Universidade Federal de Mato Grosso
Instituto de Ciências Exatas e da Terra
Departamento de Matemática

Solubilidade de equações polinomiais

Gleyca Farias Vieira

Mestrado Profissional em Matemática: PROFMAT/SBM

Orientador: **Adilson Antônio Berlatto**

Barra do Garças - MT

Abril de 2021

Solubilidade de equações polinomiais

Este exemplar corresponde à redação final da dissertação, devidamente corrigida e defendida por Gleyca Farias Vieira e aprovada pela comissão julgadora.

Barra do Garças 3 de maio de 2021.

Prof. Dr. Adilson Antônio Berlatto
Orientador

Banca examinadora:

Prof. Dr. Adilson Antônio Berlatto
Prof. Dr. Tibério Bittencourt de Oliveira Martins
Prof. Dr. Alex Carrazedo Dantas.

Dissertação apresentada ao curso de Mestrado Profissional em Matemática – PROFMAT, da Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título de **Mestre em Matemática**.

Dados Internacionais de Catalogação na Fonte.

V658s Vieira, Gleyca Farias.
Solubilidade de equações polinomiais / Gleyca Farias Vieira. -- 2021
xii, 90 f. ; 30 cm.

Orientador: Adilson Antônio Berlatto.
Dissertação (mestrado profissional) – Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação Profissional em Matemática, Pontal do Araguaia, 2021.
Inclui bibliografia.

1. Conjunto solução. 2. Solubilidade de equações polinomiais. 3. Teoria de Galois. 4. Teoria de grupos, anéis e corpos. 5. Solubilidade por radicais. I. Título.

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DE MATO GROSSO

PRÓ-REITORIA DE ENSINO DE PÓS-GRADUAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO EM EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

FOLHA DE APROVAÇÃO

TÍTULO: Solubilidade de equações polinomiais

AUTORA: MESTRANDA **Gleyca Farias Vieira**

Dissertação defendida e aprovada em **09** de **abril** de **2021**.

COMPOSIÇÃO DA BANCA EXAMINADORA

1. **Doutor Adilson Antônio Berlatto** (Presidente Banca / **Orientador**)

INSTITUIÇÃO: Universidade Federal de Mato Grosso

2. **Doutor Tibério Bittencourt de Oliveira Martins** (Membro Interno)

INSTITUIÇÃO: Universidade Federal de Mato Grosso

3. **Doutor Alex Carrazedo Dantas**(Membro Externo)

INSTITUIÇÃO: Universidade de Brasília

Barra do Garças, 09/04/2021.

Documento assinado eletronicamente por **TIBERIO BITTENCOURT DE OLIVEIRA MARTINS**, **Docente da Universidade Federal de Mato Grosso**, em 27/04/2021, às 00:19, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **ADILSON ANTONIO BERLATTO**, **Docente da Universidade Federal de Mato Grosso**, em 27/04/2021, às 00:21, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Alex Carrazedo Dantas**, **Usuário Externo**, em 30/04/2021, às 11:38, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufmt.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **3455249** e o código CRC **86D6C2B0**.

À minha família e Amigos.

Agradecimentos

Ao bondoso Deus, por tudo o que sou.

Ao meu Senhor e Salvador Cristo Jesus, pelo amor e pela vida.

Aos meus pais Zenóbia e Janivaldo, por toda a compreensão e conforto nas horas difíceis. De fato, vocês demonstram de maneira exuberante o amor que nutrem por mim, ofertando paciência, zelo, carinho e proteção.

Às minhas irmãs, Laryany, Klycia e à minha sobrinha Tafnny, companheiras de caminhada, que sempre me amaram e me deram forças para seguir em frente.

Ao meu amado, Hudson Pina, obrigada por todo companheirismo e disposição em me auxiliar, confortar e apoiar.

A meu orientador, Prof. Dr. Adilson Berlatto, pela sua assídua colaboração, pelos seus conhecimentos e ensinamentos.

Aos professores do mestrado, pelo conhecimento compartilhado. De fato, fui agraciada com a oportunidade de tê-los como meus mestres.

À minha amiga, Roberta, por todo incentivo e apoio.

Aos meus colegas de classe, obrigada por todos os momentos de estudo compartilhados.

Aos amigos e professores que, direta ou indiretamente, auxiliaram-me nesta composição.

A todos vocês, os meus sinceros agradecimentos.

"A persistência é o menor
caminho do êxito."

Charles Chaplin.

Resumo

Este trabalho apresenta o conjunto solução de equações polinomiais de grau menor ou igual a 4, bem como as condições necessárias para que a mesma exista em determinada estrutura algébrica. A solubilidade por radicais de polinômios foi amplamente estudada por Évariste Galois. Faremos uma abordagem, a partir de teoria de grupos, das possibilidades das raízes de um polinômio de grau n serem dadas a partir de seus coeficientes.

Palavras chave: Conjunto solução, solubilidade de equações polinomiais, teoria de Galois, teoria de grupos, anéis e corpos, solubilidade por radicais.

Abstract

This master thesis presents the solution set of polynomial equations, as well as the necessary conditions for it to exist in a given algebraic structure. The solubility of a polynomial equation by radicals was extensively studied by Évariste Galois. We will approach, from group theory, the possibilities of the roots of a n degree polynomial to be given from its coefficients.

Keywords: Solution set, solubility of polynomial equations, Galois theory, group theory, rings and fields, solubility by radicals.

Sumário

Lista de Figuras

Lista de Tabelas

Introdução

A modelagem de problemas do nosso cotidiano nos leva a equações que nos permite fazer uma interpretação das possibilidades de tomada de decisão com a análise das equações. Uma das primeiras equações que temos contatos são as equações polinomiais, visto que suas aplicações são mais fáceis de serem compreendidas pelos alunos. Situações simples do nosso dia-a-dia podem ser resolvidos a partir de polinômios como por exemplo: comparar o custo × benefício de um determinado item a partir do preço e quantidade de cada embalagem.

Devido a essa importância, tanto para o desenvolvimento do aluno quanto para a matemática, entendemos que escrever sobre esse assunto será mais um auxílio para professores, pois é um tema que não é abordado na licenciatura e é necessário que os docentes conheçam, pelo menos, soluções das equações de grau até 4 e tenham conhecimento de que as de grau 5 ou mais dependem de outros fatores.

As equações podem ser divididas de várias formas, por exemplo: polinomiais, diferenciais, exponenciais, entre outras. Muitos matemáticos importantes se dedicaram em desenvolver métodos para diferentes tipos de equações (Gauss, Galois, Euler, Fermat, entre outros). Neste trabalho focaremos em equações polinomiais com uma variável independente.

Um polinômio de grau n é da forma

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

onde $n \geq 0$ é um número natural e $a_0, \cdots, a_n$ são constantes que pertencem a um corpo $\mathbb{K}$, com $a_n \neq 0$.

O primeiro contato com equação polinomial é no ensino básico, na tentativa de

encontrar uma solução para equação $a \cdot x + b = 0$ no conjunto dos números reais. O valor de x que satisfaz essa identidade é denominado *raiz da equação*. Quando a, b são números reais, com $a \neq 0$, e " $\cdot$ " e " $+$ " são, respectivamente, o produto e a soma usuais de números reais a equação é de fácil solução. Veremos que tal equação pode ser resolvida em estruturas algébricas com menos propriedades em suas operações, por exemplo: seja $M_{n\times n}$ o conjunto de todas as matrizes quadradas com n linhas e n colunas e consideremos a equação

$$A \cdot X + B = 0,$$

onde $A, B \in M_{n\times n}$ e 0 representa a matriz nula do conjunto. Sabendo que o conjunto das matrizes com seu produto não é comutativo, ou seja, pode acontecer $A \cdot C \neq C \cdot A$, encontrar as raízes dessa equação requer um pouco mais de cuidado, uma vez que podemos ter matrizes não nulas cujo produto é a matriz nula.

Um problema que surge naturalmente é encontrar os valores em que o polinômio se anula; tais pontos são chamados de raízes ou zeros do polinômio. Formalmente, dizemos que um número x_0 é um zero do polinômio $p(x)$, se $p(x_0) = 0$.

