"

por

Taís Ribeiro Drabik de Almeida

Esta dissertação foi apresentada como requisito parcial à obtenção do grau de Mestre em Matemática, pelo Programa de Mestrado em Matemática em Rede Nacional - PROFMAT - da Universidade Tecnológica Federal do Paraná - UTFPR - Câmpus Curitiba, às 10h do dia 21 de março de 2014. O trabalho foi aprovado pela Banca Examinadora, composta pelos doutores:

_____
Prof. Ronie Peterson Dario, Dr.
(Presidente - UTFPR/Curitiba)

_____
Prof. Andre Krindges
(UFMT)

_____
Profa. Patricia Massae Kitani, Dra.
(UTFPR/Curitiba)

Visto da coordenação:

_____
Prof. Ronie Peterson Dario, Dr.
(Coordenador do PROFMAT/UTFPR)

"A Folha de Aprovação assinada encontra-se na Coordenação do PROFMAT/UTFPR"

Assim escreveu o Padre Antonio Vieira: ”As palavras movem, os exemplos arrastam.”. Por esse motivo dedico este trabalho ao meu pai, Alexandre.

AGRADECIMENTOS

Agradeço ao meu marido, Cleber, por ter me incentivado nos momentos em que todos os outros falharam. Por ter tido paciência com todo o meu mau humor e por abrir mão da minha companhia em incontáveis momentos nos últimos 3 anos.

Agradeço à minha filha Nathalie por ter rido comigo de muitas situações, tornando mais leve a jornada. E ao meu filho Nicholas, agradecimentos por ter dividido comigo muitos momentos de estudo da Matemática. Foi um excelente companheiro e aprendi bastante com ele.

Agradeço muito à minha família: minha mãe, irmãs, sobrinhos, sogra, cunhados, tios e primos, que entenderam minha ausência em muitos momentos, e sempre deram muito valor a este trabalho.

Muitos agradecimentos aos meus amigos, que se revezaram na tarefa de me incentivar na busca dos meus objetivos e de me consolar quando as coisas não andavam bem. Meu carinho especial ao Alexandre, à Ana Cecília, à Daihany, à Márcia, à Melissa e ao Nino.

Agradeço também aos meus colegas na Positivo Informática, pelo apoio. Em especial, ao Marcio Faria, pelo conselho de que eu deveria continuar meus estudos, e ao Alex Paiva, pelo apoio amigo e incondicional.

Não posso deixar de agradecer aos professores e colegas do PROFMAT, em especial àqueles que me inspiraram no decorrer do curso. Durante muitos anos eu quis ser uma boa professora de Matemática, mas esses professores fizeram nascer em mim o desejo de ser, também, uma boa matemática.

Agradeço especialmente ao meu orientador, professor Ronie, pela inspiração. Foi uma referência para mim mesmo antes de ter sido escolhido para me conduzir na produção deste trabalho.

Por fim, agradeço a Deus por todo o aprendizado que a experiência do mestrado me proporcionou, e por todo o auxílio que recebi, vindo muitas vezes de formas inesperadas.

RESUMO

ALMEIDA, Taís Ribeiro Drabik de. EQUAÇÕES POLINOMIAIS: AS FÓRMULAS CLÁSSICAS E A RESOLUBILIDADE POR MEIO DE RADICAIS. 46 f. Dissertação – Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

A resolução de equações polinomiais com coeficientes racionais consiste em parte significativa da história do desenvolvimento da álgebra. O problema era encontrar fórmulas que expressassem uma raiz por meio de operações aritméticas efetuadas sobre a equação original, isto é, determinar a resolubilidade por radicais da equação. O trabalho de vários matemáticos culminou, no século XVI, com a obtenção das fórmulas para a resolução de equações polinomiais de grau menor ou igual a 4. Três séculos depois, Niels Abel mostrou que não é possível obter uma fórmula para a equação geral de grau 5. Finalmente, Evariste Galois resolveu completamente o problema estudando o grupo de permutação das raízes e estabelecendo as condições exatas para a resolubilidade de uma equação polinomial. Neste trabalho apresentamos um breve histórico da obtenção de fórmulas para as raízes das equações de grau menor ou igual a 4 e a essência da matemática envolvida no estudo da resolubilidade por radiciais de equações polinomiais de grau maior ou igual a 5.

Palavras-chave: Equações polinomais, Galois, Resolubilidade por Radicais

ABSTRACT

ALMEIDA, Taís Ribeiro Drabik de. POLYNOMIAL EQUATIONS: THE CLASSIC FORMULAS AND THE SOLVABILITY BY RADICALS. 46 f. Dissertação – Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

The solvability by radicals of polynomial equations with rational coefficients is an important part of the history of algebra. The problem was to express a root by means of basic arithmetic operations and radicals. Formulas to solve polynomial equations of degree lower than or equal to 4 were obtained in XVIth century. About three centuries later, Niels Abel showed that it is not possible to find a formula for the general equation of degree 5. Finally, Evariste Galois solved the problem by studying the permutations groups, establishing the exact conditions for the solvability of a polynomial equation. In this work we present a brief history of the classic formulas for the roots of equations with degree lower or equal to 4. Then we study solvability by radicals of polynomial equations of degree higher than or equal to 5.

Keywords: polynomial equations, Galois, solvability by radicals

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Uma **equação algébrica (ou equação polinomial) de grau** n é uma equação da forma

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0,$$

onde $n \geq 1$ é um número natural e $a_0, \ldots, a_n$ pertencem a um corpo numérico fixado, com $a_n \neq 0$.

Resolver equações algébricas, encontrando suas raízes ou obtendo fórmulas gerais para essas, consiste em parte significativa da história da álgebra. Em especial, considerando os coeficientes racionais, são de grande relevância

(1) o desenvolvimento de fórmulas para raízes da equação geral de grau menor ou igual a 4;

(2) a essência da matemática envolvida no estudo da resolubilidade por radicais de uma equação algébrica de grau maior ou igual a 5.

Neste nosso trabalho abordaremos esses dois tópicos. O primeiro deles será objeto de estudo nesta introdução. O segundo tópico será desenvolvido nos capítulos seguintes e demanda entendermos a correspondência galoisiana para possibilitar a demonstração do critério da resolubidade de uma equação algébrica de grau maior ou igual a 5 em termos da resolubilidade do grupo de Galois correspondente.

Não estamos diretamente interessados na história do avanço da simbologia utilizada, por isso utilizaremos sempre a notação moderna. Contudo, vale lembrar que o simbolismo na Álgebra inciou-se com Diofante (500 d.C.). Na sua obra *Aritmética* ele discute as equações lineares. São abordados vários tipos de equações quadráticas com mais de uma incógnita e algumas equações cúbicas especiais. As soluções são sempre inteiras ou racionais, e por isso as equações desse tipo passaram a ser conhecidas como *equações diofantinas*. Diofante introduziu símbolos para as incógnitas, para "ao quadrado" e para "ao cubo".

A história da resolução das equações polinomiais começa pela resolução das equações de grau 1, pelos egípcios. Conforme [2, p.9], os primeiros registros de problemas envolvendo

a resolução desse tipo de equações aparece no *Papiro de Rhind* (também conhecido como *Papiro de Ahmes*), por volta de 1650 a.C . O método utilizado era o método da falsa posição, no qual atribui-se um valor arbitrário para a incógnita, o valor da expressão é calculado e depois efetua-se a correção por um fator que torne o valor adequado à expressão original.

Para ilustrar o método da falsa posição, vejamos o exemplo da equação

$$x + \frac{x}{5} = 18.$$

Vamos iniciar atribuindo o valor 5 para x e assim obtemos, no membro à esquerda

$$5 + \frac{5}{5} = 6.$$

Ora, o valor à direita deve ser 18, portanto o fator de correção é 3. Assim

$$3\left(5 + \frac{5}{5}\right) = 3.6, \text{ isto é, } 15 + \frac{15}{5} = 18.$$

Portanto, a solução é $x = 15$.

Euclides de Alexandria (325 a.C - 265 a.C), em sua conhecida obra *Elementos*, registrou, organizou e complementou todo o conhecimento matemático da época. Apesar de seu trabalho ser fortemente dedicado à Geometria, ele contribuiu com a resolução de equações registrando os axiomas fundamentais para o desenvolvimento da teoria, nos seguintes termos:

1) Coisas iguais a uma terceira são iguais entre si.

2) Se iguais forem somados a iguais, os resultados serão iguais.

3) Se iguais forem subtraídos de iguais, os resultados serão iguais.

4) Coisas coincidentes são iguais entre si.

5) O todo é maior do que a parte.

A segunda e a terceira afirmações, acrescidas de mais duas, abaixo enunciadas, servem de base, atualmente para a resolução das equações algébricas.

6) Iguais multiplicados por iguais continuam iguais.

7) Iguais divididos por iguais continuam iguais.

A utilização desses axiomas permite que se obtenha, por exemplo, a solução de uma equação de grau 1, apenas efetuando as operações aritméticas elementares.

As equações quadráticas, por outro lado, já eram resolvidas pelos babilônios, usando certas "receitas", que se aproximam do que hoje conhecemos como a fórmula de resolução das equações quadráticas ou fórmula de Bháskara. O método utilizado era o de completar quadrados, conforme veremos. Os babilônios também conheciam a solução para algumas formas de cúbicas e para isso se baseavam em tabelas numéricas [2, p.24].

Para uma equação do tipo

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

com a, b, c constantes e $a \neq 0$, dividindo cada termo por a, obtemos:

$$x^2 + \frac{b}{a}x + \frac{c}{a} = 0.$$

Subtraindo de cada membro $\frac{c}{a}$:

$$x^2 + \frac{b}{a}x = -\frac{c}{a}.$$

Em seguida busca-se completar um quadrado perfeito, somando-se $\frac{b^2}{4a^2}$ aos dois membros. Obtemos:

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

Assim, a expressão pode ser reescrita como

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}.$$

Extraindo a raiz quadrada dos dois lados da igualdade, obtemos

$$\sqrt{\left(x + \frac{b}{2a}\right)^2} = \pm\sqrt{\frac{b^2 - 4ac}{4a^2}},$$

donde conclui-se a fórmula conhecida:

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

Mais tarde os gregos, aparentemente, reinventaram os métodos babilônios. Os gregos eram mais ligados ao estudo da Geometria, então representavam números como quantidades

geométricas, como áreas e comprimentos. As soluções para as equações quadráticas apresentadas pelos gregos seguiam esses parâmetros.

A resolução de equações também estava sendo estudada no mundo árabe. Em 830 d.C., al-Khwarizmi (780-850 d.C.) escreveu a obra *al-Jabrw'al Muqabala*, que foi traduzida para o latim no século XII. Essa obra tem influências gregas e babilônias, e ideias do indiano Bramagupta (600 d.C.), sobre equações do primeiro grau e quadráticas. Seus sucessores trabalharam na resolução de alguns tipos de equações cúbicas.

Um entrave à obtenção de uma fórmula para a resolução das cúbicas era o desconhecimento dos números negativos. No século XI, em uma tentativa de solução, o poeta e matemático persa Omar Kayyan (1048 - 1131 d.C.) classificou as equações cúbicas em 14 tipos diferentes, justamente de forma a ter sempre termos positivos. Em linguagem moderna, podemos expressar assim os 14 tipos descritos por Kayyan [9, p.60]:

1) $ax^3 = bx^2 + cx + d$

2) $ax^3 = bx^2 + d$

3) $ax^3 = cx + d$

4) $ax^3 = d$

5) $ax^3 + bx^2 = cx + d$

6) $ax^3 + bx^2 = d$

7) $ax^3 + cx = bx^2 + d$

8) $ax^3 + cx = d$

9) $ax^3 + d = bx^2 + cx$

10) $ax^3 + d = bx^2$

11) $ax^3 + d = cx$

12) $ax^3 + bx^2 + cx = d$

13) $ax^3 + bx^2 + d = cx$

14) $ax^3 + cx + d = bx^2$

Utilizando seções cônicas, Omar Kayyan desenvolveu soluções geométricas para todos os tipos de cúbicas e as apresentou na obra *Álgebra*, de 1079. Ele dividiu as soluções em algébricas, aquelas com resultados inteiros, e geométricas, nas quais os resultados eram expressos em comprimentos, áreas e volumes.

No século XVI, entretanto, ainda buscava-se uma verdadeira solução algébrica para as cúbicas. É fato marcante na história da Matemática a disputa que ocorreu na época pelos créditos da solução obtida por Girolamo Cardano (1501 - 1576), Scipione del Ferro (1465 - 1526), Nicolau Tartaglia (1499 - 1557) e Antonio Fior (cujas datas exatas de nascimento e morte são desconhecidas).

Del Ferro obteve uma solução para uma certa categoria de cúbicas, e essa solução foi reproduzida e ampliada por Tartaglia em uma competição contra Fior. A solução chegou

às mãos de Cardano, que se compremeteu a não publicá-la, mas acabou fazendo-o, embora dando os créditos adequados. Mas Tartaglia, que pretendia obter vantagens financeiras com sua descoberta, não ficou muito satisfeito com a publicação [9, p.73].

A fórmula publicada por Cardano para a resolução de uma equação da forma $x^3 + ax = b$, seria, em uma notação moderna:

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

Embora a fórmula se aplique apenas a esse formato específico de cúbica, com algumas substituições é possível empregá-la para resolver qualquer outra equação de grau 3, como veremos na sequência.

A equação geral da cúbica tem a forma

$$ax^3 + bx^2 + cx + d = 0,$$

onde a, b, c e d são constantes e $a \neq 0$.