Entre os métodos mais conhecidos para encontrar os zeros de um polinômio o mais utilizado são: a fórmula de Bhaskara, usada para polinômios quadráticos, o método de Cardano - Tartaglia, desenvolvido para encontrar raízes de polinômios cúbicos foi proposto por Girolamo Cardano e Niccolo Fontana (conhecido como Tartaglia), em 1945, e tempos depois, para determinar as raízes de polinômios quárticos, o método de Ferrari, por Cardano e Lodovico Ferrari, que consta no grande livro de Cardano intitulado *Ars Magna* (Arte maior ou a grande arte).

Todos esses métodos expressam as raízes do polinômio em termos de seus coeficientes, usando apenas as operações algébricas usuais (adições, subtrações, multiplicações e divisões) e aplicações de radicais (raiz quadrada, raiz cúbica, etc). Sempre que é possível expressar as raízes a partir de seus coeficientes dizemos que o polinômio é solúvel por radicais.

E para os polinômios de grau 5, será possível encontrar uma fórmula usando apenas os coeficientes do polinômio de modo a determinar todas as suas raízes? Grandes matemáticos como Euler e Lagrange, tentaram a partir das técnicas usadas nas de graus três e quatro, e concluíram que não era possível utilizar os mesmos métodos para polinômios de grau cinco. Em 1824, acreditando não ser possível, o matemático Niels

Henrik Abel acabou com tais suspeitas, e provou que uma certa classe de polinômios de quinto grau não é solúvel por radicais.

A dúvida no entanto permaneceu quanto as equações de graus maior do que 5. A resposta para essa pergunta foi dada pelo matemático Évariste Galois, onde caracteriza em quais circunstâncias um polinômio de qualquer grau pode ou não apresentar soluções por meio de radicais.

Évariste Galois, matemático, nascido em 25 de outubro de 1811, em Bourg-la-Reine, um vilarejo ao sul de Paris. Aos 16 anos iniciou o curso de matemática e aos 17 anos já tinha progressos suficientes sobre o estudo de soluções de equações de grau maior ou igual a 5.

Continuou fazendo pesquisas e sua obsessão era descobrir o porquê algumas equações polinomiais de grau maior ou igual a 5 não possuíam solução a partir de seus coeficientes, considerado o grande problema da época. Durante este período, foi preso duas vezes, por questões políticas e, por fim, foi desafiado a um duelo, a ocorrer na manhã de quarta-feira, 30 de maio de 1832, por ter se envolvido com uma mulher comprometida. Sabendo das habilidades de seu desafiante com pistola, passou a noite escrevendo suas ideias que solucionavam o enigma das equações de grau maior ou igual a 5, explicando em quais circunstâncias um polinômio de qualquer grau pode ou não apresentar soluções por meio de radicais. Nesta carta destinada a seu amigo Auguste Chevalier, ele já adiantava os resultados alcançados, pedindo que, caso morresse, aquelas páginas fossem enviadas aos grandes matemáticos da Europa.

"Meu Querido Amigo,

Eu fiz algumas novas descobertas em análise. A primeira se refere à teoria das equações do quinto grau e as outras, às funções integrais.

Na teoria das equações eu pesquisei as condições para a solução de equações por radicais. Isso me deu a oportunidade de aprofundar esta teoria e descrever todas as transformações possíveis em uma equação, mesmo que ela não seja resolvida pelos radicais. Está tudo aqui nesses três artigos...

Em minha vida eu frequentemente me atrevi a apresentar ideias sobre as quais não tinha certeza. Mas tudo que escrevi aqui estava claro em minha mente durante um ano e não seria de meu interesse deixar suspeitas de que anunciei teoremas dos quais não tenho a demonstração completa.

Faça um pedido público a Jacobi ou Gauss para que deem suas opiniões, não pela verdade, mas devido à importância desses teoremas. Afinal, eu espero que alguns homens achem valioso analisar esta confusão.

Um abraço caloroso."

Évariste Galois. Singh (2014)

Galois faleceu aos 20 anos na manhã de 30 de maio de 1832 após receber um tiro fatal no duelo. Mais detalhes sobre a vida de Galois, Singh (2014).

Para entender esta teoria desenvolvida por ele, veremos inicialmente a Teoria dos Corpos. Na sequência, uma introdução à extensão de corpos, muito importante para a associarmos a solubilidade por radicais dos polinômios a conjuntos com propriedades que compravam a possibilidade de obter as raízes de um polinômio por meio de radicais.

Durante a elaboração deste trabalho, alguns tópicos não previstos inicialmente foram inseridos, na tentativa de abranger todas as equações polinomiais. Em vista disto, alguns teoremas ficaram sem demonstração, mas deixamos indicado suas referências.

No primeiro Capítulo apresentamos uma breve introdução dá Teoria de Grupos, essencial para a compreensão da Teoria de Galois e apresentamos soluções para equações polinomiais de primeiro grau definidas a partir de uma operação em um determinado

conjunto.

No Capítulo 2, resolvemos equações polinomiais de primeiro grau com mais de uma operação e para isso é introduzido o conceito de Anéis e Corpos. Para equações polinomiais irredutíveis em $\mathbb{Q}$, veremos como estender afim de possibilitar a redução dos polinômios em questão.

Nos Capítulos 4 e 5, temos os principais resultados da teoria de Galois e exemplos que ilustram as possibilidades de identificação das raízes de um polinômio a partir de seus coeficientes.

Capítulo 1

Conjuntos e grupos

Neste capítulo iremos expor algumas definições, propriedades e exemplos sobre grupos que são indispensáveis para a compreensão de conjunto solução e solubilidade de equações polinomiais. Existe uma vasta literatura sobre o assunto, para o trabalho as principais referências foram Hygino e Iezzi (2003), Gonçalves (2006) e Bewersdorff (2006). Aqui faremos um apanhado teórico afim de compreender a Teoria de Galois.

1.1 Conjuntos

Conjunto é um agrupamento de objetos que partilham de mesmas características; tais objetos são chamados de elementos do conjunto. Quando esses elementos são números, essa união passa a ser conhecida como conjunto numérico. Dentro da matemática, pode-se agrupar os números de diversas formas, gerando assim inúmeros conjuntos numéricos. Um conjunto que não possui elementos é chamado de conjunto vazio.

Porém, alguns desses conjuntos são mais notórios por conta da frequência que aparecem nas soluções e demonstrações matemáticas e são indicadas pelas seguintes notações:

$$\begin{aligned}
&\mathbb{N} = \{0, 1, 2, 3, 4, 5 \dots\} && \text{Números Naturais}\\
&\mathbb{Z} = \{\cdots -2, -1, 0, 1, 2 \dots\} && \text{Números Inteiros}\\
&\mathbb{Q} = \left\{ \frac{p}{q};\ \ (p,q) \in \mathbb{Z} \times \mathbb{Z}^* \ \ e \ \ mdc(p,q) = 1 \right\} && \text{Números Racionais}\\
&\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} - \mathbb{Q}) && \text{Números Reais}\\
&\mathbb{C} = \{a + bi;\ \ (a,b) \in \mathbb{R}^2\} && \text{Números Complexos}
\end{aligned}$$

Se B indica um dos conjuntos acima, adotamos:

1. $B^* = B - \{0\}$

2. $B_+ = \{x \in B\,;\ x \geq 0\}$

3. $B_- = \{x \in B\,;\ x \leq 0\}$

4. $B_+^* = \{x \in B\,;\ x > 0\}$

5. $B_-^* = \{x \in B\,;\ x < 0\}$

Observe que os itens $2, 3, 4$ e 5 não podem ser aplicados no conjunto dos números complexos, uma vez que não há relação de ordem total no conjunto dos números complexos.

1.1.1 Subconjuntos

Se A e B são conjuntos e todo elemento de A também é elemento de B, dizemos que A é subconjunto de B e denotaremos essa relação por $A \subset B$ (lê-se A está contido em B) ou $B \supset A$ (lê-se B contém A). Dois conjuntos A e B são ditos iguais se $A \subset B$ e $B \subset A$. Isso significa que os dois conjuntos constam exatamente dos mesmos elementos.