Fazendo $x = \left(y - \frac{b}{3a}\right)$ e substituindo na expressão, obtemos

$$0 = a\left(y - \frac{b}{3a}\right)^3 + b\left(y - \frac{b}{3a}\right)^2 + c\left(y - \frac{b}{3a}\right) + d$$

$$= ay^3 + \left(b - 3a\frac{b}{3a}\right)y^2 + \left(\frac{b^2}{3a} - \frac{2b^2}{3a} + c\right)y + \frac{b^3}{27a^2} + \frac{b^3}{9a^2} - \frac{cb}{3a} + d.$$

Como $b - 3a\frac{b}{3a} = 0$, e se considerarmos $p = \frac{b^2}{3a} - \frac{2b^2}{3a} + c$ e $q = \frac{b^3}{27a^2} + \frac{b^3}{9a^2} - \frac{cb}{3a} + d$,

então obtemos a equação $ay^3 + py + q = 0$.

Agora, fazendo $x = u + v$, temos

$$x^3 = (u+v)^3 = u^3 + v^3 + 3uv(u+v) = u^3 + v^3 + 3uvx.$$

Assim obtemos

$$x^3 - 3uvx - (u^3 + v^3) = 0.$$

Essa é uma equação cúbica na qual podemos considerar $p = -3uv$ e $q = -(u^3 + v^3)$. Mas isso significa que u^3 e v^3 são raízes da equação de segundo grau $z^2 + qz - \frac{p^3}{27} = 0$.

Resolvendo-a, obtemos

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \quad \text{e} \quad v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Portanto

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

Vejamos o exemplo da equação $x^3 - 6x - 9 = 0$. Utilizando a fórmula de Cardano com $p = -6$ e $q = -9$, temos

$$x = \sqrt[3]{\frac{9}{2} + \sqrt{\frac{(-9)^2}{4} + \frac{(-6)^3}{27}}} + \sqrt[3]{\frac{9}{2} - \sqrt{\frac{(-9)^2}{4} + \frac{(-6)^3}{27}}} =$$

$$= \sqrt[3]{\frac{9}{2} + \sqrt{\frac{49}{4}}} + \sqrt[3]{\frac{9}{2} - \sqrt{\frac{49}{4}}} = \sqrt[3]{4} + \sqrt[3]{1} = 2 + 1 = 3.$$

Na sua obra *Ars Magna*, Cardano apresentou a resolução da equação $x^3 - 15x - 4 = 0$, e obteve a raiz

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}.$$

Diretamente verifica-se que $x = 4$ é raiz dessa equação, embora Cardano não tenha conseguido obtê-la a partir de sua fórmula.

Na época, já se conheciam os números hoje chamados de *complexos*, mas como não havia um significado para eles, havia receio em utilizá-los. Foi em 1572, na sua obra *Álgebra*, que Rafael Bombelli teve a ideia de manipular as raízes de números negativos utilizando as mesmas operações empregadas com outros números, e assim percebeu que $(2 + \sqrt{-1})^3 = 2 + \sqrt{-121}$ e que $(2 - \sqrt{-1})^3 = 2 - \sqrt{-121}$. Somando as duas raízes cúbicas, então, obtém-se o 4, a raiz "perdida".

Com a ajuda de Ludovico Ferrari, Cardano também conseguiu incluir em sua obra a fórmula para a resolução das equações de grau 4.

A forma geral da equação de quarto grau é $x^4 + ax^3 + bx^2 + cx + d = 0$, com a, b, c e d constantes e $a \neq 0$. Para se obter uma fórmula resolutiva, começamos por eliminar o termo de grau 3, completando quadrados:

$$\left(x^2 + \frac{1}{2}ax\right)^2 = \left(\frac{1}{4}a^2 - b\right)x^2 - cx - d.$$

Temos um quadrado perfeito no primeiro membro da equação, então seria conveniente

que o segundo membro também fosse um quadrado perfeito. Somando a expressão $y^2+2y\left(x^2+\frac{1}{2}ax\right)$ aos dois membros da igualdade, obtemos:

$$\left[\left(x^2+\frac{1}{2}ax\right)+y\right]^2=\left(2y+\frac{1}{4}a^2-b\right)x^2+(ya-c)x+(y^2-d). \quad (1)$$

No segundo membro temos uma equação do segundo grau em x. Para que tenhamos um quadrado perfeito nesse membro basta que tenhamos o discriminante da quádrica igual a zero.

$$(ya-c)^2-4\left(2y+\frac{1}{4}a^2-c\right)(y^2-d)=0.$$

Desenvolvendo essa expressão obtemos uma cúbica:

$$8y^3-4by^2+(2ac-8d)y+(4bd-da^2-c^2)=0.$$

Agora, essa equação pode ser resolvida pela fórmula de Cardano. Escolhendo um dos valores obtidos para y e substituindo em (1), obtemos uma igualdade entre quadrados perfeitos:

$$\left[\left(x^2+\frac{1}{2}ax\right)+y\right]^2=(\alpha x+\beta)^2.$$

A resolução dessa equação, por fim, permite encontrar as raízes do polinômio de grau 4.

Para ilustrar o método resumidamente, vamos encontrar as raízes da equação $x^4-4x^3+x^2+4x-2=0$. A cúbica que nos permitirá obter um valor para y é $-8y^3+4y^2+16y-8=0$. Uma das suas soluções, que podemos encontrar utilizando a fórmula de Cardano, é $y=\sqrt{2}$. Utilizando esse valor de y, obtemos:

$$\begin{aligned}\left(x^2-4x+\sqrt{2}\right)^2 &= \left(2\sqrt{2}+\frac{1}{4}(-4)^2-1\right)x^2+(-4\sqrt{2}-4)x+(\sqrt{2})^2+2\\ &= (2\sqrt{2}+3)x^2+(-4\sqrt{2}-4)x+4\\ &= [(\sqrt{2}+1)x+2]^2,\end{aligned}$$

ou seja,

$$\left(x^2-4x+\sqrt{2}\right)^2=[(\sqrt{2}+1)x+2]^2.$$

Assim, para obtermos as raízes, resolvemos as equações

$$(x^2-4x)+\sqrt{2}=(\sqrt{2}+1)x+2 \text{ e } (x^2-4x)+\sqrt{2}=-(\sqrt{2}+1)x-2.$$

As raízes assim obtidas são $-1, 1, 2+\sqrt{2}, 2-\sqrt{2}$.

As técnicas de redução empregadas na obtenção das fórmulas da cúbica e quártica foram aplicadas na busca de fórmulas para as equações de grau 5 e superior, sem sucesso, entretanto. Esperava-se que o padrão observado para as equações de terceiro e quarto graus se repetisse e que a obtenção de uma fórmula para a equação de grau 5 envolvesse a resolução de uma equação de grau 4. Isso não ocorreu pois, empregando os mesmos processos, chegou-se uma equação de grau 6.

O problema foi abordado por grandes matemáticos, que não conseguiram resolvê-lo. Euler ($\pm$ 1750) tentou reduzir a equação de grau 5 a uma quártica. Lagrange ($\pm$ 1780) também falhou na mesma tentativa. Ruffini ($\pm$ 1810) tentou demonstrar que é impossível resolver, em geral, as equações de grau 5 por meio de radicais.

Finalmente, após três séculos da resolução da equação de grau 4, N. H. Abel (1802-1829) demonstrou o resultado hoje conhecido como Teorema de Abel-Ruffini, que revela a impossibilidade da obtenção da fórmula para a equação de grau 5.

Mas o problema geral continuava em aberto, no sentido que se esperava o mesmo para a equação geral de grau superior a 5 e, principalmente, determinar quando uma equação particular poderia ou não ser resolvida por meio de radicais.

Utilizando algumas ideias de Lagrange e Viète sobre a permutação de raízes, foi o jovem francês Evariste Galois (1811-1832) quem finalmente resolveu o problema geral. Na noite antes de sua morte num duelo tolo, deixou registrada a solução de um dos maiores problemas da matemática até então.

Na sequência do nosso trabalho faremos uma exposição do método introduzido por Galois. O próximo capítulo é inteiramente dedicado à teoria básica de grupos, em especial, os grupos de permutações. Vale lembrar que foi Galois quem introduziu o conceito de grupo, fato considerado o nascimento da álgebra abstrata.

No terceiro e último capítulo abordamos alguns conceitos e resultados da teoria de corpos. Estudamos a correspondência galoisiana, que permite demonstrar o Teorema de Galois sobre a resolubilidade de uma equação polinomial por meio de radicais.

2 GRUPOS

2.1 NOÇÕES DA TEORIA ELEMENTAR DOS GRUPOS

Um conjunto não vazio G, munido de uma operação binária $* : G \times G \longrightarrow G$, que associa o par (g_1, g_2) com $g_1 * g_2$, é chamado de **grupo** quando são satisfeitas as três condições:

1) A operação é associativa, isto é, $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$, para todos $g_1, g_2, g_3 \in G$.

2) Existe um elemento neutro, isto é, existe $e \in G$ tal que, para todo $g \in G$, $g * e = g = e * g$.

3) Todo elemento de G admite inverso, isto é, dado $g \in G$ existe $g' \in G$ tal que $g * g' = e = g' * g$.

Caso a operação seja comutativa, ou seja, $g_1 * g_2 = g_2 * g_1$, para todos $g_1, g_2 \in G$, então dizemos que G é grupo **abeliano** ou **comutativo**.

Existe um único elemento neutro em um grupo G, pois se $e_1, e_2 \in G$ são neutros, então $e_1 = e_1 * e_2 = e_2$. Também, dado $g \in G$, existe um único $g' \in G$, inverso de G.

A operação do grupo pode ser a adição, a multiplicação, a composição, etc, conforme veremos nos exemplos seguintes. Será mais frequente utilizarmos a notação multiplicativa, onde $e = 1$, $g' = g^{-1}$ e ignora-se o símbolo "$*$".

O conjunto $\mathbb{Z}$ dos números inteiros, com a operação usual da adição é um grupo abeliano. De fato, a operação é associativa, $e = 0$ e $a' = -a$, para todo $a \in \mathbb{Z}$.

Seja C um conjunto com n elementos. O conjunto de todas as bijeções de C, munido da operação de composição de funções, é um grupo. É denominado **grupo das permutações de n elementos** e é denotado por S_n. Que a operação é associativa, verifica-se facilmente. O elemento neutro é a função identidade e, como todas as funções são bijetoras, a existência da inversa é garantida. Note que S_n possui $n!$ elementos.

O número de elementos de um grupo finito G é chamado de **ordem** de G e é denotada por $|G|$. No exemplo anterior, temos $|S_n| = n!$.

O conjunto $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$ munido da operação da adição é um exemplo de grupo abeliano. O elemento neutro é aquele em que $a = b = 0$ e o oposto de $x = a+b\sqrt{2}$ é $x' = -a-b\sqrt{2}$.

Seja G um grupo e $H \subset G$, H não vazio. Se H, com a restrição da operação de G também for um grupo, então dizemos que H é um **subgrupo** de G. Dado um grupo G, $\{e\}$ e G são subgrupos de G. Se H é subgrupo de G, e_H é o elemento neutro de H e e_G é o elemento neutro de G, temos que $e_G = e_H$. De fato, se $g \in H$ então $g \in G$ e, portanto, $ge_H = g$ e $ge_G = g$. Também temos que $g^{-1}(ge_H) = g^{-1}g$. Portanto, $e_H = e_G$.

Proposição 2.1. *H é subgrupo de G se, e somente se, para todos $g,h \in H$, $gh \in H$ e $g^{-1} \in H$.*

Demonstração: ($\Rightarrow$) Segue imediatamente do fato de H ser subgrupo de G e $e_H = e_G$.
($\Leftarrow$) Supondo que para todos $g,h \in H$ temos $gh \in H$ e $g^{-1} \in H$, vamos provar que $H \subset G$ é grupo com a restrição da operação de G. Dados $h_1,h_2,h_3 \in H$, temos que $(h_1h_2)h_3 = h_1(h_2h_3)$, pois $h_1,h_2,h_3 \in G$ e G é grupo. Dado $h \in H$, então, por hipótese, $h^{-1} \in H$. Logo, $hh^{-1} \in H$ e, portanto, $e_H \in H$. Também da hipótese já temos que para todo $h \in H$, $h^{-1} \in H$.

□

Fixe $n \in \mathbb{Z}$ e seja $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$. Verifica-se diretamente que o conjunto $n\mathbb{Z}$, munido da operação de adição é um subgrupo de $\mathbb{Z}$.

Sejam G um grupo e $S \subset G$. Então denotaremos por $\langle S \rangle$ ao conjunto $\{a_1a_2...a_n \mid n \in \mathbb{N},\ a_i \in S \text{ ou } (a_i)^{-1} \in S\}$. Esse subconjunto forma um subgrupo de G, dito o **subgrupo gerado por** S. Se $S = \{a_1,a_2,...,a_n\}$ é um conjunto finito, indicaremos o grupo gerado por S por $S = \langle a_1,a_2,...,a_n \rangle$. Um grupo G é dito **cíclico** quando G é gerado por um único elemento $g \in G$. Nesse caso, denotamos $G = \langle g \rangle$. Um exemplo imediato é o conjunto $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$, que é gerado por n, ou seja, $n\mathbb{Z} = \langle n \rangle$.

Seja G grupo e $g \in G$. Então, a **ordem** do elemento g é definida como

$$|g| = \min\{n \in \mathbb{N} \ ; \ g^n = 1\}.$$

Se $g^k = 1$, para algum $k \in \mathbb{Z}$, então $n = |g|$ divide k. De fato, pelo Algoritmo da Divisão Euclidiana, existem q e $r \in \mathbb{N}$ tais que $k = nq + r$ e $0 \leq r < n$. Então, $1 = g^k = (g^n)^q g^r = g^r$. Temos que $r = 0$. Caso contrário, teríamos uma contradição com a minimalidade de n.

Seja G um grupo aditivo e H subgrupo de G. Vamos introduzir uma relação de equivalência em G, estabelecendo que dois elementos x e y estão relacionados ($x \sim y$) quando $x-y \in H$, com $x-y = x+(-y)$. De fato trata-se de uma relação de equivalência em G, isto é,

uma relação reflexiva, simétrica e transitiva. A reflexividade é imediata, já que $x-x=0\in H$. Como $x-y\in H$ implica $-(x-y)=y-x\in H$, temos a simetria. Para a transitividade, se $x-y\in H$ e $y-z\in H$, então $(x-y)+(y-z)=x+(-y+y)-z=x-z\in H$.

Fixando $x\in G$, o conjunto $\{g\in G\ ;\ g\sim x\}$ de todos os elementos de G que se relacionam com x é dado por

$$\overline{x}:=\{g\in G\ ;\ g\sim x\}=\{x+h\ ;\ h\in H\}\ :=\ x+H,$$

pois $\overline{x}=\{g\in G\ ;\ g-x\in H\}=\{g\in G\ ;\ g\in x+H\}$ e é denominado de **classe de equivalência** de x. O conjunto de todas as classes de equivalência de elementos de G é chamado **conjunto quociente** de G por H, denotado por $\overline{G}$, ou por G/H. Assim,

$$G/H=\{\overline{x}\ ;\ x\in G\}=\{x+H\ ;\ x\in G\}.$$

O exemplo mais elucidativo de relação de equivalência é a congruência, módulo um inteiro positivo n, no grupo aditivo $G=\mathbb{Z}$. Dois inteiros a e b estão relacionados (são congruentes módulo n) quando n divide a diferença $a-b$, ou seja, existe $\alpha\in\mathbb{Z}$ tal que $a-b=n\alpha\in n\mathbb{Z}=H$. Denota-se por $a\equiv b \bmod n$. Afirmar que a e b são congruentes módulo n também equivale a dizer que eles deixam o mesmo resto na divisão por n. Isso verifica-se diretamente, assim a simetria, reflexividade e transitividade, que fazem da congruência uma relação de equivalência. A classe de $a\in\mathbb{Z}$ é dada por

$$\overline{a}=\{b\in\mathbb{Z}\ ;\ a\equiv b \bmod n\}=a+n\mathbb{Z}$$

e o conjunto quociente é $\mathbb{Z}_n:=\mathbb{Z}/n\mathbb{Z}=\{\overline{a}\ ;\ a\in\mathbb{Z}\}$, denominado **conjunto dos inteiros módulo** n.

Dada uma relação de equivalência no grupo G, podemos enunciar a seguinte proposição.

Proposição 2.2. *Para todos $a,b\in G$, tem-se:*

1) $\overline{a}\cap\overline{b}=\emptyset$ *ou* $\overline{a}=\overline{b}$.

2) $x\in\overline{a}\Leftrightarrow\overline{x}=\overline{a}$.

A demonstração pode ser consultada em [4, p.9]. No nosso exemplo, as propriedades acima permitem verificar que

$$\mathbb{Z}_n=\{\overline{0},\overline{1},\overline{2},...,\overline{n-1}\}.$$

De fato, do Teorema da Divisão Euclideana [3, p.5] o resto da divisão de um número inteiro por n é único e assim, as classes $\overline{0}, \overline{1}, ..., \overline{n-1}$ são distintas (e, portanto, disjuntas). Ainda, dado $m \geq n$, novamente do Teorema da Divisão Euclideana, existem únicos inteiros q e r tais que $m = nq + r$ e $r \in \{0, 1, ..., n-1\}$. Segue que $\overline{m} = \overline{r} \in \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$.

Surge naturalmente a questão de determinar se o conjunto quociente G/H é munido de uma operação que o torne grupo. Para respondê-la, é necessário passar ao conceito de subgrupo normal, que pode ser estudado de maneira mais clara usando a notação multiplicativa para G. Agora

$$G/H = \{gH \ ; \ g \in G\}, \text{ onde}$$

$$\overline{g} = gH = \{gh \ ; \ h \in H\} \ \text{ e } \ g_1 \sim g_2 \Leftrightarrow g_1 g_2^{-1} \in H.$$

Diremos que N é **subgrupo normal** (denotamos $N \trianglelefteq G$) quando, para todos $\overline{a}, \overline{b} \in G/N$ valer a condição

$$a_1 \in aH \text{ e } b_1 \in bH \Rightarrow abH = a_1 b_1 H.$$

Isso é equivalente a:

$$a_1 \in \overline{a}, \ b_1 \in \overline{b} \Rightarrow \overline{ab} = \overline{a_1 b_1},$$

que por sua vez significa que está bem definida a operação

$$\begin{array}{rcl} G/N \times G/N & \longrightarrow & G/N \\ (\overline{a}, \overline{b}) & \longmapsto & \overline{a}\overline{b} = \overline{ab}, \end{array}$$

no sentido de que não importa a particular escolha dos representantes em $\overline{a}$ e $\overline{b}$, que o resultado da operação será o mesmo.

Proposição 2.3. *Seja G um grupo denotado multiplicativamente e N um subgrupo de G. São equivalentes:*

(i) $N \trianglelefteq G$;

(ii) $gN = Ng = \{ng \ ; \ n \in N\}$, *para todo* $g \in G$;

(iii) $gNg^{-1} = N$, *para todo* $g \in G$.

Demonstração: A demonstração pode ser encontrada em [3, p.138].

Se H é subgrupo de G e G é abeliano, então $H \trianglelefteq G$. De fato, $gH = \{gh \ ; \ h \in H\} = \{hg \ ; \ h \in H\} = Hg$, para todos $g \in G$.

Por exemplo, $n\mathbb{Z} \trianglelefteq \mathbb{Z}$, para cada $n \in \mathbb{Z}$. Assim, o conjunto quaociente $\mathbb{Z}_n$ é grupo cíclico, gerado por $\overline{1}$ (portanto abeliano). Ainda mais, se p é um número primo, então $\mathbb{Z}_p \backslash \{\overline{0}\}$ é também grupo multiplicativo. De fato, se $\overline{x} \neq \overline{0}$, tem-se pelo Lema de Bezout, que existem $r, s \in \mathbb{Z}$ tais que $1 = rx + sn$, pois $\text{mdc}(x,n) = 1$. Segue que $\overline{1} = \overline{rx} = \overline{r}.\overline{x}$.

Outro exemplo interessante é o subgrupo cíclico $H = \langle \overline{3} \rangle$ de $\mathbb{Z}_{12} = \{\overline{0}, ..., \overline{11}\}$. Note que $H = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$. Denotemos $\mathbb{Z}_{12}/H = \{\overline{\overline{a}};\ \overline{a} \in \mathbb{Z}_{12}\}$, onde $\overline{\overline{a}} = \overline{a} + H$.

Calculando todas as classes, temos

$$\overline{\overline{0}} = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} = H \qquad \overline{\overline{6}} = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} = H$$

$$\overline{\overline{1}} = \{\overline{1}, \overline{4}, \overline{7}, \overline{10}\} \qquad \overline{\overline{7}} = \{\overline{1}, \overline{4}, \overline{7}, \overline{10}\} = H + \overline{1}$$

$$\overline{\overline{2}} = \{\overline{2}, \overline{5}, \overline{8}, \overline{11}\} \qquad \overline{\overline{8}} = \{\overline{2}, \overline{5}, \overline{8}, \overline{11}\} = H + \overline{2}$$

$$\overline{\overline{3}} = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} = H \qquad \overline{\overline{9}} = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} = H$$

$$\overline{\overline{4}} = \{\overline{1}, \overline{4}, \overline{7}, \overline{10}\} = H + \overline{1} \qquad \overline{\overline{10}} = \{\overline{1}, \overline{4}, \overline{7}, \overline{10}\} = H + \overline{1}$$

$$\overline{\overline{5}} = \{\overline{2}, \overline{5}, \overline{8}, \overline{11}\} = H + \overline{2} \qquad \overline{\overline{11}} = \{\overline{2}, \overline{5}, \overline{8}, \overline{11}\} = H + \overline{2}$$

Portanto, $\mathbb{Z}_{12}/H = \{\overline{\overline{0}},\ \overline{\overline{1}},\ \overline{\overline{2}}\}$.

Vimos que se N é subgrupo normal de G, então está bem definida uma operação em G/N, herdada de G. Ainda, para todos $\overline{a}, \overline{b}, \overline{c} \in\ G/N$, $\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + \overline{b+c} = \overline{a + (b+c)} = \overline{a+b} + \overline{c} = (\overline{a} + \overline{b}) + \overline{c}$, que nos diz que a operação em G/N é associativa. Ainda, $\overline{0}$ é o elemento neutro e $-(\overline{g}) = \overline{-g}$, para todo $g \in G$. Assim, G/N herda a estrutura de grupo de G. Herda ainda outras propriedades, conforme a proposição a seguir, na qual utilizaremos a notação multiplicativa para o grupo .

Proposição 2.4. *Seja G grupo e H subgrupo normal de G. Se G é abeliano, então $\overline{G} = G/H$ também é abeliano. E se G é cíclico, então $\overline{G}$ também é cíclico.*

Demonstração: Tomando $\overline{x}, \overline{y} \in \overline{G}$, temos que $\overline{x}.\overline{y} = \overline{xy} = \overline{yx} = \overline{y}.\overline{x}$. Se G é cíclico, temos $G = \langle x \rangle = \{x^m;\ m \in \mathbb{Z}\}$. Então, para todo $\overline{y} \in \overline{G}$ temos que $y \in G$. Assim, $y = x^m$ para algum $m \in \mathbb{Z}$. Segue que $\overline{y} = \overline{x^m} = (\overline{x})^m \in \langle \overline{x} \rangle = \{(\overline{x})^k; k \in \mathbb{Z}\}$. Portanto, $\overline{G} = \langle \overline{x} \rangle$.

□

Veremos agora um teorema que relaciona as ordens de um grupo, de um subgrupo normal dele e do quociente entre os dois.

Teorema 2.5 (Lagrange). *Seja G grupo finito e N subgrupo normal de G. Então*

$$|G| = |N|(G : N)$$

sendo $(G:H)$ *a ordem de* $G/N = \{gN\ ;\ g \in G\}$.

Demonstração: Como G é finito, podemos supor que existe um número também finito $s \geq 1$ de classes laterais direitas de H, duas a duas distintas, tais que $G/H = \{Hx_1, ..., Hx_s\}$, para certos elementos $x_1, ..., x_s$ de G. Sendo distintas, as classes laterais são também disjuntas, pois assumem as propriedades das classes de equivalência, detalhadas na Proposição 2.2. Então $G = Hx_1 \cup ... \cup Hx_s$, donde $|G| = |Hx_1| + ... + |Hx_s|$. Mas $|Hx_k| = |H|$, para cada k, $1 \leq k \leq s$. De fato, $hx_k \mapsto h$ é bijetiva. Então $|G| = s|H|$ e $\dfrac{|G|}{|H|} = |G/H| = s$.

□

Sejam G_1 e G_2 dois grupos e φ uma função de G_1 em G_2. Diz-se que φ é um **homomorfismo** se, para todo $x, y \in G_1$, temos $\varphi(xy) = \varphi(x)\varphi(y)$. Claro que as operações podem ser diferentes (G_1 pode ser multiplicativo e G_2 aditivo, por exemplo). Note que $f(1_{G_1}) = 1_{G_2}$ e $f(x)^{-1} = f(x^{-1})$. De fato, $f(1_{G_1}) = f(1_{G_1}1_{G_1}) = f(1_{G_1})f(1_{G_1})$. Logo $f(1_{G_1}) = 1_{G_2}$. E $f(x)f(x)^{-1} = 1_{G_2} = f(1_{G_1}) = f(xx^{-1}) = f(x)f(x^{-1})$. Um homomorfismo que seja bijetivo é chamado de **isomorfismo**. Um isomorfismo definido do grupo G no próprio G é denominado **automorfismo**.

Exemplo 2.6. *Dado um grupo cíclico* $G = \langle g \rangle$ *de ordem n, a aplicação que associa g com* $\overline{1}$ *é um isomorfismo entre G e* $\mathbb{Z}_n$. *Ainda mais, todo grupo G de ordem p, com p primo, é cíclico. De fato, utilizando o Teorema de Lagrange (Teorema 2.5), dado* $g \in G \backslash \{1\}$, *a ordem do sugbrupo* $\langle g \rangle$ *divide* $p = |G|$. *Logo,* $|\langle g \rangle| = |G|$, *pois p é primo. Portanto,* $G = \langle g \rangle \cong \mathbb{Z}_p$.

Outro exemplo importante é a projeção canônica. Se H é um subgrupo normal de G, então verifica-se diretamente que é um homomorfismo a aplicação (projeção canônica)

$$\begin{aligned} \pi : G &\longrightarrow G/H \\ g &\longmapsto g + H. \end{aligned}$$

O **núcleo** de um homomorfismo $\varphi : G \to H$, denotado por $\mathrm{Ker}(\varphi)$, é definido como o conjunto $\mathrm{Ker}(\varphi) = \{x \in G : \varphi(x) = e\}$. Se $\varphi : G \to H$ é homomorfismo de grupos, então o núcleo de φ é subgrupo normal de G e o conjunto imagem de φ é subgrupo de H. Verifica-se isso diretamente.

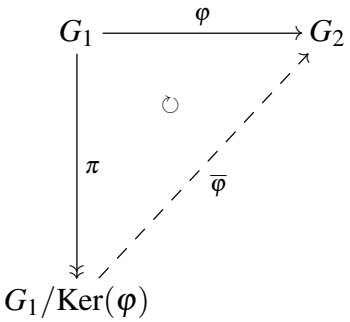
Proposição 2.7. *Seja* $\varphi : G_1 \to G_2$ *homomorfismo de grupos (denotados aditivamente). Então* φ *é injetivo se, e somente se,* $\mathrm{Ker}(\varphi) = \{0\}$.

Demonstração: ($\Rightarrow$) Sejam $a, b \in \mathrm{Ker}(\varphi)$. Então $\varphi(a) = \varphi(b) = 0$. Como φ é homomorfismo, $0 = \varphi(0)$. Como φ é injetivo, temos $a = b = 0$.

($\Leftarrow$) Sejam $a,b \in G_1$ tais que $\varphi(a) = \varphi(b)$. Logo, $\varphi(a) - \varphi(b) = 0$. Sendo φ um homomorfismo, temos $\varphi(a) - \varphi(b) = \varphi(a-b)$, então $a-b \in \text{Ker}(\varphi)$. Mas $\text{Ker}(\varphi) = \{0\}$, logo $a = b$ e φ é injetivo.