A igualdade de conjuntos é denotada pelo símbolo usual de igualdade. Por exemplo: se $A = \{x \in \mathbb{Z};\ 3 < x < 9\}$ e $B = \{4, 5, 6, 7, 8\}$, então $A = B$. Dessa forma, podemos observar que:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

1.2 Grupos

Os grupos são uma das mais importantes estruturas algébricas e servem como base para o estudo das mais diferentes áreas do conhecimento. Iremos expor algumas definições, propriedades e exemplos sobre grupos, corpos e anéis que são indispensáveis para o entendimento de equações polinomiais.

Para entendermos as estruturas envolvidas precisamos inicialmente entender as operações definidas nos conjuntos. Em matemática, uma operação sobre um conjunto não vazio G é uma função $* : G \times G \to G$, que associa a dois elementos de G um terceiro elemento: $*(a, b) = a * b$, onde $a, b \in G$.

Definição 1. *Um sistema matemático constituído de um conjunto não vazio G e uma operação $(x, y) \mapsto x * y$ sobre G é chamado de grupo, e representado por $(G, *)$ se a operação satisfaz as seguintes propriedades:*

i) Se $a, b \in G$ então $a * b \in G$ (Propriedade do Fechamento);

ii) $(a * b) * c = a * (b * c)$, quaisquer que sejam $a, b, c \in G$ (Associatividade);

iii) Existe um elemento $e \in G$ tal que $a * e = e * a = a$, $\forall\, a \in G$. (Existência do Elemento Neutro);

iv) Para todo $a \in G$ existe $a^{-1} \in G$ tal que $a * a^{-1} = a^{-1} * a = e$ (Existência de simétricos).

O grupo será dito abeliano ou comutativo, se além das propriedades acima, satisfizer a comutatividade, ou seja, para quaisquer $a, b \in G$ temos:

$$a * b = b * a.$$

Com o objetivo de facilitar a notação, um grupo poderá ser indicado apenas por G para representar o grupo G com a operação $*$, $(G, *)$.

1.2.1 Solução para a equação $a * x = b$

Considere a equação abaixo:

$$a * x = b, \tag{1.1}$$

onde a, b pertencem a um conjunto qualquer G. Se $(G, *)$ não for um grupo, a equação (1.1) possui solução em G?

Por exemplo: se $G = \mathbb{Z}$ e $*$ é a multiplicação usual de números, podemos garantir que as soluções de (1.1) estão em $\mathbb{Z}$?

E a resposta é simples e direta. Considere:

$$2 \cdot x = -5.$$

Como bem vemos, os coeficientes são inteiros, mas sua solução não é inteira,

$x = -\frac{5}{2}$. Neste caso, o que falta na estrutura $(\mathbb{Z}, \cdot)$ que faz com que a equação acima, nem sempre, tenha solução? A falta do simétrico multiplicativo faz com que, dependendo dos coeficientes, seja impossível determinar a solução no conjunto. Assim, se $(G, *)$ é um grupo, podemos sempre garantir a existência de solução da equação (1.1) e sua solução será dada usando todas as propriedades da operação $*$:

Considere a equação em G:

$$a * x \quad = \quad b.$$

Como $a \in G$ tem simétrico, obtemos

$$a^{-1} * (a * x) = a^{-1} * b.$$

Agora, pela associatividade, ficamos com

$$(a^{-1} * a) * x = a^{-1} * b.$$

Como $e \in G$,

$$e * x = a^{-1} * b.$$

E por G ser fechado

$$x = a^{-1} * b \quad \rightarrow \quad a^{-1} * b \in G.$$

Com isso, podemos dizer que o grupo, da forma como conhecemos, é uma estrutura algébrica adequada de modo a garantir solução da equação (1.1). Sendo assim

Lema 1 (Propriedades)**.** *Seja G um grupo, então:*

i) O elemento neutro de G é único;

ii) O elemento inverso é único;

iii) Para todo $a \in G$ $(a^{-1})^{-1} = a$;

iv) Para todo $a \in G$ $(a * b)^{-1} = b^{-1} * a^{-1}$.

v) Se $a, b \in G$, então $x * a = b$ tem uma única solução, a saber $b * a^{-1} \in G$.

Demonstração. i) Supondo que existam e_1, $e_2 \in G$ elementos neutros, então,

$$e_1 = e_1 * e_2 = e_2.$$

Logo o elemento neutro é único.

ii) Supondo que não seja único, seja $a \in G$ e sejam b_1, $b_2 \in G$ os elementos inversos de a, temos,

$$b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2,$$

o que nos diz que quaisquer dois simétricos de $a \in G$ são iguais. Logo o elemento simétrico é único.

iii) Como, $a^{-1} * a = a * a^{-1} = e$, o simétrico de a^{-1} é a; logo $(a^{-1})^{-1} = a$.

iv) Para que $(a * b)^{-1} = b^{-1} * a^{-1}$, devemos ter $(a * b) * (b^{-1} * a^{-1}) = (b^{-1} * a^{-1}) * (a * b) = e$. Vejamos:

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e$$

e

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

Pela unicidade do simétrico, segue o resultado.

v) De fato, se c é uma solução de $x * a = b$ então $c * a = b$, logo

$$c * a * a^{-1} = b * a^{-1} \Longrightarrow c = b * a^{-1}.$$

Vamos mostar que $b * a^{-1}$ é solução da equação.

$$\begin{aligned} x * a &= b, \text{ substituindo} \\ (b * a^{-1}) * a &= b \\ b * (a^{-1} * a) &= b \\ b &= b \end{aligned}$$

□

1.2.2 Conjunto das matrizes

Aqui vamos considerar o conhecimento prévio de algumas definições e propriedades sobre matrizes, como por exemplo determinantes e o cálculo da matriz adjunta.

A estrutura algébrica dos grupos também permite que sejam resolvidos determinados tipos de sistemas de equações. Para essa aplicação, necessitamos da linguagem da álgebra linear, como faremos.

Considere o conjunto das matrizes quadradas com entradas reais denotado por $M_{n\times n}(\mathbb{R})$. Veremos no decorrer do trabalho que é possível trabalhar com matrizes cujas entradas estão em outros conjuntos, desde que tenham propriedades mais específicas. Dados $A \in M_{m\times n}(\mathbb{R})$ e $B \in M_{n\times p}(\mathbb{R})$ podemos escrevê-las da seguinte forma

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} = [a_{ij}], \quad \mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1p} \\ b_{21} & b_{22} & \cdots & b_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{np} \end{pmatrix} = [b_{ij}].$$

Definimos o produto de duas matrizes $A = [a_{ij}]$ e $B = [b_{ij}]$ por

$$c_{ij} = \sum_{r=1}^{n} a_{ir}b_{rj} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj},$$

onde $[c_{ij}] = C \in M_{m\times p}(\mathbb{R})$. Caso as matrizes A e B sejam quadradas e de mesma dimensão temos que a matriz resultante do produto de A e B terá a mesma dimensão de A e B, neste caso, dizemos que este conjunto é fechado com relação a esta operação. Mas se tomamos o conjunto de todas as matrizes quadradas de mesma dimensão, este conjunto é um grupo multiplicativo? Para entender melhor precisamos primeiramente definir a inversa de uma matriz.

Definição 2. *Seja $A \in M_{n\times n}(\mathbb{R})$ dizemos que B é a inversa de A se $A \cdot B = I_n$ e denotaremos por A^{-1}, onde I_n é a matriz identidade de ordem $n \times n$.*

Observação 1. Se existe A^{-1} de A então:

1. A inversa de uma matriz é única.

2. $A^{-1}A = AA^{-1} = I_n$

3. A matriz inversa de uma matriz invertível é também invertível, sendo que a inversa da inversa de uma matriz é igual à própria matriz: $A = \left(A^{-1}\right)^{-1}$.

4. Em geral, uma matriz quadrada é invertível se, e somente se, o seu determinante é diferente de zero (se $\det(A) \neq 0$). E sua inversa é dada por:

$$\mathbf{A}^{-1} = \frac{1}{\det(\mathbf{A})} \cdot \mathrm{adj}(\mathbf{A}).$$

Um grande problema ao trabalhar com matrizes é o fato de quando considerado matrizes não nulas cujo o produto entre elas é exatamente a matriz nula, por exemplo

$$A = \begin{bmatrix} 2 & 1 \\ 0 & 0 \end{bmatrix} \quad e \quad B = \begin{bmatrix} 0 & 2 \\ 0 & -4 \end{bmatrix},$$

temos que

$$A \cdot B = \begin{bmatrix} 2 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 2 \\ 0 & -4 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Mas se considerarmos apenas matrizes que são invertíveis este problema não ocorre.