□

Teorema 2.8 (dos Homomorfismos)**.** *Seja $\varphi : G_1 \to G_2$ homomorfismo de grupos. Existe um único isomorfismo $\overline{\varphi}$ que torna o diagrama seguinte comutativo, isto é, $\varphi = \overline{\varphi} \circ \pi$.*



Demonstração: Dado $\overline{a} \in G_1/\text{Ker}(\varphi)$, definimos $\overline{\varphi}(\overline{a}) = \varphi(a)$. Primeiramente, $\overline{\varphi}$ está bem definido, no sentido de que $\varphi(a) = \varphi(b)$ para qualquer $b \in \overline{a}$. De fato, $b \in \overline{a} \quad \Rightarrow \quad \overline{b} = \overline{a}$ pela Proposição 2.2. Daí, $\varphi(a) = \overline{\varphi}(\overline{a}) = \overline{\varphi}(\overline{b}) = \varphi(b)$. Vejamos que $\overline{\varphi}$ é homomorfismo: $\overline{\varphi}(\overline{a}+\overline{b}) = \overline{\varphi}(\overline{a+b}) = \varphi(a+b) = \varphi(a)+\varphi(b) = \overline{\varphi}(\overline{a})+\overline{\varphi}(\overline{b})$. Agora vejamos que $\overline{\varphi}$ é injetiva. Seja $\overline{a} \in \text{Ker}(\overline{\varphi})$. Então $\overline{\varphi}(\overline{a}) = 0$, ou seja, $\overline{\varphi}(\overline{a}) = \varphi(a) = 0$. Assim, $a \in \text{Ker}(\varphi)$ e, portanto, $\overline{a} = \overline{0}$ em $G_1/Ker(\varphi)$. Logo, $\text{Ker}(\overline{\varphi} = \{\overline{0}\}$. Pela Proposição 2.7, $\overline{\varphi}$ é injetiva. A sobrejetividade é óbvia. Portanto, $\overline{\varphi}$ é isomorfismo e por definição $\overline{\varphi} \circ \pi = \varphi$ (torna o diagrama comutativo). Falta verificar a unicidade de $\overline{\varphi}$. Suponha $\overline{\rho}$ isomorfismo e $\overline{\rho} \circ \pi = \varphi$. Então $\varphi(a) = \overline{\rho}(\overline{a})$, para todo $\overline{a} \in G_1/\text{Ker}(\varphi)$, isto é, $\overline{\rho} = \overline{\varphi}$ □

A partir de agora estudaremos os grupos solúveis, que serão utilizados no próximo capítulo para estudar a resolubilidade das equações polinomiais.

Um grupo G é chamado de **grupo solúvel** quando admite subgrupos $G_0 = \{1\}$, $G_n = G$ e $G_1, G_2, ..., G_{n-1}$, tais que para todo $i \in \{0, ..., n\}$, G_{i-1} é subgrupo normal de G_i e G_i/G_{i-1} é abeliano.

Todo grupo abeliano é solúvel, pois basta tomar $n = 1$ e temos $G_0 = \{1\} \trianglelefteq G = G_1$.

O grupo de permutações de três elementos, denotado por S_3, é solúvel. Primeiramente, é conveniente denotar uma permutação $\sigma : \{1,2,3\} \to \{1,2,3\}$ por $\sigma = (\sigma(1)\ \sigma(2)\ \sigma(3))$. Com isto, verifica-se diretamente que $S_3 = \{id, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$, onde $\alpha = (231)$ e $\beta = (213)$. Definindo $A_3 := \langle \alpha \rangle = \langle id, \alpha, \alpha^2 \rangle$, obtemos um subgrupo normal de S_3 e ainda, pelo Teorema de Lagrange, $|S_3/A_3| = \dfrac{|S_3|}{|A_3|} = 2$. Segue que S_3/A_3 é abeliano, pois grupos de ordem 2 são abelianos, conforme o Exemplo 2.6. Logo, $\{1\} \trianglelefteq A_3 \trianglelefteq S_3$, donde conclui-se que S_3 é solúvel.

Proposição 2.9. *Seja G um grupo solúvel, H subrupo de G e N subgrupo normal de G. Então H e G/N são solúveis.*

Demonstração: A demonstração pode ser encontrada em [4, Proposição 12].

Um elemento $g \in S_n$ é dito **r-ciclo** se existe um subconjunto $\{j_1, j_2, ..., j_r\}$ de elementos diferentes de $\{1,2,...,n\}$ tal que, para todo $i \in \{1,...,n\}\backslash\{j_1, j_2, ..., j_r\}$, $g(i) = i$ e

$$g(j_i) = j_{i+1}, \text{ para todo } i \in \{1,2,...,r-1\}, \;\; g(j_r) = j_1.$$

O número r é denominado o **comprimento** do ciclo g e é denotado por $r = |g|$. Um elemento $g \in S_n$ é uma **transposição** se g é um 2-ciclo, isto é, existe $i \neq j$ tal que $g = (ij)$. Se α, β ciclos em S_n (possivelmente de comprimento diferente de n), dizemos que α e β são **disjuntos** caso não exista j tal que $\alpha(j) \neq j$ e $\beta(j) \neq j$.

Por exemplo, $g = (231)$ é um 3-ciclo. Já $\alpha = (12)$ e $\beta = (345)$ são ciclos disjuntos em S_n, para $n \geq 5$. Por outro lado, $\chi = (123)$ e $\delta = (145)$ não são disjuntos, pois $\chi(1) = 2 \neq 1$ e $\delta(1) = 4 \neq 1$.

Proposição 2.10. *Seja α um r-ciclo em S_n. Se $\alpha = \gamma_1 ... \gamma_k$, onde $\gamma_1, ..., \gamma_k$ são ciclos em S_n, dois a dois disjuntos, então*

$$|\alpha| = \text{mmc}\{|\gamma_1|, ..., |\gamma_k|\}.$$

Se $g \in S_n$ é tal que $g \neq 1$, então g pode ser escrito como o produto de ciclos disjuntos de comprimentos maiores ou iguais a 2. Essa fatoração é única a menos da ordem dos fatores.

Demonstração: Ver [3, Proposição V.10.5, p. 199].

Um elemento g de S_n é uma permutação **par** quando pode ser escrito como o produto de um número par de transposições. Adotaremos aqui uma outra notação para uma permutação, na qual indicaremos apenas os elementos que não são fixados. Assim, denotaremos por (23) , por exemplo, a transposição (13245), na qual os elementos 1, 4 e 5 foram fixados. A identidade será denotada simplesmente por (1).

Seja A_n um subconjunto de S_n definida por $A_n = \{\alpha \in S_n$ é permutação par $\}$. Esse conjunto é denominado **grupo alternado** ou **grupo das permutações pares** de S_n.

Proposição 2.11. *O grupo alternado A_n é subgrupo de S_n e tem índice 2.*

Demonstração: Seja $\gamma : S_n \to \{-1, +1\}$ tal que $\gamma(g) = 1$ se g é par e $\gamma(g) = -1$ se g é ímpar. A função γ é claramente um homomorfismo sobrejetor e $\text{Ker}(\gamma) = A_n$. Portanto, o resultado segue do Teorema 2.8.

□

Por exemplo, A_4 é subgrupo normal de S_4. Diretamente verifica-se que o conjunto $V_4 := \{(1);(12)(34);(13)(24);(14)(23)\}$ é subgrupo normal de A_4. Temos portanto uma cadeira de subgrupos normais $\{1\} \trianglelefteq H \trianglelefteq A_4 \trianglelefteq S_4$ que garante que S_4 é solúvel. De fato, os quocientes S_4/A_4 e A_4/V_4 possuem ordem prima e portanto são abelianos (Exemplo 2.6).

Se $g \in S_n$, com $n \geq 2$, e $g = (a_{11}a_{12}...a_{1r_1})...(a_{i1}a_{i2}...a_{ir_i})$ é a sua decomposição em ciclos disjuntos com $r_1 \leq r_2 \leq ... \leq r_i$, dizemos que $\{r_1,...,r_i\}$ é o **tipo de decomposição** de g.

Lema 2.12. *Seja $g \in S_n$ tal que $g = (a_{11}a_{12}...a_{1r_1})(a_{21}a_{22}...a_{2r_2})...(a_{i1}a_{i2}...a_{ir_i})$ é produto de ciclos disjuntos.*

1) *Seja $\tau \in S_n$. Então*

$$\tau g \tau^{-1} = (\tau(a_{11})\tau(a_{12})...\tau(a_{1r_1}))(\tau(a_{21})\tau(a_{22})...\tau(a_{2r_1}))...(\tau(a_{i1})\tau(a_{i2})...\tau(a_{ir_i}))$$

é produto de ciclos disjuntos. Em particular, g e $\tau g \tau^{-1}$ têm o mesmo tipo de decomposição.

2) *Se $g, g' \in S_n$ são permutações com o mesmo tipo de decomposição, então existe $\tau \in S_n$ tal que $g' = \tau g \tau^{-1}$.*

3) *Se $g, g' \in S_n$ são permutações com o mesmo tipo de decomposição e g fixa no mínimo dois elementos de $\{1,...,n\}$, então existe $\mu \in A_n$ tal que $g' = \mu g \mu^{-1}$.*

Demonstração: A demonstração pode ser encontrada em [3, Lema V.10.16, p. 205].

Proposição 2.13. *Todo elemento de A_n é um produto de 3-ciclos.*

Demonstração: Seja (ijk) um 3-ciclo qualquer. Podemos escrever $(ijk) = (ik)(ij)$. Portanto, um 3-ciclo é uma permutação par. Agora, dadas duas transposições disjuntas, $g = (ij)$ e $h = (kl)$, podemos escrever o produto entre elas como

$$hg = (kl)(ij) = (kl)(ki)(ik)(ij) = (kil)(ijk).$$

Então, o produto entre essas transposições pode ser escrito como o produto de dois 3-ciclos. Se g e h não forem disjuntas, com $g = (ij)$ e $h = (jk)$, por exemplo, então $hg = (jk)(ij) = (ijk)$, um 3-ciclo. Portanto, como queríamos demonstrar, A_n é o sugrupo de S_n gerado pelos 3-ciclos de S_n.

□

Um grupo G é dito **simples** se seus únicos subgrupos normais são os triviais. Veremos agora que esse é o caso dos grupos alternados em que n é igual ou superior a 5.

Teorema 2.14. *A_n é grupo simples, para todo $n \geq 5$.*

Demonstração: Seja H um subgrupo normal de A_n, com $H \neq \{1\}$. Deve-se verificar que $H = A_n$. Lembre que A_n é o subgrupo de S_n gerado pelos 3-ciclos, isto é,

$$A_n = \left\langle \left\{ \text{3-ciclos em } S_n \right\} \right\rangle.$$

Assim, basta mostrar que todo 3-ciclo está em H. Veremos ainda que é suficiente mostrar apenas que *existe um* 3-ciclo em H. De fato, se $(ijk) \in H$, fixamos (abc) um 3-ciclo arbitrário. O 3-ciclo (ijk) fixa $n-3$ elementos e como $n \geq 5$, temos $n-3 \geq 2$. Pelo item (3) do Lema 2.12, existe $\sigma \in A_n$ tal que $\sigma(ijk)\sigma^{-1} = (abc)$. Mas $(ijk) \in H$ e $H = \sigma H \sigma^{-1}$, para todo $\sigma \in A_n$. Logo, $(abc) \in H$.

Para verificar que sempre existe um 3-ciclo $(ijk) \in H$, iniciamos escolhendo $\sigma \in H$, com $\sigma \neq 1$. Seja

$$m = |\sigma| = \min\{n \in \mathbb{N};\ \ \sigma^n = 1\}.$$

Sejam $\sigma_1, \ldots, \sigma_k$ ciclos irredutíveis tais que $\sigma = \sigma_1\sigma_2...\sigma_k$ e $|\sigma| = \text{mmc}\{|\sigma_1|, ..., |\sigma_k|\}$, onde $|\sigma_i|$ é o comprimento do ciclo. Como $\sigma \neq 1$, temos $|\sigma| > 1$. Seja $p \in \mathbb{N}$, p primo tal que $p|m$. Então existe $\alpha \in \mathbb{N}$ tal que $m = p\alpha$ e $\alpha = m/p < m$. Além disso, $\sigma^{m/p} \neq 1$, pela definição de m, e $(\sigma^{m/p})^p = \sigma^m = 1$. Se fizermos $\tau = \sigma^{m/p}$, então $\tau^p = 1$ e $p = |\tau|$. Pela Proposição 2.10, $\tau = \rho_1\rho_2...\rho_s$ produto de ciclos disjuntos e $|\tau| = mmc\{|\rho_1|, ..., |\rho_s|\}$. Como $p = |\tau|$, então $|\rho_j| = p$, para todo $j \in \{1, ..., s\}$. Portanto, ρ_j é p-ciclo para todo $j \in \{1, ..., s\}$.

Vamos estudar as possibilidades para p.