De fato, se A é invertível e B é qualquer matriz de mesma ordem, com o produto $AB = 0$ teríamos:

$$AB = 0 \Leftrightarrow A^{-1}(AB) = 0 \Leftrightarrow B = 0, \tag{1.2}$$

aqui usamos a associatividade da multiplicação de matrizes. Então, como veremos ainda neste capítulo, o conjunto das matrizes invertíveis é um grupo e denotamos por $GL_n(\mathbb{R})$.

Com tais propriedades podemos agora voltar ao nosso problema inicial considerando os coeficientes sendo matrizes e $*$ sendo a operação de multiplicação de matrizes. A equação

$$A * X = B, \tag{1.3}$$

com $A \in GL_n(\mathbb{R})$, sempre possui solução.

Um caso particular para este tipo de equação é conhecida na literatura como **Regra de Cramer** e consiste em determinar soluções para a equação (1.3), como veremos a seguir.

1.2.3 Regra de Cramer

A regra de Cramer é um teorema em Álgebra Linear, que dá a solução de um sistema de equações lineares em termos de determinantes. Recebe este nome em homenagem a Gabriel Cramer (1704 - 1752).

Considere o sistema linear

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \quad \vdots \qquad \vdots \qquad\qquad \vdots \qquad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = b_n. \end{cases}$$

Sejam

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}, \mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \text{ e } \mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}.$$

Podemos reescrever o sistema da seguinte forma matricial:

$$A\mathbf{x} = \mathbf{b}.$$

Se A é uma matriz invertível, então

$$Ax = b \Leftrightarrow A^{-1}(Ax) = A^{-1}b \Leftrightarrow x = A^{-1}b.$$

Cramer mostrou que para todo j, $1 \leq j \leq n$, a solução $x = (x_1, \cdots, x_n)$ do sistema, onde x_j é uma das coordenadas de x, é dada por:

$$x_j = \frac{|A_j|}{|A|} = \frac{det(A_j)}{det(A)},$$

em que usamos $|A| = \det(A)$ e A_j é a matriz que se obtém da matriz A substituindo a coluna j pela coluna dos termos independentes b. Para detalhes da demonstração veja Boldrini e Figueiredo (1980).

Exemplo 1. Considere o sistema linear

$$\begin{cases} x - y &= 2 \\ 2x + y &= 1 \end{cases}$$

Sua forma matricial é

$$\begin{bmatrix} 1 & -1 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}.$$

pela regra de Cramer, x e y podem ser calculados:

$$x = \frac{\begin{vmatrix} \mathbf{2} & -1 \\ \mathbf{1} & 1 \end{vmatrix}}{\begin{vmatrix} 1 & -1 \\ 2 & 1 \end{vmatrix}} = \frac{2 * 1 - (-1) * 1}{1 * 1 - (-1) * 2} = 1$$

e

$$y = \frac{\begin{vmatrix} 1 & \mathbf{2} \\ 2 & \mathbf{1} \end{vmatrix}}{\begin{vmatrix} 1 & -1 \\ 2 & 1 \end{vmatrix}} = \frac{1 * 1 - 2 * 2}{1 * 1 - (-1) * 2} = -1.$$

Agora, considerando o conjunto $GL_n(\mathbb{R})$ munido da multiplicação de matrizes é um grupo por satisfazer todas as propriedades de grupo, para mais veja Hygino e Iezzi (2003). E então, a equação

$$A \cdot X = B,$$

terá uma única solução sempre que $A \in GL_n(\mathbb{R})$ e $B \in M_{n\times n}(\mathbb{R})$. E observe que não existe a necessidade da matriz B ser invertível, por conta de (1.2).

Para simplificar notação representaremos $a * b$ em um grupo G apenas por ab.

1.2.4 Ordem de um grupo

Um grupo $(G, *)$ em que o número de elementos é finito, é chamado de grupo finito, representamos o número de elementos de G, chamado "ordem de G", por $|G|$, dessa forma, se G possui n elementos então $|G| = n$. Caso contrário, o grupo possui infinitos

elementos e escrevemos $|G| = \infty$.

Definição 3. *A ordem de um elemento a, $o(a)$, de um grupo G é o menor número natural n tal que $a^n = e$. Se este valor não existe, o elemento tem ordem infinita.*

Se a é elemento de um grupo multipicativo G denotaremos por $\langle a \rangle$ o subconjunto de G formado pelas potências inteiras de a, ou seja, $\langle a \rangle = \{a^m \,;\, m \in \mathbb{Z}\}$, onde

$$a^m = \underbrace{a \cdot a \cdots a}_{m-vezes}.$$

Caso G seja aditivo,

$$a^m = \underbrace{a + a + \cdots + a}_{m-vezes} = m \cdot a$$

.

1.2.5 Grupos cíclicos

Definição 4. *Um grupo G será chamado de grupo cíclico se, para algum elemento $a \in G$, se verificar a igualdade $G = \langle a \rangle$. Nessas condições, o elemento a é chamado gerador do grupo G.*

Exemplo 2. .

1. Os inteiros, $\mathbb{Z} = \langle 1 \rangle$;

2. O conjunto dos restos módulo m, $\mathbb{Z}_m = \langle \overline{1} \rangle$;

3. O conjunto gerado por todas potências de $i \in \mathbb{C}$, é um grupo cíclico gerado por i. De fato, por definição, $\langle i \rangle = \{i^m; m \in \mathbb{Z}\}$. Mas como se vê no estudo dos números complexos, esse conjunto só tem quatro elementos $1, i, -1, -i$, obtidos respectivamente quando $m = 4q$, $m = 4q + 1$, $m = 4q + 2$, $m = 4q + 3$, onde $q \in \mathbb{Z}$. Como $i^4 = 1$, segue que se r é o resto da divisão de m por 4 ($m = 4k + r$), temos $i^m = i^{4k+r} = i^{4k} i^r = i^r$.

Grupos não cíclicos podem ser gerados por um número finito de elementos, para estes grupos, sempre que necessário, usaremos uma notação semelhante a usada para

descrever grupos cíclicos, como por exemplo: Se G é um grupo gerado por dois elementos, podemos escrever:

$$G = \langle a, b; a^3, b^2, (ab)^3 \rangle,$$

onde, o grupo G é gerado por a, b; com $o(a) = 3$, $o(b) = 2$ e $o(ab) = 3$.

1.3 Exemplos de grupos

Daremos alguns exemplos de forma breve, para mais veja Hygino e Iezzi (2003).

Grupos aditivos e abelianos

A operação desses grupos é a soma, $(x, y) \mapsto x + y$, o elemento neutro é 0 e o simétrico de x é $-x$; para todo $x \in \mathbb{K}$. Os mais comuns são $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$.

Ilustrando o que foi dito no final da sessão anterior, tomando o grupo $G = (\mathbb{Z}, +)$. Observe que G não possui elementos de ordem finita. Se $a \neq 0$ então ma também será, $\forall\, m > 0$.

O conjunto gerado pelo elemento 2 é

$$\langle 2 \rangle = \{2^m \,; m \in \mathbb{Z}\} = \{\cdots -6, -4, -2, 0, 2, 4, 6, \ldots\}.$$

Grupos multiplicativos e abelianos

A operação desses grupos é a multiplicação usual, $(x, y) \mapsto x \cdot y$, o elemento neutro é 1 e o simétrico de x é x^{-1}; para todo $x \in \mathbb{K}^*$. Os mais comuns são $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$.

Veja que o grupo $(\mathbb{C}^*, \cdot)$ tem elementos de ordem finita, por exemplo $i^4 = 1$ e elementos que não tem ordem finita, por exemplo qualquer $a \in \mathbb{Z} - \{-1, 0, 1\} \subset \mathbb{C}^*$.

Grupo aditivo e abeliano das matrizes

Este grupo é representado por $(M_{m\times n}(\mathbb{K}), +)$, onde $\mathbb{K} = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, com $M_{m\times n}(\mathbb{K})$ representando o conjunto das matrizes sobre $\mathbb{K}$ com m linhas e n colunas. O elemento neutro é a matriz nula.

Grupos lineares de grau n

O conjunto $M_{n\times n}(\mathbb{K}) = M_n(\mathbb{K})$ das matrizes quadradas de ordem n sobre $\mathbb{K}$ não forma um grupo sob a multiplicação de matrizes, uma vez que a matriz nula, por exemplo, não admite um inverso. No entanto o subconjunto $GL_n(\mathbb{K}) = \{M \in M_n(\mathbb{K}) : det(M) \neq 0\}$ é um grupo não abeliano, se $n > 1$, sob a multiplicação de matrizes, com elemento neutro sendo a matriz identidade quadrada, com $\mathbb{K}$ podendo ser $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

Grupos aditivos de classes de restos

Pelo algoritmo de Euclides temos que, dado dois números b, $m \in \mathbb{Z}$, existem q, $r \in \mathbb{Z}$ tais que

$$b = mq + r,$$

onde $0 \geq r \geq m-1$. O número r é chamado de resto e a identificação de cada inteiro com o seu resto da divisão por m gera o conjunto das classes (conjunto das classes módulo m). Este conjunto munido da soma é um grupo e representado por $(\mathbb{Z}_m, +)$, onde $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots \overline{m-1}\}$. Por exemplo, para $m = 6$, $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$.

Dizemos que $a \sim b$ se, e somente se, a e b deixam o mesmo resto na divisão por m. Isso define uma relação de equivalência sobre $\mathbb{Z}$. Daí, em $\mathbb{Z}_m$, $\overline{a} = \overline{b}$ se, e somente se, deixam o mesmo resto.

Sem perda de generalidade, utilizaremos a multiplicação usual e não uma operação qualquer $*$ pois, dados $\overline{a}, \overline{b} \in \mathbb{Z}_m$, então existem $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tais que:

$$\begin{aligned} a &= mq_1 + r_1 \\ b &= mq_2 + r_2. \end{aligned}$$

E daí,

$$\begin{aligned} a \cdot b &= (mq_1 + r_1)(mq_2 + r_2) \\ &= m(mq_1q_2 + q_1r_2 + +q_2r_1) + r_1r_2. \end{aligned}$$

Logo,

$$\begin{aligned}\overline{a \cdot b} &= \overline{\overline{m(mq_1q_2 + q_1r_2 + +q_2r_1) + r_1r_2}} \\ &= \overline{\overline{m(mq_1q_2 + q_1r_2 + +q_2r_1)} + \overline{r_1r_2}} = \overline{r_1r_2}.\end{aligned}$$

Portanto,

$$\overline{a} \cdot \overline{b} = \overline{r_1} \cdot \overline{r_2} = \overline{r_1r_2}.$$

Com isso, $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

Grupos multipicativos de classes de restos

Tomando agora o conjunto $\mathbb{Z}_m^*$ com a multiplicação usual temos que $(\mathbb{Z}_m^*, \cdot)$ será grupo se, e somente se, m for primo. De fato!

($\Rightarrow$) Suponhamos que m não fosse primo. Como $m > 1$, podem ser encontrados dois inteiros $1 < a, b \leq m - 1$ tais que $ab = m$. Dessa igualdade resulta que $\overline{ab} = \overline{m}$. Como $\overline{a} \cdot \overline{b} = \overline{ab}$ e $\overline{m} = \overline{0}$, então $\overline{a} \cdot \overline{b} = \overline{0}$, o que é impossível pela hipótese.

($\Leftarrow$) A única possibilidade de a multiplicação módulo m, quando restrita aos elementos de $\mathbb{Z}_m^*$, não ser uma operação sobre esse conjunto é acontecer de $\overline{a \cdot b} = \overline{0}$ para algum par de elementos desse conjunto. Mas isso implica $\overline{ab} = \overline{0}$ e, portanto, $ab \equiv 0 (\mathrm{mod}\, m)$. Daí, $m|ab$ e, como m é primo por hipótese, então $m|a$ ou $m|b$. Considerando-se, por exemplo, a primeira hipótese, $a = mq$, para algum inteiro q, e, portanto:

$$\overline{a} = \overline{mq} = \overline{m} \cdot \overline{q} = \overline{0} \cdot \overline{q} = \overline{0},$$

o que é um absurdo, visto que, por hipótese, $\overline{a} \in \mathbb{Z}_m^*$.

Mostraremos agora que, se m é primo, a multiplicação módulo m, quando restrita aos elementos de $\mathbb{Z}_m^*$, faz desse conjunto um grupo. Para isso basta mostrar que, qualquer que seja o elemento $\overline{a} \in \mathbb{Z}_m^*$, pode encontrar $\overline{b} \in \mathbb{Z}_m^*$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$.

De fato, $\overline{a} \in \mathbb{Z}_m^*$, então a não é múltilpo de m, pois $1 < a, b \leq m - 1$. E, como m é primo então $mdc(m, a) = 1$. Daí $mx_0 + ay_0 = 1$, para conveniente inteiros x_0 e y_0 (identidade de Bezout). Reduzindo-se essa igualdade módulo m:

$$\overline{mx_0 + ay_0} = \overline{m} \cdot \overline{x_0} + \overline{a} \cdot \overline{y_0} = \overline{a} \cdot \overline{y_0} = \overline{1},$$

o que mostra que $\overline{y_0}$ (que pertence a $\mathbb{Z}_m^*$) é o inverso de $\overline{a}$.

Grupos de permutações

Na teoria dos grupos entendemos por permutação uma bijeção de um conjunto nele mesmo.

Sejam S um conjunto não vazio e " $\circ$ " a operação de composição de funcões. Tomando o conjunto $G = \{f : S \to S\,;\, f \text{ é uma bijeção}\}$; temos que G é um grupo, chamado de grupo das permutações do conjunto S. Se $S = \{1, 2, 3, \ldots, n\}$ denotaremos esse grupo por S_n, e terá exatamente $n!$ elementos, uma vez que o número de permutações de n elementos é $n!$.

Denotaremos um elemento $f \in S_n$ por:

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}$$

Observação 2. .

- Para simplificar a notação, considerando a órbita por f de um elemento i de S_n, vamos denotar por $f^k(i) = ff \cdot f(i)$ operando f por k vezes. Digamos que $f^t(i) = i$ e que os demais elementos fora da órbita de i fiquem fixos por f. Então podemos denotar f por $(i, f(i), f^2(i), \cdots, f^{t-1})$. Por exemplo, dada uma função $f \in S_n$ onde $f(1) = 3$ e $f(3) = 1$ e para os demais temos $f(k) = k$. Denotaremos f por (13),

  $$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \ldots & n \\ 3 & 2 & 1 & 4 & 5 & \ldots & n \end{pmatrix} = (13),$$

  ou seja, a função f que permuta apenas os números 1 e 3 e fixa os demais, poderá ser representada apenas por $f = (13)$. Logo, os números que não aparecem são pontos fixos da função. Permutações de apenas dois elementos são chamadas de transposições ou 2-ciclos. Definimos por r-ciclo, com $1 < r \leq n$, uma permutação de r elemetos de S_n.

- Toda permutação pode ser escrita como composições de transposições, veja Hygino

e Iezzi (2003), por exemplo:

$$(12345) = (15)(14)(13)(12).$$

E ainda, toda permutação pode ser escrita como produto de ciclos disjuntos.

- Chamamos de grupo Alternado A_n o conjunto de todas as permutações que podem ser representadas a partir de um número par de transposições de S_n.

  Em particular, temos que:
  S_1 - o grupo trivial de um único elemento;
  S_2 - grupo abeliano, com $2! = 2$ elementos;
  S_3 - é um grupo com $3! = 6$ elementos, listados abaixo:

$$S_3 = \{f_0 = 1, f_1 = (123), f_2 = (132), g_1 = (23), g_2 = (13), g_3 = (12)\},$$

com

$$\begin{aligned} f_1 \circ g_1 &= (123) \circ (23) = (12) = g_3 \\ g_1 \circ f_1 &= (23) \circ (123) = (13) = g_2. \end{aligned}$$

O grupo S_3 é o "menor"grupo não abeliano. Todo grupo contendo no máximo 5 elementos é abeliano, para mais detalhes veja Gonçalves (2006).