Caso 1: $p = 2$. Seja H subgrupo normal de A_n. Temos $\tau = \rho_1\rho_2...\rho_s$, onde cada ρ_i é uma transposição (2-ciclo). Mas $\tau \in A_n$, logo, s é par (≥ 2) e $\tau = (ab)(cd)\rho_3...\rho_s$. Seja $\sigma = (abc)$. Note que, pelo item (1) do Lema 2.12, temos

$$\sigma\tau\sigma^{-1} = (\sigma(a)\sigma(b))(\sigma(c)\sigma(d))\rho_3\rho_4...\rho_s = (bc)(ad)\rho_3...\rho_s,$$

ou seja, σ fixa $\rho_3, ..., \rho_s$ (pela definição de σ e de τ). Então

$$\sigma\tau\sigma^{-1}\tau^{-1} = ((bc)(ad)\rho_3...\rho_s)\tau^{-1} = (bc)(ad)\rho_3...\rho_s((ab)(cd)\rho_3...\rho_s)^{-1} =$$

$$(bc)(ad)\rho_3...\rho_s\rho_s^{-1}...\rho_3^{-1}(cd)^{-1}(ab)^{-1} = (bc)(ad)(cd)(ab) = (ac)(bd).$$

Temos que $\tau \in H$ e $H = \sigma H \sigma^{-1}$, pois H é subgrupo normal de A_n. Portanto, $\sigma\tau\sigma^{-1} \in H$. Além disso, como $\tau \in H$, temos $\tau^{-1} \in H$. Como $\sigma\tau\sigma^{-1}\tau^{-1} = (ac)(bd)$, então $(ac)(bd) \in H$. Seja $k \in H$ tal que $k \neq a, b, c, d$ (isso é possível pois $n \geq 5$). Então $(akc)(ac)(bd)(akc)^{-1} \in H$, pois $(akc), (akc)^{-1} \in A_n$ e $(ac)(bd) \in H$. Como (akc) é um 3-ciclo, então $(akc)^3 = 1$. Consequentemente, $(akc)(akc)^2 = 1$ e $(akc)^{-1} = (akc)^2$, o que implica em que $(akc)^{-1} =$

$(akc)(akc)$. Portanto,

$$(akc)(ac)(bd)(akc)^{-1} = (akc)(ac)(bd)(akc)(akc) = (ka)(bd) \in H.$$

Segue que $(ac)(bd)((ka)(bd))^{-1} \in H$. Como $(ac)(bd) \in H$ e $((ka)(bd))^{-1} = (bd)^{-1}(ka)^{-1}$, temos

$$(ac)(bd)((ka)(bd))^{-1} = (ac)(bd)(bd)^{-1}(ka)^{-1} = (ac)(ka) = (kca).$$

Como a primeira expressão da igualdade está em H, temos que (kca) também está em H. Logo, H possui um 3-ciclo.

Caso 2: $p = 3$. Seja $\tau = \rho_1 ... \rho_s$, com ρ_i um 3-ciclo. Se $s = 1$, então $\tau = \rho_1$ e existe um 3-ciclo que pertence a H. Se $s \geq 2$, então $\tau = (abc)(def)\rho_3 ... \rho_s$. Seja $\sigma = (bcd)$. Então $\sigma \in A_n$ e σ fixa $\rho_3 ... \rho_s$. Assim,

$$\sigma\tau\sigma^{-1} = (bcd)\tau(bcd)^{-1} = (bcd)(abc)(def)\rho_3 ... \rho_s(bcd)^{-1} =$$

$$(\sigma(a)\sigma(b)\sigma(c))(\sigma(d)\sigma(e)\sigma(f))\rho_3 ... \rho_s = (acd)(bef)\rho_3 ... \rho_s.$$

Temos que $\sigma\tau\sigma^{-1} \in H$ e, como $\tau \in H$, então $\tau^{-1} \in H$. Portanto, $(\sigma\tau\sigma^{-1})\tau^{-1} \in H$. Mas

$$(\sigma\tau\sigma^{-1})\tau^{-1} = (acd)(bef)\rho_3 ... \rho_s(\rho_s^{-1} ... \rho_3^{-1})(def)^{-1}(abc)^{-1} = (acd)(bef)(fed)(acd),$$

que, por sua vez, é igual a $(adbce)$, que é um 5-ciclo. Com isso, mostramos que existe um 5-ciclo em H, o que reduz o caso 2 ao caso 3.

Caso 3: $p \geq 5$. Seja $\sigma = \rho_1 ... \rho_s$, com ρ_i p-ciclo. Então $\rho_1 = (a_1 a_2 ... a_p)$. Seja $\sigma = (a_1 a_2 a_3)$. Então $\sigma\tau\sigma^{-1} = \sigma((a_1 a_2 ... a_p)\rho_2 ... \rho_s)\sigma^{-1} = (\sigma(a_1) ... \sigma(a_p))\rho_2 ... \rho_s = (a_2 a_3 a_1 a_4 ... a_p)\rho_2 ... \rho_s$. Agora, $(\sigma\tau\sigma^{-1})\tau^{-1}$ está em H e

$$(\sigma\tau\sigma^{-1})\tau^{-1} = (a_2 a_3 a_1 a_4 ... a_p)\rho_2 ... \rho_s(\rho_s^{-1} ... \rho_2^{-1}(a_1 a_2 ... a_p)^{-1}) =$$

$$(a_2 a_3 a_1 a_4 ... a_p)(a_1 a_2 ... a_p)^{-1} = (a_2 a_3 a_1 a_4 a_5 ... a_p)(a_{p-1} a_{p-2} ... a_2 a_1 a_p).$$

Fazendo $t = (a_2 a_3 a_1 a_4 a_5 ... a_p)(a_{p-1} a_{p-2} ... a_2 a_1 a_p)$, temos

$$a_1 \longrightarrow a_p \longrightarrow a_2 \quad \Rightarrow \quad a_1 \longrightarrow a_2$$

$$a_2 \longrightarrow a_1 \longrightarrow a_4 \quad \Rightarrow \quad a_2 \longrightarrow a_4$$

$$a_3 \longrightarrow a_2 \longrightarrow a_3 \quad \Rightarrow \quad a_3 \longrightarrow a_3$$

$$a_4 \longrightarrow a_3 \longrightarrow a_1 \quad \Rightarrow \quad a_4 \longrightarrow a_1$$

Assim, para $s \leq i \leq p$, temos $a_i \longrightarrow a_{i-1} \longrightarrow a_i$. Ou seja, $t(a_i) = a_i$. Portanto, $(\sigma\tau\sigma^{-1})\tau^{-1} = (a_1 a_2 a_4)$, que é um 3-ciclo em H.

□

Assim mostramos que para $n \geq 5$, A_n não possui subgrupos normais diferentes dos triviais. Com isso fica demonstrado que, para esses casos, S_n não é solúvel. De fato, se S_n fosse solúvel, pela Proposição 2.9, A_n seria solúvel. Mas isso não ocorre porque a única cadeia (de subgrupos normais) para A_n é $\{1\} \trianglelefteq \{A_n\}$, já que A_n é simples. Mas nessa cadeia, o quociente é o próprio A_n, não abeliano.

No próximo capítulo veremos que a não solubilidade de S_n para $n \geq 5$ pode ser utilizada para justificar a não solubilidade da equação geral de grau maior ou igual a 5.

3 CORRESPONDÊNCIA GALOISIANA E RESOLUBILIDADE POR RADICAIS

Iniciaremos este capítulo com uma breve introdução sobre a teoria de corpos. Em especial, estudaremos a correspondência galoisiana entre os corpos intermediários de uma extensão galoisiana de corpos e os subgrupos do grupo de Galois da extensão. Esta correspondência permite demonstrar o teorema de maior interesse para o nosso trabalho - Teorema 3.6 - que estabelece a condição para a resolubilidade de uma equação polinomial por meio de radicais. Concluiremos o trabalho com aplicações do teorema e com a explicação do motivo da existência das fórmulas resolutivas para equações polinomiais de grau menor ou igual a 4, e da não existência de fórmula análoga para o polinômio geral de grau maior ou igual a 5.

3.1 NOÇÕES DA TEORIA DE CORPOS

Seja um conjunto A não vazio, munido das operações de adição e multiplicação. Dizemos que A é um **anel** quando A, munido da adição, é grupo abeliano e o produto é associativo e distributivo com relação à adição. O **oposto** de x é denotado por $-x$ e a operação definida por $x-y=x+(-y)$ é chamada de **subtração** em A. Um anel que possua um elemento 1 tal que, para todo $x \in A$, $x1 = 1x = x$ é um **anel com unidade**. Se em um anel o produto também apresenta a comutatividade, então dizemos que A é um **anel comutativo**. Um anel **sem divisores de zero** é um anel para o qual $x = 0$ ou $y = 0$, sempre que dois elementos x, y tiverem o produto nulo. Como somente utilizaremos este caso, assumiremos sempre que um **anel** significa um anel comutativo, com unidade, e sem divisores de zero.

O exemplo mais conhecido é o anel dos números inteiros, com as operações usuais. Outro exemplo que utilizaremos bastante é o anel dos polinômios. Considere o anel A e seja

$$A[x] = \{p(x) : p(x) = \sum_{i=0}^{n} a_i x^i, a_i \in A;\ n \in \mathbb{N}\}.$$

Então, $A[x]$ é o conjunto dos polinômios sobre a indeterminada x com coeficientes em A. Esse conjunto também forma um anel, dito o **anel dos polinômios** sobre x, com coeficientes em A.

Dados $p(x) = \sum_{i=0}^{n} a_i x^i$ e $q(x) = \sum_{j=0}^{m} b_j x^j$, a adição é definida como

$$p(x) + q(x) = \sum_{i=0}^{m+n} (a_i + b_i) x^i,$$

Completa-se com coeficientes nulos, se necessário. O produto é definido como

$$p(x)q(x) = \sum c_k x^k, \text{ onde } c_k = \sum_{i+j=k} a_i b_j.$$

Verifica-se diretamente que de fato $A[x]$ é um anel.

Se no anel A (comutativo, com unidade e sem divisores de zero), todo elemento não nulo $x \in A$ admitir um elemento $x^{-1} \in A$ tal que $xx^{-1} = 1$, então A é chamado de **corpo**. O principal exemplo que utilizaremos neste trabalho é o corpo dos números racionais, denotado por $\mathbb{Q}$. O conjunto $\mathbb{R}$ dos números reais e o conjunto $\mathbb{C}$ dos números complexos são outros exemplos de corpos. Neste trabalho, sempre que nos referirmos a um corpo F, estaremos assumindo que $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$.

Seja A um anel e $B \subset A$, B não vazio. Suponha que B é fechado para as operações de adição e multiplicação de A, isto é, para todo $x, y \in B$, temos $x+y,\ xy \in B$. O conjunto B com a restrição das operações de A é dito um **subanel** de A.

Pode-se verificar diretamente que com estas operações, B continua sendo um anel. Isto ainda é equivalente a assumir outras três condições: o elemento neutro aditivo de A pertence a B, e para todos $x, y \in B$, temos $xy,\ x - y \in B$ [4, Proposição 1, p. 43].

Fixado $n \in \mathbb{Z}$, o conjunto $n\mathbb{Z} = \{n\alpha,\ \alpha \in \mathbb{Z}\}$ já estudado no capítulo anterior, é subanel de $\mathbb{Z}$.

Considere dois anéis, A e A', com elementos neutros aditivos, 0 e $0'$, e unidades 1 e $1'$, respectivamente. Uma função $f : A \to A'$ é chamada de **homomorfismo** de A em A' se, para todo $x, y \in A$, temos $f(x+y) = f(x) + f(y)$ e $f(xy) = f(x)f(y)$. Segue desta definição que $f(0) = 0'$ e $f(x^{-1}) = f(x)^{-1}$, para todo elemento não nulo $x \in A$.

Seja K um corpo e $F \subset K$. Se F, com a restrição das operações de K também for um corpo, dizemos que F é **subcorpo** de K. Dizemos também que K é uma **extensão** de F, denotada por $K|F$. Um elemento $\alpha \in K$ é **algébrico** sobre F se existe um polinômio não nulo $f(x) \in F[x]$ tal que $f(\alpha) = 0$. Se não existir tal $f(x)$ dizemos que α é **transcendente** sobre F. Se todo $\alpha \in K$ é algébrico sobre F, então $K|F$ é uma **extensão algébrica**. Por exemplo, $i = \sqrt{-1}$ é algébrico sobre $\mathbb{Q}$, pois é raiz do polinômio $x^2 + 1 \in \mathbb{Q}[x]$. Por outro lado, não

existe $f(x) \in \mathbb{Q}[x]$, tal que $f(\pi) = 0$ [8, Teorema de Lindemann-Weierstrass, p. 134], isto é, π é transcendente sobre $\mathbb{Q}$.

Seja $K|F$ extensão de corpos. Dizemos que K é uma **extensão simples** de F se existe $\alpha \in K$, α algébrico sobre F, tal que K é a **adjunção** de α sobre F, ou seja:

$$K = F(\alpha) := \{f(\alpha);\ f(x) \in F[x]\}.$$

Por exemplo, se $\alpha = \sqrt{2}$ e $F = \mathbb{Q}$, pelo algoritmo da divisão de polinômios, temos que

$$f(x) = q(x)(x^2 - 2) + r(x),$$

com grau de $r(x) < 2$; isto é, $r(x) = ax + b$, para certos $a, b \in \mathbb{Q}$. Assim, $f(\sqrt{2}) = r(\sqrt{2}) = a\sqrt{2} + b$, donde concluímos que

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2};\ a, b \in \mathbb{Q}\}.$$

Pode-se verificar diretamente que de fato $F(\alpha)$ é um corpo. Ainda, o processo de adjunção pode ser repetido para mais elementos. Por exemplo,

$$\mathbb{Q}(\sqrt{2},\ i) := (\mathbb{Q}(\sqrt{2}))(i).$$

Um corpo K, gerado pela adjunção de α_1, α_2, ...,α_n a F, tais que $K = F(\alpha_1, \alpha_2, ..., \alpha_n)$ é chamado de extensão **finitamente gerada** de F.

Uma extensão de corpos $K|F$ pode ser vista como um espaço vetorial de K sobre F. Se a dimensão desse espaço for finita, dada por n, dizemos que K é uma **extensão finita de grau** n sobre F, e denotaremos esse grau por $[K : F]$.

Dados os corpos F, K e L tais que $F \subset K \subset L$, suponha $n = [L : F]$, $r = [K : F]$ e $s = [L : K]$, isto é, todas as dimensões finitas. Então

$$[L : F] = [K : F][L : K]. \tag{5}$$

A demonstração pode ser encontrada em [6, Lema 11.2, p. 223]. Ainda, por indução pode-se estender o resultado para o caso com n corpos, $n > 2$ [6, Corolário 11.1, p. 223].