Agora considere S_4, ou seja, o grupo das permutações de 4 elementos. Então o número de elementos de S_4 será $4! = 4 \times 3 \times 2 \times 1 = 24$, listados abaixo.

$$S_4 = \{1, (12)(34), (13)(24), (14)(23), (123), (124), (134), (234), (132), (142), (143),$$

$$(243), (12), (13), (14), (23), (24), (34), (1234), (1243), (1324), (1432), (1342), (1423)\}.$$

Observe que S_4 também não é abeliano, basta que $S_3 \leq S_4$. Para isso, basta considerar S_3 como os elementos de S_4 que fixam o 4.

Quando construímos polígonos regulares, podemos ordenar os seus vértices para formar uma espécie de referência: imagine os elementos de $S = \{1, 2, 3, 4\}$ como vértices de um quadrado. [1]

Ao considerarmos as diversas configurações que preservam distância e adjacências

[1] Figuras sobre simetrias retiradas do Wikipédia

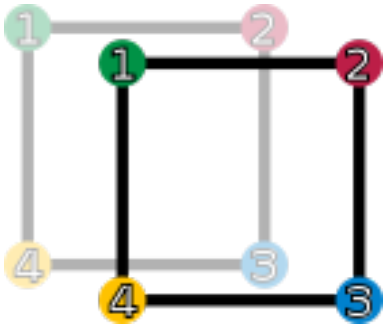
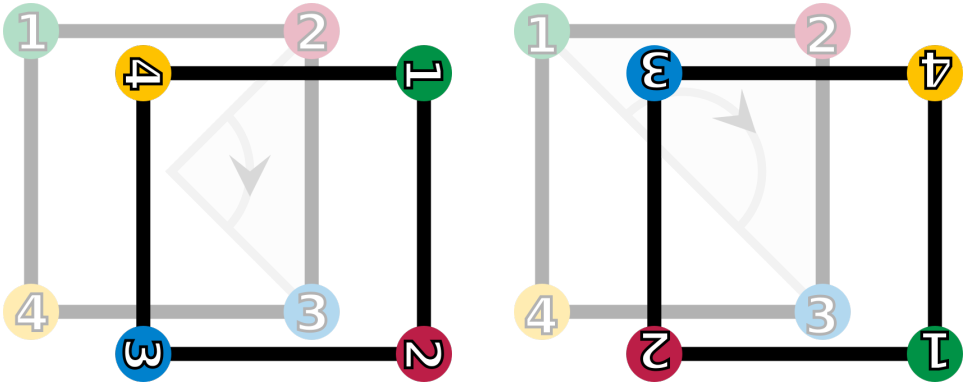


Figura 1.1: Simetrias do quadrado

temos um subconjunto de S_4, chamado de grupo diedral D_4. Observe que estas simetrias do quadrado permutam os seus vértices. Com isso, as simetrias do quadrado podem ser consideradas como elementos do grupo S_4 e denotado por D_4. Seus elementos são as rotações R_0, R_1, R_2, R_3 de 90° no sentido horário e as reflexões X, Y, Z, W.

Entendemos por uma rotação de 90° a mudança dos vértices do quadrado em uma unidade, no sentido horário. ou seja, $1 \to 4$, $2 \to 1$, $3 \to 2$ e $4 \to 3$, como mostra a figura abaixo:



(a) Rotação 90° (b) Rotação 180°

Figura 1.2: Rotações no quadrado

Para a reflexão temos quatro casos distintos, como mostra a figura abaixo, onde duas delas são feitas a partir das diagonais: x determinada pelos vértices 1 e 3 e y determinada pelos vértices 2 e 4, as outras duas são a partir de duas retas que dividem o quadrado em partes iguais, uma reta w horizontal e outra vertical z, determinadas por AC e BD, respectivamente.

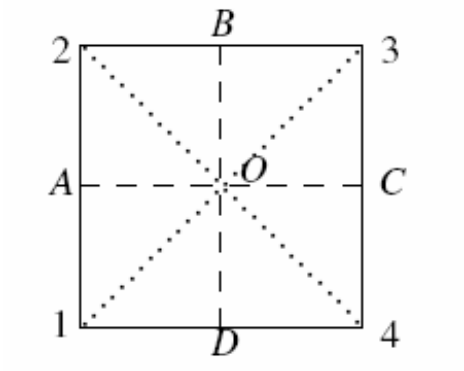
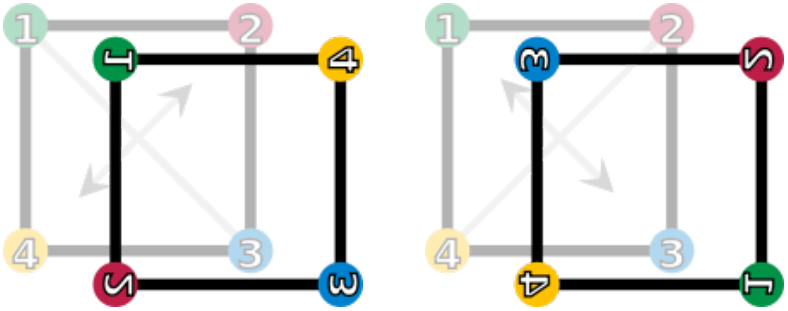


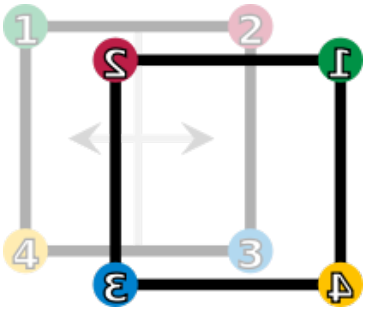
Figura 1.3: Reflexões no quadrado

As reflexões serão:

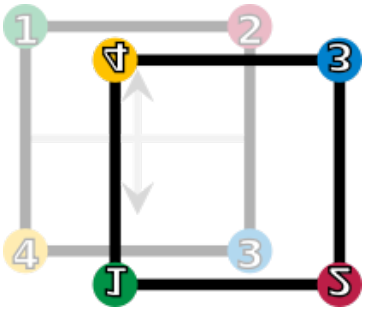


(a) Reflexão com relação a x

(b) Reflexão com relação a y



(c) Reflexão com relação a z



(d) Reflexão com relação a w

Figura 1.4: Reflexões no quadrado

Agora, exibiremos todos os elementos de D_4 e mostraremos que é um grupo. Inicialmente observemos que o conjunto de todas as rotações e reflexões do quadrado é

$$\{R_0, R_1, R_2, R_3, X, Y, Z, W\}.$$

A operação desse conjunto é a composição de funções, daí, analisando as figuras acima, identificamos termo a termo, respectivamente, com os seguintes elementos de S_4:

$$D_4 = \{1, (1432), (13)(24), (1234), (24), (13), (12)(34), (14)(23)\},$$

onde 1 representa a função identidade, que fixa todo elemento de $\{1, 2, 3, 4\}$. Essa identificação produz um subconjunto do grupo de permutação de oito elementos. Vamos olhar para a tábua de composição desse conjunto.