Se F é um corpo e $f(x) \in F[x]$ é um polinômio, então existe uma extensão $K|F$ que contém todas as raízes de $f(x)$ [6, Teorema de Kronecker, p.228]. Como consequência, se F é um corpo e $f_i(x) \in F[x], i \in \{1, ..., n\}$, então existe uma extensão $K|F$ onde $f_1(x), f_2(x), ..., f_n(x)$ possuem todas as suas raízes.

Nem sempre é necessária uma extensão de um corpo F para encontrar suas raízes. Pode ocorrer que todo polinômio $f(x) \in F[x]$ tenha suas raízes no próprio F. Nesse caso, dizemos que o corpo é **algebricamente fechado**. O Teorema Fundamental da Álgebra afirma que todo polinômio não constante $f(x) \in \mathbb{C}[x]$ possui ao menos uma raiz em $\mathbb{C}$. Isto quer dizer que $\mathbb{C}$ é algebricamente fechado.

Uma extensão de F que contenha todas as raízes de todos os polinômios de $F[x]$ é chamada um **fecho algébrico** de F. O único caso que utilizaremos neste trabalho é o corpo dos números complexos, que é o fecho algébrico de $\mathbb{Q}$, e de qualquer subcorpo $K : \mathbb{Q} \subset K \subset \mathbb{C}$. O fecho algébrico é único a menos de isomorfismo. Mais detalhes sobre o fecho algébrico, assim como sua construção, podem ser vistos em [8, p.11, 31, 40].

Seja um corpo F e um polinômio $f(x) \in F[x]$. Uma extensão $K|F$ que contenha todas as raízes $\alpha_1, ..., \alpha_n$ de $f(x)$ e seja da forma $K = F(\alpha_1,...,\alpha_n)$ é chamada de **corpo de decomposição** de $f(x)$. Seja um corpo F e uma família de polinômios de $F[x]$. Seja $A = \{x_1, ..., x_n\}$ o conjunto de todas as raízes de todos esses polinômios. Se $A \subset K$ e $K = F(A)$, então K é chamada de **corpo de decomposição** dessa família de polinômios. Dois corpos de decomposição de um polinômio fixado (ou de uma família deles) são isomorfos, isto é, o corpo de decomposição é único a menos de isomorfismo.

Teorema 3.1. *São equivalentes:*

i) K é o corpo de decomposição de alguma família de polinômios de $F[x]$;

ii) Se um polinômio de $F[x]$ possui uma raiz em K, então ele possui todas as raízes em K.

Demonstração: [6, Teorema 11.7, p. 236]

Uma extensão algébrica que satisfaça a qualquer das condições acima é chamada de **extensão normal**. A extensão de corpos $K|F$ é chamada de extensão **galoisiana** quando é finita e normal. Como primeiro exemplo, consideremos a extensão $\mathbb{C}|\mathbb{R}$. A dimensão de $\mathbb{C}$ como $\mathbb{R}$-espaço vetorial é 2, já que a base é $\{1, i\}$, onde $i = \sqrt{-1}$. É normal, pois $\mathbb{C}$ é o corpo de decomposição do polinômio $x^2 + 1 \in \mathbb{R}[x]$.

Sendo $i = \sqrt{-1}$, verifica-se diretamente que o conjunto $\{1, i, \sqrt{2}, i\sqrt{2}\}$ é uma base (como $\mathbb{Q}$-espaço vetorial) de $K = \mathbb{Q}(i, \sqrt{2})$ sobre $\mathbb{Q}$. Portanto, o grau $[K : \mathbb{Q}]$ é igual a 4. Além disso, K é corpo de decomposição do conjunto de polinômios $\{x^2 + 1, x^2 - 2\}$, ou simplesmente, K é o corpo de decomposição do polinômio $x^4 - x^2 - 2$. Temos, portanto, mais um exemplo de extensão galoisiana.

Exemplos interessantes de extensões galoisianas também podem ser obtidas considerando as raízes da unidade.

Definição 3.2. *Fixando um número natural n, uma* **raiz *n*-ésima da unidade** *é um número complexo ξ tal que $\xi^n = 1$. Caso $\xi^k \neq 1$, para todo natural k tal que $0 < k < n$, então dizemos que ξ é uma raiz n-ésima* **primitiva** *da unidade.*

Seja ξ uma raiz n-ésima primitiva da unidade. Expressando o número complexo na sua forma trigonométrica e utilizando a Fórmula de De Moivre, obtém-se que

$$\xi = \cos\frac{2\pi}{n} + i\text{sen}\frac{2\pi}{n}.$$

No caso particular $n = 3$, temos $\xi = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$, donde segue que $\xi^2 = -\frac{1}{2} - \frac{i\sqrt{3}}{2}$ e que $\xi^3 = 1$. Claro que $\xi^n = 1$, para todo $n \geq 3$ e n múltiplo de 3. Assim, percebe-se que o conjunto das raízes cúbicas da unidade é dado por $\mu_3 := \{1, \xi, \xi^2\}$ e que este conjunto é fechado para a multiplicação. A aplicação $\mu_3 \to \mathbb{Z}_3$ definida por $\xi \mapsto \bar{1}$ produz um isomorfismo.

Podemos então definir a extensão $\mathbb{Q}(\xi)|\mathbb{Q}$, que tem grau 3. A base é dada por $\{1, \xi, \xi^2\}$ e $\mathbb{Q}(\xi)$ é o corpo de decomposição de $x^3 - 1$. Note que as raízes cúbicas da unidade estão relacionadas ao polinômio $x^3 - 1$, mas esse polinômio não é o polinômio com coeficientes racionais de menor grau que tem ξ como raiz. De fato, como 1 é raiz, dividindo $x^3 - 1$ por $x - 1$ obtemos o polinômio $x^2 + x + 1$, que tem ξ e $\xi^2 = \overline{\xi}$ como raízes.

3.2 A CORRESPONDÊNCIA GALOISIANA

Seja $K|F$ extensão finita de corpos. O **grupo de Galois** de $K|F$, que denotaremos por $G(K;F)$, é o grupo de todos os automorfismos σ de K sobre F que restritos a F produzem a identidade de F, isto é, $\sigma(x) = x$, para todo $x \in F$. Tais funções são denominadas de F-automofismos de K. Assim,

$$G(K;F) = \{\sigma : K \to K \mid \sigma \text{ é } F\text{-automorfismo de } K\}.$$

Por exemplo, considere a extensão $\mathbb{C}|\mathbb{R}$. Vejamos que um elemento σ de $G(\mathbb{C};\mathbb{R})$ é a aplicação identidade e o outro, a conjugação complexa $a + bi \mapsto a - bi$. De fato, para quaisquer $a, b \in \mathbb{R}$, tem-se $\sigma(a + bi) = \sigma(a) + \sigma(b)\sigma(i) = a + b\sigma(i)$. Por outro lado, como $i^2 = -1$, temos que

$$-1 = \sigma(i^2) = \sigma(i)^2.$$

Logo, $\sigma(i)$ é i ou $-i$. Na primeira possibilidade, σ é aplicação identidade. Na segunda, é a conjugação complexa. Portanto, $G(\mathbb{C};\mathbb{R})$ é o grupo de ordem 2 (isto é, é isomorfo à $\mathbb{Z}_2$).

Há uma interpretação interessante dos F-automorfismos na Álgebra Linear. Vimos que K é um espaço vetorial sobre F de dimensão $[K:F]$. Assim, um F-automofismo σ de K é uma transformação linear bijetiva de K (isto é, um isomorfismo). De fato, σ é bijetiva por definição. Vamos verificar a linearidade. Para todo $\alpha \in F$ e todos $k_1, k_2 \in K$, tem-se $\sigma(\alpha k_1 + k_2) = \sigma(\alpha)\sigma(k_1) + \sigma(k_2)$. Como σ fixa F, a última expressão é igual a $\alpha\sigma(k_1) + \sigma(k_2)$. Um fato conhecido da Álgebra Linear é que um isomorfismo de espaços vetoriais transforma uma base do primeiro espaço numa base do segundo [1, Corolário 5.3.11, p. 173]. Vejamos em um exemplo como isto ocorre.

Retomemos o exemplo $K = \mathbb{Q}(\sqrt{2}, i)$, o corpo de decomposição de $\{x^2+1; x^2-2\}$ sobre $\mathbb{Q}$. Uma base para K como $\mathbb{Q}$-espaço vetorial é $\{1, i, \sqrt{2}, i\sqrt{2}\}$. Naturalmente, um elemento de $G(K;\mathbb{Q})$ é a aplicação identidade e qualquer outro $\mathbb{Q}$-automorfismo aplica o elemento 1 da base no próprio 1. Como $\sigma(i\sqrt{2}) = \sigma(i)\sigma(\sqrt{2})$, basta então conhecermos $\sigma(i)$ e $\sigma(\sqrt{2})$ para completarmos a definição de σ. De fato, o grupo de Galois $G(K;\mathbb{Q})$ tem quatro elementos: *id*, σ_1, σ_2 e σ_3, sendo

(i) $\sigma_1(i) = -i$ e $\sigma_1(\sqrt{2}) = \sqrt{2}$;

(ii) $\sigma_2(i) = i$ e $\sigma_2(\sqrt{2}) = -\sqrt{2}$;

(iii) $\sigma_3(i) = -i$ e $\sigma_3(\sqrt{2}) = -\sqrt{2}$.

O próximo teorema esclarece completamente porque não pode haver outros elementos no grupo de Galois do exemplo que acabamos de ver. Também relaciona este fato com os corpos de decomposição, estudados no final da seção anterior.

Teorema 3.3. *Seja K o corpo de decomposição de $f(x) \in F[x]$ e $\sigma \in G(K;F)$. Se α é uma raiz de $f(x)$, então $\sigma(\alpha)$ também o é.*

Demonstração: Suponha $f(x) = a_0 + a_1x + \ldots + a_nx^n \in F[x]$. então

$$0 = f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n$$

$$\Rightarrow 0 = \sigma(0) = \sigma(f(\alpha)) = a_0 + a_1\sigma(\alpha) + \ldots + a_n(\sigma(\alpha))^n.$$

Logo, $\sigma(\alpha)$ é também raiz de $f(x)$.

□

Em um exemplo anterior, $\mathbb{C}$ é o corpo de decomposição de $x^2+1 \in \mathbb{R}[x]$. Então $\sigma(i) = i$ ou $\sigma(i) = -i$ para um $\mathbb{R}$-automorfismo. $K = \mathbb{Q}(i, \sqrt{2})$ é o corpo de decomposição de $x^4 - x^2 - 2 = (x^2+1)(x^2-2)$. Assim, no primeiro caso, necessariamente $\sigma(i) = i$ ou $\sigma(i) = -i$. Note que no segundo, temos a explicação do motivo de não haver mais do que os quatro elementos estudados em $G(K;\mathbb{Q})$.

Passamos agora a estudar a correspondência galoisiana, conforme citado anteriormente. Seja $N|F$ uma extensão galoisiana de corpos e $G = G(N;F)$ o grupo de Galois correspondente. Consideremos o conjunto de todas as extensões intermediárias

$$\{N : F\} = \{L \ ; \ L \text{ é corpo e } F \ \subseteq \ L \ \subseteq \ N\}$$

e o conjunto de todos os subgrupos de G:

$$\{G : 1\} = \{H \ ; \ H \text{ é subgrupo de } \ G\}.$$

A um elemento L de $\{N : F\}$ está associado o grupo de Galois

$$G(N;L) = \{\sigma \in G \ ; \ \sigma(x) = x, \text{ para todo } x \in L\}.$$

Note que $G(N;L)$ é um subgrupo de G, isto é, $G(N;L) \in \{G : 1\}$. Ainda, é claro que se $L_1 = L_2 \in \{N : 1\}$ então $G(N;L_1) = G(N;L_2)$. Podemos então definir uma aplicação

$$\begin{array}{rccc} \varphi : & \{N : F\} & \longrightarrow & \{G : 1\} \\ & L & \longmapsto & G(N;L) \end{array}$$

Note que tem-se $\varphi(F) = G$ e $\varphi(N) = \{id\}$. Por outro lado, dado um subgrupo H de $G = G(N;F)$, isto é, um elemento H de $\{G : 1\}$, definimos o **corpo fixo** de H como

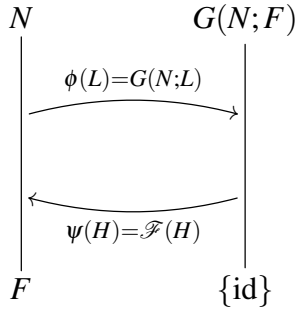
$$\mathscr{F}(H) = \{x \in N \ ; \ \sigma(x) = x, \text{ para todo } \sigma \in H\}.$$

Diretamente verifica-se que $\mathscr{F}(H)$ é um subcorpo de N e que se $H_1 = H_2 \in \{G : 1\}$, então $\mathscr{F}(H_1) = \mathscr{F}(H_2)$. Podemos então definir uma nova aplicação, representada abaixo.

$$\begin{array}{rccc} \psi : & \{G : 1\} & \longrightarrow & \{N : F\} \\ & H & \longmapsto & \mathscr{F}(H) \end{array}$$

Observa-se que $\psi(\{\text{id}\}) = N$ e que $\psi(G) = F$. Juntando todas as informações, podemos esquematizar as aplicações φ e ψ.

$$\Big\{L:\ L \text{ corpo e } F \subseteq L \subseteq N\Big\} \longleftrightarrow \Big\{H:\ H \text{ subgrupo de } G\Big\}$$



$$\phi(L) = \{\sigma \in G(N;F) \mid \sigma(x) = x, \text{ para todo } x \in L\} = G(N;L)$$
$$\psi(H) = \{x \in N \mid \tau(x) = x \text{ para todo } \tau \in H\} = \mathscr{F}(H)$$

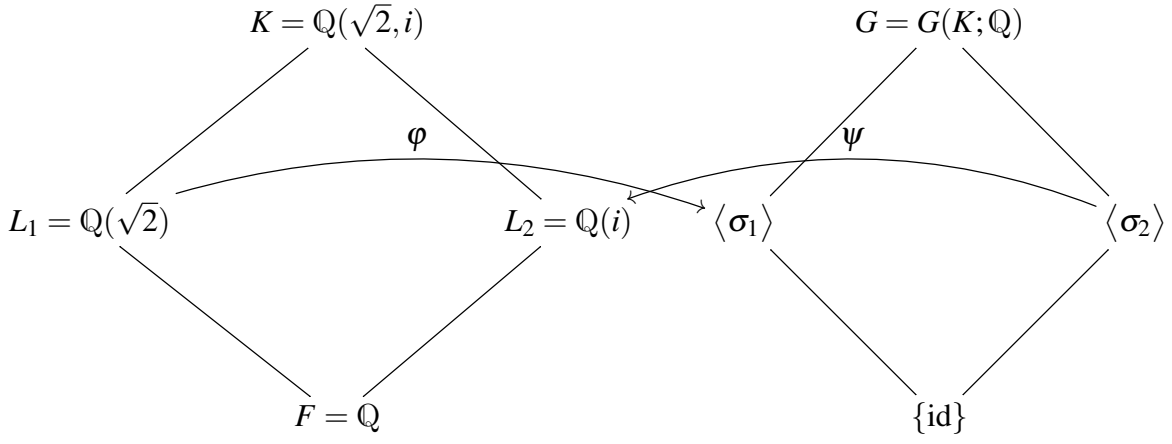
Vimos o exemplo da extensão galoisiana $K|\mathbb{Q}$, onde $K = \mathbb{Q}(\sqrt{2}, i)$ em que o grupo de Galois é $G(K;\mathbb{Q}) = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3\}$. Lembre que K é o corpo de decomposição do conjunto de polinômios $\{x^2-2,\ x^2+1\} \subseteq \mathbb{Q}[x]$. Vimos que σ_2 permuta as raízes $x_1 = \sqrt{2}$ e $x_2 = -\sqrt{2}$, e fixa as raízes $x_3 = i$ e $x_4 = -i$. Segue que $\sigma_2(a+bi) = a+bi$, para todos $a, b \in \mathbb{Q}$. Assim, σ_2 fixa $L_2 = \mathbb{Q}(i)$, isto é, $\sigma_2 \in G(K;L_2) = \varphi(L_2)$. Lembrando das definições de σ_1 e σ_3, temos que estes não são elementos de $G(K;L_2)$. Assim,

$$G(K;L_2) = \{\mathrm{id},\ \sigma_2\} = \langle \sigma_2 \rangle.$$

De maneira análoga, podemos verificar que

$$G(K;L_1) = \{\mathrm{id},\ \sigma_1\} = \langle \sigma_1 \rangle.$$

Neste caso, temos que $\psi\Big(\langle \sigma_1 \rangle\Big) = L_1$ e $\psi\Big(\langle \sigma_2 \rangle\Big) = L_2$.



As aplicações φ e ψ são inversas uma da outra e revertem a inclusão, conforme estabelece o próximo resultado. Há portanto uma bijeção entre $\{G:1\}$ e $\{N|F\}$.

Proposição 3.4. *Mantendo a notação estabelecida para φ e ψ, tem-se*

1) $F \subseteq L_1 \subseteq L_2 \subseteq N \Rightarrow G(N;L_2) \subseteq G(N;L_1)$, *isto é,* $\varphi(L_2) \subseteq \varphi(L_1)$.

2) $\{id\} \subseteq H_1 \subseteq H_2 \subseteq G(N;F) \Rightarrow \mathscr{F}(H_2) \subseteq \mathscr{F}(H_1)$, *isto é,* $\psi(H_2) \subseteq \psi(H_1)$.

3) *Para todo* $L \in \{N:F\}$, $\psi\big(\varphi(L)\big) = L$,

4) *Para todo* $H \in \{G:1\}$, $\varphi\big(\psi(H)\big) = H$.

Demonstração: Vamos demonstrar (1). Se $\sigma \in G(N;L_2)$, então $\sigma : N \to N$ é automorfismo e $\sigma(x) = x$, para todo $x \in L_2$. Como $L_1 \subseteq L_2$, temos que $\sigma(x) = x$, para todo $x \in L_1$. Segue que $\varphi(L_2) \subseteq \varphi(L_1)$. Para ver que vale (2), se $x \in \mathscr{F}(H_2)$, então $\sigma(x) = x$, para todo $\sigma \in H_2$. Como $H_1 \subseteq H_2$, temos que $\sigma(x) = x$, para todo $\sigma \in H_1$. Para a demonstração de (3) e (4), ver [8, p. 36] e [4, Proposição 6, p. 180].

□

Podemos finalmente enunciar o Teorema Fundamental da Teoria de Galois Finita. Parte de sua demonstração acabamos de estudar. Contudo, a demonstração completa demanda um estudo mais aprofundadado da teoria de corpos. Uma boa referência para a demonstração completa é [8, p. 51].

Teorema 3.5 (Teorema Fundamental da Teoria de Galois)**.** *Seja $N|F$ uma extensão galoisiana finita de corpos e $G = G(N;F)$. Existe uma correspondência bijetiva, que reverte a inclusão, entre os conjuntos $\{N:F\}$ e $\{G:1\}$. Além disso, H é subgrupo normal de G se, e somente se, $L|F$ é galoisiana, onde $L = \mathscr{F}(H)$. Neste caso,*

$$G(L;F) \cong G(N;F)/G(N;L).$$

3.3 SOLUBILIDADE POR RADICAIS

No primeiro capítulo estudamos as equações polinomiais de grau menor ou igual a 4 e mostramos como uma raiz pode ser expressa em termos de operações elementares e radicais, envolvendo os coeficientes do polinômio associado à equação.

Vimos que as mesmas técnicas, no passado, foram empregadas para se tentar obter as fórmulas resolutivas para a equação geral de grau 5, mas os matemáticos que trabalharam dessa

forma não obtiveram sucesso. Muito tempo se passou até que Abel (1802-1829) mostrasse que não há tal fórmula.

A história completa só foi descoberta por Galois (1811-1832), estudando o grupo de permutações das raízes do polinômio. Utilizando algumas ideias de Lagrange (1736-1813) Galois descobriu qual é a exata condição para que uma equação polinomial de grau 5 ou superior possa ser resolvida por meio de operações elementares e radicais. Essencialmente, ele transferiu o problema para os grupos de permutações, que estudamos no segundo capítulo. A uma equação polinomial está associado um grupo, que por sua vez, é subgrupo de um grupo de permutações. Dependendo da estrutura deste grupo de permutações (se é solúvel ou não), a equação pode ou não ser resolúvel.

Afirmar que um polinômio é solúvel por meio de radicais é o mesmo que dizer que suas raízes podem ser expressas por meio de operações elementares e radicais. Tornaremos esta noção precisa do ponto de vista algébrico nas próximas definições. Antes vejamos um exemplo que ilustra a situação. Considere o polinômio

$$p(x) = x^6 - 6x^3 + 7,$$

que possui como uma de suas raízes o número

$$\alpha = \sqrt[3]{3+\sqrt{2}}.$$

Note que há um processo de construção aritmética de α: extração da raiz de 2, soma com 3 e extração da raiz cúbica de $3+\sqrt{2}$. Na teoria de corpos, este processo está associado com a construção da cadeia de corpos

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{3+\sqrt{2}}\right)$$

por meio das adjunções consecutivas dos números

$$\alpha_1 = \sqrt{2} \text{ e } \alpha_2 = \sqrt[3]{3+\alpha_1}.$$

Fazendo ainda $F_0 = \mathbb{Q}$, $F_1 = F_0(\alpha_1)$ e $F_2 = F_1(\alpha_2)$, temos

$$F_0 \subseteq F_1 \subseteq F_2,$$

com $\alpha_1^2 \in F_0$ e $\alpha_2^3 = 3 + \alpha_1 \in F_1$. O corpo F_2 é uma extensão de $\mathbb{Q}$ que é conhecida como **extensão radical**. Em geral, dizemos que um corpo K é uma **extensão radical** de $\mathbb{Q}$ se existir

uma cadeia de corpos

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq ... \subseteq F_r = K$$

tal que, para cada $i \in \{1, ..., r\}$, temos $F_i = F_{i-1}(a_i)$ e alguma potência de a_i pertence a F_{i-1}.

Desta forma, afirmar que um polinômio é solúvel por meio de radicais significa que é possível obter uma extensão radical de $\mathbb{Q}$ que contenha todas as raízes do polinômio. De maneira mais precisa, dado um polinômio $p(x) \in \mathbb{Q}[x]$ e K o corpo de decomposição de $p(x)$ sobre $\mathbb{Q}$, dizemos que $p(x)$ é um **polinômio solúvel por meio de radicais** se existe uma extensão radical L de $\mathbb{Q}$ que contém K.

Voltemos ao exemplo do polinômio $p(x) = x^6 - 6x^3 + 7$. Os elementos do conjunto de suas raízes são os números $\sqrt[3]{3 \pm \sqrt{2}}$, $\xi \sqrt[3]{3 \pm \sqrt{2}}$ e $\xi^2 \sqrt[3]{3 \pm \sqrt{2}}$, onde $\xi = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$ é a raiz cúbica primitiva da unidade (Definição 3.2). Assim, a cadeia correspondente é

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \alpha) \subseteq \mathbb{Q}(\sqrt{2}, \alpha, \beta) \subseteq \mathbb{Q}(\sqrt{2}, \alpha, \beta, \xi) = L$$

onde $\alpha = \sqrt[3]{3 + \sqrt{2}}$, $\beta = \sqrt[3]{3 - \sqrt{2}}$.

No Exemplo 2.12, do polinômio $f(x) = x^4 - x^2 + 2 = (x^2 - 2)(x^2 + 1)$, temos a cadeia

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

Vimos que o Teorema Fundamental da Teoria de Galois (Teorema 3.5) estabelece uma correspondência entre os subcorpos de uma extensão galoisiana $K|F$ e os subgrupos do grupo de Galois $G(K;F)$ dos automorfismos que K que fixam F. Esta correspondência, denominada correspondência galoisiana, permite demonstrar o teorema principal desta seção, que traduz para a teoria de grupos a resolubilidade de um polinômio.

Teorema 3.6 (Galois)**.** *Seja $f(x) \in \mathbb{Q}[x]$ e K o corpo de decomposição de $f(x)$ sobre $\mathbb{Q}$. O polinômio $f(x)$ é solúvel por radicais sobre $\mathbb{Q}$ se, e somente se, $G(K;\mathbb{Q})$ é um grupo solúvel.*

Demonstração: Suponha que f é solúvel por radicais. Então existe uma extensão L de $\mathbb{Q} = F$ e corpos F_i tais que

$$F = F_0 \subseteq F_1 \subseteq ... \subseteq F_r = L$$

onde $F_{i+1} = F_i(\alpha_i)$ e alguma potência α_i está em F_i, para todo $i \in \{0, ..., r\}$. A cadeia de corpos pode ser construída de forma que $F_{i+1}|F_i$ é galoisiana com grupo de Galois abeliano [8, Teorema 4.9, p.42]. Fazendo $G = G(L;F)$ e $H_i = G(L;F_i)$, pelo Teorema 3.5, temos a cadeia de subgrupos

$$\{id\} = H_r \subseteq H_{r-1} \subseteq ... \subseteq H_0 = G.$$

Novamente pelo Teorema 3.5, temos que $H_{i+1} \trianglelefteq H_i$ (pois $F_{i+1}|F_i$ é galoisiana) e

$$\frac{H_i}{H_{i+1}} = \frac{G(L;F_i)}{G(L;F_{i+1}))} \cong G(F_{i+1};F_i).$$

Segue que $G(F_{i+1};F_i)$ é abeliano, pois $\dfrac{H_i}{H_{i+1}}$ é abeliano. Assim, G é solúvel. Portanto, $G(K;F)$ é também solúvel, pois $G(K;F) \cong \dfrac{G}{G(L;F)}$. Lembre que no segundo capítulo, o Teorema 2.9 afirma que o quociente de grupo solúvel é solúvel. A recíproca utiliza a outra direção da correspondência, isto é, dada a cadeia de subgrupos, utilizar os corpos fixos correspondentes [8, Teorema 4.9, p.42].

□

Pelo teorema, a possibilidade da construção de cadeias de corpos semelhantes às exemplificadas anteriormente corresponde, na teoria de grupos, à noção de solubilidade do grupo de Galois correspondente.

No exemplo ilustrativo do Teorema 3.1 descrevemos o grupo de Galois $G(K;\mathbb{Q})$, onde $K = \mathbb{Q}(\sqrt{2},i)$ é o corpo de decomposição (neste caso extensão radical) do polinômio $f(x) = x^4 - x^2 + 2 = (x^2-2)(x^2+1)$. Vimos que $G(K;\mathbb{Q}) = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3\}$ e descrevemos esses elementos, que são os automofismos de K que fixam $\mathbb{Q}$. O conjunto $H = \{\mathrm{id}, \sigma_1\}$ é um subgrupo normal de $G = G(K;\mathbb{Q})$ e o quociente $\dfrac{G}{H}$ é abeliano, pois tem ordem 2 (lembre do Teorema de Lagrange, Teorema 2.5). Assim, temos

$$\{\mathrm{id}\} \trianglelefteq H \trianglelefteq G(K;\mathbb{Q}),$$

com os respectivos quocientes abelianos. Portanto, $G(K;\mathbb{Q})$ é solúvel.

Uma maneira mais eficiente de estudar a resolubilidade de um grupo de Galois é utilizando o Teorema de Cayley para transferir o problema para os grupos de permutações, cuja resolubilidade foi estudada no capítulo anterior.