Tabela 1.1: Tábua de operações do grupo D_4

$\circ$	R_0	R_1	R_2	R_3	X	Y	Z	W
R_0	R_0	R_1	R_2	R_3	X	Y	Z	W
R_1	R_1	R_2	R_3	R_0	Z	W	Y	X
R_2	R_2	R_3	R_0	R_1	Y	X	W	Z
R_3	R_3	R_0	R_1	R_2	W	Z	Y	X
X	X	Z	Y	W	R_0	R_2	R_1	R_3
Y	Y	W	X	Z	R_2	R_0	R_3	R_1
Z	Z	Y	W	X	R_3	R_1	R_0	R_2
W	W	X	Z	Y	R_1	R_3	R_2	R_0

Sabemos que a composição de funções é associativa. Além disso, da tabela, podemos ver que D_4 é um grupo, pois é fechado com relação a composição, possui elemento neutro - R_0 e todos os elementos possuem simétrico (pois R_0 aparece em todas as linhas da tabela uma única vez). Também podemos observar que é um grupo não abeliano, uma vez que sua tábua não é simétrica em relação à diagonal principal. Note também que $R_1^2 = R_2$, $R_1^3 = R_1^2 \circ R_1 = R_2 \circ R_1 = R_3$, $X \circ R_1 = Z$, $X \circ R_1^2 = X \circ R_2 = Y$ e $X \circ R_1^3 = X \circ R_3 = W$. Assim,

$$D_4 = \{R_1^0,\ \ R_1,\ \ R_1^2,\ \ R_1^3,\ \ X,\ \ X \circ R_1,\ \ X \circ R_1^2,\ \ X \circ R_1^3\},$$

ou seja, é gerado apenas pelos elementos R_1 e X e como R_1 é a rotação dos vértices em $\pi/2$ então $R_1^4 = R_0$. Ainda, como X é a reflexão temos $X^2 = R_0$, ou seja, a ordem X é 2 e a priore, temos que a ordem de R_1 divide 4, como $R_1^2 \neq R_0$, segue que $o(R_1) = 4$. Podemos reescrever D_4 a partir dos seus geradores e suas ordens como

$$D_4 = \langle R_1, X :\ R_1^4 = X^2 = 1, R_1^3 = X \circ R_1 \circ X \rangle.$$

Observe que D_4 é um subconjunto de S_4 e pela tábua de operações ele é fechado com relação a composição, assim, D_4 tem estrutura de grupo. Veremos que subconjuntos de grupos com tais propriedades são chamados de subgrupos.

Um fato interessante sobre grupos de permutações é o seguinte teorema.

Teorema 2. *Os ciclos* (12) *e* $(12 \cdots n)$ *geram o grupo* S_n.

A demonstração pode ser encontrada em Gonçalves (2006).

1.4 Subgrupos

Definição 5. *Seja $(G, *)$ um grupo. Diz - se que um subconjunto não vazio $H \subset G$ é um subgrupo de G se:*

- *H é fechado para a operação $*$ (isto é, se $a, b \in H$ então $a * b \in H$);*
- *$(H, *)$ também é um grupo (aqui o símbolo $*$ indica a restrição da operação de G aos elementos de H).*

Proposição 3. *Seja $(G, *)$ um grupo. Para que um subconjunto não vazio $H \subset G$ seja um subgrupo de G é necessário e suficiente que: $a * b^{-1} \in H$, $\forall\, a, b \in H$.*

Demonstração. ($\Rightarrow$) Para $h \in H$, temos que $h \in G$. Como H é grupo, exite $h' \in H$, inverso de h, e temos que H é fechado. Logo, $hh' \in H$. Como $h \in G$ e $hh' = e$, temos que $e \in H$. Ainda, $hh' = e_H$. Pela unicidade de neuto em H, segue que $e = e_H$.

Tomemos agora um elemento $b \in H$ e indiquemos por b^{-1} e b_h^{-1} seus simétricos em G e H, respectivamente. Como, porém,

$$b_h^{-1} * b = e_h = e = b^{-1} * b$$

então, $b_h^{-1} = b^{-1}$. Por fim, se a, $b \in H$, então $a * b_h^{-1} \in H$, uma vez que, por hipótese, $(H, *)$ é um grupo. Mas $b_h^{-1} = b^{-1}$ e, portanto, $a * b^{-1} \in H$.
($\Leftarrow$) Como, por hipótese, H não é vazio, podemos considerar um elemento $x_0 \in H$. Juntando esse fato à hipótese: $x_0 * x_0^{-1} = e \in H$. Considerando agora um elemento $b \in H$, da hipótese e da conclusão anterior segue que $e * b^{-1} = b^{-1} \in H$.

Mostremos agora que H é fechado para a operação $*$. De fato, se $a, b \in H$, então, levando em conta a conclusão anterior, $a, b^{-1} \in H$. De onde (novamente usando a hipótese):

$$a * (b^{-1})^{-1} = a * b \in H.$$

Falta mostrar a associatividade em H, mas isso é trivial, pois, se $a, b, c \in H$, então $a, b, c \in G$ e, portanto, $a * (b * c) = (a * b) * c$ (já que essa propriedade vale em G). □

Exemplo 3. *1.* $\{e\}$ e G são subgrupos de G, chamados de subgrupos triviais.

2. Observando a Tábua 1.1 conseguimos dois subgrupos de fácil vizualização de D_4, sendo um formado pelas rotações e o segundo formado pela reflexão

$$C_4 = \{R_1^0, R_1, R_1^2, R_1^3\} = \langle R_1 \rangle \qquad F = \{1, X\} = \langle X \rangle.$$

3. Consideremos o grupo aditivo $M_2(\mathbb{R})$, vamos mostrar, usando a propriedade anterior que

$$H = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_2(\mathbb{R});\ a_{11} + a_{22} = 0 \right\}$$

é um subgrupo de $M_2(\mathbb{R})$. Trata-se de um conjunto não vazio. Note que as matrizes de H se caracterizam pelo fato de os elementos de H da diagonal principal serem opostos um do outro. Observado isso, tomemos duas matrizes de H

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & -a_{11} \end{pmatrix} \text{ e } B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & -b_{11} \end{pmatrix},$$

como as entradas dessas matrizes são número reais, fazendo $A+(-B) = C$, teremos

$$C = \begin{pmatrix} a_{11} - b_{11} & a_{12} - b_{12} \\ a_{21} - b_{21} & -a_{11} + b_{11} \end{pmatrix}$$

e a soma da diagonal principal será

$$a_{11} - b_{11} + (-a_{11} + b_{11}) = 0.$$

Logo, $A + (-B) \in H$.

Observação 3. *Seja $(G, *)$ um grupo. O subconjunto $H = \{\langle a \rangle;\ a \in G\}$ é um subgrupo grupo de G. com $|H| = o(a)$.*

1.4.1 Teorema de Lagrange e subgrupos normais

Definição 6. *Sejam G um grupo, H um subgrupo e $a \in G$. Os subconjuntos de G, $aH = \{ah; h \in H\}$ e $Ha = \{ha; h \in H\}$ são chamados classe lateral à esquerda e classe*

lateral à direita de H em G, respectivamente.

Da definição acima decorre uma relação de equivalência definida por $a \sim b$ se, e somente se, $a^{-1}b \in G$, onde $a, b \in H \subseteq G$. E com isso o conjunto das classes laterais, em relação a H, determina uma partição de G, ou seja:

$$\textbf{i)} \quad \text{se} \quad a \in G, \text{então} \;\; aH \neq \emptyset; \tag{1.4}$$

$$\textbf{ii)} \quad \text{se} \quad a, b \in G, \text{então} \;\; aH = bH \;\; \text{ou} \;\; aH \cap bH = \emptyset; \tag{1.5}$$

$$\textbf{iii)} \quad \text{a união de todas as classes laterais é igual a} \;\; G. \tag{1.6}$$

O conjunto das classes laterais à esquerda aH, ou à direita Ha, é chamado de conjunto quociente e denotado por G/H. Observe que: é indiferente usarmos o conjunto quociente como sendo o conjunto das classes à esquerda (que usaremos) ou à direita devido a existência da bijeção

$$\begin{array}{rccc} f: & G/H & \to & G/H \\ & aH & \longmapsto & f(a) = Ha^{-1} \end{array}.$$

Exemplo 4. Seja G o grupo aditivo $\mathbb{Z}_8$, ou seja $\mathbb{Z}_8 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}$. Considerando o subgrupo $H = \{\overline{0}, \overline{4}\}$, temos:

$$\overline{0} + H = H, \;\; \overline{1} + H = \{\overline{1}, \overline{5}\}, \;\; \overline{2} + H = \{\overline{2}, \overline{6}\}, \;\; \overline{3} + H = \{\overline{3}, \overline{7}\},$$
$$\overline{4} + H = \{\overline{4}, \overline{0}\}, \;\; \overline{5} + H = \{\overline{5}, \overline{1}\}, \;\; \overline{6} + H = \{\overline{6}, \overline{2}\}, \;\; \overline{7} + H = \{\overline{7}, \overline{3}\}.$$

O conjunto das classes é formado apenas pelas classes distintas, então:

$$G/H = \{H, \;\; \overline{1} + H, \;\; \overline{2} + H, \;\; \overline{3} + H\}$$

e também

$$G = \bigcup_{j=0}^{3} (\overline{j} + H).$$

Se G é um grupo finito, então o conjunto G/H também é finito. O número de elementos de G/H é chamado índice de H em G e é denotado por $(G : H)$. Assim, no exemplo anterior temos: $(G : H) = 4$.