Suponha que K é o corpo de decomposição do polinômio $f(x) \in \mathbb{Q}[x]$. Seja $A = \{x_1, \ldots, x_n\}$ o conjunto de suas raízes, onde n é o grau de f. Seja S_n o grupo das permutações de A. Considere a aplicação

$$\begin{array}{rccc} \varphi: & G(K;\mathbb{Q}) & \longrightarrow & S_n \\ & \sigma & \longmapsto & \varphi(\sigma) \end{array} \tag{6}$$

onde $\varphi(\sigma)$ é a permutação de A que associa x_i à $\sigma(x_i)$, para cada $i \in \{1, \ldots, n\}$, isto é,

$$\begin{array}{rccc} \varphi(\sigma): & A & \longrightarrow & A \\ & x_i & \longmapsto & \varphi(\sigma)(x_i) := \sigma(x_i) \end{array}$$

Pelo Teorema 3.3, a aplicação está bem definida. Pelo Teorema de Cayley [4, Corolário 1, p. 146], φ é um homomorfismo injetivo. Podemos interpretar $G(K;\mathbb{Q})$ com um subgrupo do grupo de permutações S_n das raízes do polinômio cujo corpo de decomposição é K. Identificamos então σ como uma permutação das raízes e podemos denotá-la como:

$$\sigma = \begin{pmatrix} x_1 & \dots & x_n \\ \sigma(x_1) & \dots & \sigma(x_n) \end{pmatrix}.$$

Voltando ao exemplo do polinômio $f(x) = x^4 - x^2 + 2$, temos que $A = \{x_1 = i,\ x_2 = -i,\ x_3 = \sqrt{2},\ x_4 = -\sqrt{2}\}$ é o conjunto das raízes. Utilizando o procedimento que acabamos de estudar, obtemos as seguintes representações para os automorfismos de $G(K;\mathbb{Q})$ (já descritos anteriormente):

$$\mathrm{id} = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix},$$

$$\sigma_1 = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_1 & x_3 & x_4 \end{pmatrix}, \sigma_2 = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_1 & x_2 & x_4 & x_3 \end{pmatrix} \text{ e } \sigma_3 = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_1 & x_4 & x_3 \end{pmatrix}.$$

Neste caso, $G(K;\mathbb{Q})$ é subgrupo de S_4, que é solúvel. Como subgrupo de grupo solúvel é também solúvel (Teorema 2.9), temos que $G(K;\mathbb{Q})$ é solúvel. Pelo Teorema de Galois (Teorema 3.6), $f(x)$ é resolúvel por radicais.

No capítulo inicial deste trabalho estudamos as fórmulas resolutivas para os polinômios de grau 2, 3 e 4. A existência destas fórmulas é garantida pelo homomorfismo injetivo entre os grupos de Galois desses polinômios e os grupos de permutações S_2, S_3 e S_4, respectivamente. Esses grupos são solúveis. Lembre que S_2 é abeliano, portanto, é solúvel. Já mostramos a solubilidade de S_3 e S_4 anteriormente.

Por exemplo, $f(x) = ax^2 + bx + c$, com $a, b, c \in \mathbb{Q}$ e $a \neq 0$, tem corpo de decomposição dado por $K = \mathbb{Q}(\sqrt{\Delta})$, onde $\Delta = b^2 - 4ac$. A cadeia de corpos é simplesmente

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{\Delta}).$$

Como $G(K;\mathbb{Q}) \leq S_2$ e $|S_2| = 2$, temos $G(K;\mathbb{Q}) = S_2$. Portanto, é solúvel (bastava observar que que $G(K;\mathbb{Q})$ é abeliano).

No caso do polinômio geral de grau 3, vimos no capítulo introdutório que o mesmo pode ser reduzido à forma

$$h(x) = x^3 + px + q \in \mathbb{Q}[x]. \tag{7}$$

Seja K o corpo de decomposição de h sobre $\mathbb{Q}$. Temos que $G(K;\mathbb{Q})$ é isomorfo a um subgrupo de S_3, que é solúvel. Como subgrupo de grupo solúvel é também solúvel (Teorema 2.9) temos que $G(K;\mathbb{Q})$ é solúvel. Daí decorre a existência da fórmula para o polinômio de grau 3, que vimos no capítulo inicial deste trabalho. Lembrando que

$$S_3 = \{id, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$$

onde $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ e $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, temos mais dois possíveis subgrupos de S_3, além de $\{id\}$ e S_3. O primeiro é o subgrupo cíclico $\{id, \alpha, \alpha^2\} \cong \mathbb{Z}/3\mathbb{Z}$ e o segundo é $\{id, \beta\} \cong \mathbb{Z}/2\mathbb{Z}$. O subgrupo de S_3 que será isomorfo a $G(G;\mathbb{Q})$ vai depender do valor de $-p^3 - 27q^2$, conforme [4, Exemplo 2, p.177].

Como já observamos, a partir do grau 5 a história é diferente. Por exemplo, o polinômio

$$f(x) = x^5 - 4x + 2$$

não é solúvel por radicais. Vamos verificar esse fato. Com a ajuda do Cálculo observamos que existem exatamente três raízes reais distintas, conforme a Figura 1, denotadas por α_1, α_2 e α_3. Aproximadamente os valores são $\alpha_1 \approx -1,5, \alpha_2 \approx 0,5$ e $\alpha_3 \approx 1,2$. Há duas raízes complexas, $\alpha_4 = \overline{\alpha_5} = \alpha + \beta i$, onde $\alpha \approx 0,1$ e $\beta \approx 0,4$.

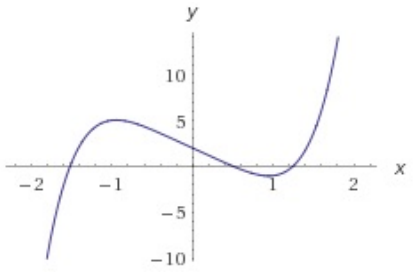


Figura 1: Gráfico de $p(x) = x^5 - 4x + 2$.

Seja K o corpo de decomposição de $p(x)$ sobre $\mathbb{Q}$. Definindo $\sigma : K \to K$, tal que $\sigma(\alpha_i) = \alpha_{i+1}$ e estendendo-o a K, temos que σ é um $\mathbb{Q}-$automorfismo. Justificaremos esse fato no estudo do polinômio geral de grau $n \geq 5$ abaixo. Note que σ corresponde, na aplicação φ da página 39, ao 5-ciclo (12345) em S_5. Portanto, no subgrupo H de S_5 que correponde a $G(K;\mathbb{Q})$, temos um 5-ciclo. Ainda, veremos que H também tem uma transposição. De fato, definindo $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$, temos que $K = L(\alpha_4)$, onde α_4 é uma raiz complexa de $f(x)$. Um elemento de $G(K;L)$ é $\tau : K \to K$, tal que $\tau(\alpha_4) = \overline{\alpha_4} = \alpha_5$. Ainda, τ é definido fixando L.

Assim, temos $\tau \in G(K;\mathbb{Q})$ e corresponde, em S_5, à transposição (12). Logo, $H \cong G(K;\mathbb{Q})$ e H contém a transposição (12) e o 5-ciclo (12345). Pelo [4, Corolário 1, p.164], S_5 é gerado por (12) e (12345), logo $H \cong S_5$. Segue que $G(K;\mathbb{Q})$ não é solúvel. Pelo Teorema 3.6, $f(x)$ não é solúvel por radicais.

Podemos agora mostrar que a não solubilidade por radicais se aplica ao **polinômio geral de grau** $n \geq 5$, dado por

$$f(x) = x^n + a_n x^{n-1} + ... + a_1 x + a_0, \text{ com } a_0, ..., a_{n-1} \in \mathbb{Q}. \tag{8}$$

Essencialmente, isso deve-se ao fato de que S_n, para $n \geq 5$, não é solúvel.

Vamos verificar que $G(K;\mathbb{Q}) \cong S_n$, utilizando o Teorema 3.6. Precisaremos de mais algumas definições e resultados preliminares.

O anel dos polinômios $\mathbb{Q}[x]$ pode ser estendido para o caso de $n \geq 2$ variáveis. Denotando por $\mathbb{Q}[x_1, ..., x_n]$ o conjunto dos polinômios (com coeficientes racionais) e sobre as variáveis $x_1, ..., x_n$, temos que este conjunto também é um anel (comutativo e com unidade). A verificação é análoga ao caso de uma variável. O **corpo das funções racionais** é definido como

$$\mathbb{Q}(x_1, ..., x_n) = \left\{ \frac{f(x_1, ..., x_n)}{g(x_1, ..., x_n)};\ f, g \in \mathbb{Q}[x_1, ..., x_n] \text{ e } g \neq 0 \right\}.$$

Note que, de fato, trata-se de um corpo. O inverso de $f \neq 0$ é exatamente a fração $\frac{1}{f}$.

Vamos também denotar por $\alpha_1, ..., \alpha_n$ as raízes do polinômio geral (8) e vamos assumir $n \geq 5$. A existência de $\alpha_1, ..., \alpha_n$ é garantida pelo Teorema Fundamental da Álgebra [7, Teorema 20, p.368]. Assim

$$\begin{aligned} f(x) &= x^n + a_n x^{n-1} + ... + a_1 x + a_0 \\ &= (x - \alpha_1)(x - \alpha_2)...(x - \alpha_n) \\ &= x^n - s_1 x^{n-1} + s_2 x^{n-2} + ... + (-1)s_n \end{aligned}$$

onde

$$\begin{aligned} s_1 &= \alpha_1 + \alpha_2 + ... + \alpha_n \\ s_2 &= \alpha_1\alpha_2 + ... + \alpha_{n-1}\alpha_n \\ &\vdots \\ s_n &= \alpha_1\alpha_2...\alpha_n \end{aligned}$$

Seja K o corpo de decomposição de f sobre $\mathbb{Q}$, isto é, $K = \mathbb{Q}(\alpha_1, ..., \alpha_n)$. Esse corpo

é obtido pela adjunção sucessiva das raízes, mas também é igual a calcular todas as frações de $\mathbb{Q}(x_1,...,x_n)$ em $\alpha_1,...,\alpha_n$.

Agora, sendo $L=\mathbb{Q}(s_1,...,s_n)$, temos que $f(x)\in L[x]$ (basta ver a notação anterior). Assim, K também é o corpo de decomposição de f sobre L. Portanto, $K|L$ é galoisiana.

Ocorre que todo elemento de S_n dá origem a um automorfismo (distinto) de $G(K;L)$. De fato, se $\begin{pmatrix} 1 & 2 & ... & n \\ l_1 & l_2 & ... & l_n \end{pmatrix}$ é uma permutação em S_n, definimos

$$\sigma(\alpha_i)=\alpha_{l_i}$$

sobre as raízes $\alpha_1,...\alpha_n$ e estendemos para K, fixando os elementos de $\mathbb{Q}$, fazendo:

$$\sigma\Big(\frac{f(\alpha_1,...,\alpha_n)}{g(\alpha_1,...,\alpha_n)}\Big)=\frac{f(\alpha_{l_1},...,\alpha_{l_n})}{g(\alpha_{l_1},...,\alpha_{l_n})}.$$

Por exemplo, se $K=\mathbb{Q}(\alpha_1,\alpha_2)$ e $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ é a permutação não trivial de S_2, então

$$\sigma\Big(\frac{f(\alpha_1,\alpha_2)}{g(\alpha_1,\alpha_2)}\Big)=\frac{f(\alpha_2,\alpha_1)}{g(\alpha_2,\alpha_1)}.$$

A verificação de que σ é realmente um L-automorfismo pode ser vista em [8, Exemplo 2.22, p.24].

Desta forma, $G(K;L)$ tem ao menos $n!=|S_n|$ elementos. Por outro lado, temos que $G(K;L)\cong H\leq S_n$. Note que isto implica $G(K;\mathbb{Q})\cong S_n$. Pelo Teorema 2.14, S_n não é solúvel para $n\geq 5$. Finalmente, pelo Teorema 3.6, o polinômio geral de grau $n\geq 5$ não é resolúvel por radicais.

4 CONCLUSÃO

O objetivo deste trabalho era o de apresentar as fórmulas resolutivas para as equações algébricas e compreender a matemática que torna possível a sua existência.

Pesquisando a história da descoberta dessas fórmulas, verifica-se que, para graus iguais ou superiores a 5, não é possível obter uma fórmula resolutiva. As propriedades das raízes das equações é que definem a possibilidade de se obter tal fórmula.

No início do século XIX, o jovem Évariste Galois identificou a estrutura na qual estão inseridas as raízes das equações de graus 2, 3 e 4, e que não se mantém para as equações de grau 5 e superior, não permitindo a sua solução por meio de uma fórmula.

Para que uma fórmula exista é necessário que o polinômio que dá origem à equação seja solúvel por radicais. Isso significa que o corpo no qual o polinômio têm suas raízes, deve ser obtido pela adjunção de radicais ao corpo onde estão os coeficientes do polinômio, numa estrutura chamada de extensão radical.

Tal construção não pode ser feita para o polinômio geral com grau igual ou superior a 5, portanto, conclui-se pela impossibilidade da existência de fórmulas resolutivas para esse polinômio.

REFERÊNCIAS

[1] BOLDRINI, J.L. **Álgebra linear**, São Paulo: Harper & Row do Brasil, 1986.

[2] BOYER, C.B. **História da matemática**, São Paulo: Edgard Blucher, 1996.

[3] GARCIA,A.; LEQUAIN,Y. **Elementos de Álgebra**, Rio de Janeiro: IMPA, 2003.

[4] GONÇALVES, A. **Introdução à álgebra**, Rio de Janeiro: IMPA, 1979.

[5] HEFEZ, A.; VILLELA, M. L. T. **Polinômios e equações algébricas**, Rio de Janeiro: SBM, 2012.

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

[7] MONTEIRO, L.H.J. **Elementos de Álgebra**, Rio de Janeiro: IMPA, 1974.

[8] MORANDI, P., **Field and Galois Theory**, Springer, Berlim, 1996.

[9] STEWART, I. **Uma História da simetria na Matemática**, Rio de Janeiro: Zahar, 2012.