Proposição 4. *Seja H um subgrupo de G. Então duas classes laterais quaisquer em relação a H são subconjuntos de G que têm a mesma cardinalidade.*

Demonstração. Dadas duas classes laterais aH e bH, temos que mostrar que é possível construir uma aplicação bijetora $f : aH \to bH$. Lembrando a forma geral dos elementos dessas classes, é natural definir f da seguinte maneira: $f(ah) = bh$, para qualquer $h \in H$. Vamos mostrar que f é injetora e sobrejetora. De fato:

- (injetora) Se $h, h_1 \in H$ e $f(ah) = f(ah_1)$, então $bh = bh_1$; operando b^{-1} a esquerda em ambos os lados, então $h = h_1$.
- (sobrejetora) Seja $y \in bH$. Então $y = bh$, para algum $h \in H$. Tomando-se $x = ah \in aH$, então $f(x) = f(ah) = bh = y$. □

1.4.2 Teorema de Lagrange

Teorema 5 (Lagrange)**.** *Seja H um subgrupo de um grupo finito G. Então $|G| = (G : H)|H|$ e, portanto, $\dfrac{|G|}{|H|}$ é um número inteiro.*

Demonstração. Suponhamos que o $(G : H) = r$ e seja $G/H = \{a_1H, a_2H, \cdots, a_rH\}$. Então pelas equações 1.4, 1.5 e 1.6, $G = a_1H \cup a_2H \cup \cdots \cup a_rH$ com $a_iH \cap a_jH = \emptyset$, sempre que $i \neq j$. Mas, pela proposição (4), o número de elementos de cada uma das classes laterais é igual ao número de elementos de H, ou seja, é igual a $|H|$. Portanto:

$$|G| = |H| + |H| + \cdots + |H|,$$

em que o número de parcelas é $r = (G : H)$. De onde:

$$|G| = (G : H)|H|$$

e $\dfrac{|G|}{|H|}$ é inteiro. □

Corolário 6. *Seja G um grupo finito. Então a ordem de um elemento $a \in G$ divide a ordem de G e $(G : H) = |G|/|H|$, em que $H = \langle a \rangle$.*

Demonstração. Basta lembrar que a ordem de a é igual a ordem de $\langle a \rangle$ e que, devido ao Teorema de Lagrange:

$$|G| = (G : \langle a \rangle)|\langle a \rangle|.$$

□

Corolário 7. *Se a é um elemento de um grupo finito G, então $a^{|G|} = e$ (elemento neutro do grupo).*

Demonstração. Seja n a ordem de a. Portanto, n é o menor inteiro estritamente positivo tal que $a^n = e$ (elemento neutro do grupo). Mas, devido ao corolário anterior:

$$|G| = (G : H)n,$$

em que $H = \langle a \rangle$. Portanto:

$$a^{|G|} = a^{(G:H)n} = (a^n)^{(G:H)} = e^{(G:H)} = e.$$

□

Corolário 8. *Seja G um grupo finito cuja ordem é um número primo. Então G é cíclico. Em particular é abeliano, e os únicos subgrupos de G são os triviais, ou seja, $\{e\}$ e o próprio G.*

Demonstração. Seja $p = |G|$. Como $p > 1$, o grupo G possui um elemento a diferente do elemento neutro. Assim, se $H = \langle a \rangle$, o teorema de Lagrange garante que $|H| \,|\, p$. Logo, $|H| = 1$ ou p e, portanto, $H = \{e\}$ ou $H = G$. Como a primeira dessas hipóteses é impossível, então $G = H$ e, portanto, G é cíclico. Por outro lado, se J é um subgrupo de G, então, ainda devido ao teorema de Lagrange, $|J| \,|\, |G|$. Daí, $|J| = 1$ ou p e, portanto, $J = \{e\}$ ou $J = G$. □

Teorema 9 (Teorema de Cauchy)**.** *Se um primo p divide a ordem de um grupo finito G, então G tem um elemento de ordem p.*

A demonstração pode ser encontrada em Gonçalves (2006).

Proposição 10. *Se G é um grupo tal que $|G| \leq 5$ então G é abeliano.*

Demonstração. Se $|G| = 1$ então $G = \{e\}$. Agora, se $|G| = 2, 3$ ou 5 então $|G|$ é prima implicando que G é cílico e logo é abeliano. Se $|G| = 4$ e existe $x \neq e$, $x \in G$ tal que $\langle x \rangle = G$ então G é cíclico e portanto abeliano.

Suponhamos então que: $\forall\, x \in G$, temos $\langle x \rangle \neq G$. Ora pelo Teorema de Lagrange segue imediatamente que $|\langle x \rangle| = 2$. Assim,

$$x^2 = e,\ \forall\, x \in G.$$

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

Isso nem sempre é verdade se a ordem de um grupo G é maior que 5. Se considerarmos o grupo das permutações de grau 3, S_3. Vimos que $|S_3| = 3! = 6$, e seus elementos são:

$$S_3 = \{f_0 = 1, f_1 = (123), f_2 = (132), g_1 = (23), g_2 = (13), g_3 = (12)\}.$$

Operando dois de seus elementos, teremos:

$$\begin{aligned} f_1 \circ g_2 &= (123) \circ (13) = (23) = g_1 \\ g_2 \circ f_1 &= (13) \circ (123) = (12) = g_3, \end{aligned}$$

onde vemos que S_3 não é abeliano.

Mas observe que, para todo $n > 0$, $\mathbb{Z}_n$ é abeliano (aditivo). Ou seja, existem grupos abelianos para qualquer ordem.

1.4.3 Subgrupos normais

Definição 7. *Seja $(G, \cdot)$ um grupo e A e B subconjuntos de G. Indicaremos por AB e chamaremos de produto de A por B o seguinte subconjunto de G:*

$$AB = \emptyset, \quad se \quad A = \emptyset \quad ou \quad B = \emptyset$$
$$AB = \{xy : x \in A \quad e \quad y \in B\}, \quad se \quad A \neq \emptyset \quad e \quad B \neq \emptyset.$$

No contexto de teoria de grupos, dado H um subgrupo de G então $HH = H$, pois é fechado com relação a operação. E esse fato será importante para os próximos tópicos.

Definição 8. *Um subgrupo N de um grupo G é chamado subgrupo normal se, para todo $x \in G$, se verifica*

$$xN = Nx.$$

Ou seja, a classe lateral à esquerda, com relação a N, determinada por x, é igual a classe

lateral à direita, com relação a N, determinada por x, para qualquer $x \in G$. Para indicar que N é um subgrupo normal de G usaremos a notação: $N \lhd G$.

Exemplo 5. Considerando o grupo diedral $D_4 = \{R_1^0, R_1, R_1^2, R_1^3, X, XR_1, XR_1^2, XR_1^3\}$. Lembrando que $R_1^0 = 1, R_1 = (1432), R_1^2 = (13)(24), R_1^3 = (1234)$. O subgrupo $H = C_4 = \{R_1^0, R_1, R_1^2, R_1^3\}$ é normal, pois, como se pode ver, conferindo a Tábua 1.1:

$$\begin{array}{ll} R_1^0H = \{R_1^0, R_1, R_1^2, R_1^3\} = HR_1^0 & XH = \{X, XR_1, XR_1^2, XR_1^3\} = HX \\ R_1H = \{R_1, R_1^2, R_1^3, R_1^0\} = HR_1 & (XR_1)H = \{XR_1, XR_1^2, XR_1^3, X\} = H(XR_1) \\ R_1^2H = \{R_1^2, R_1^3, R_1^0, R_1\} = HR_1^2 & (XR_1^2)H = \{XR_1^2, XR_1^3, X, XR_1\} = H(XR_1^2) \\ R_1^3H = \{R_1^3, R_1^0, R_1, R_1^2\} = HR_1^3 & (XR_1^3)H = \{XR_1^3, X, XR_1, XR_1^2\} = H(XR_1^3) \end{array}$$

Como há duas classes laterais distintas: R_1^0H e XH então $(D_4 : C_4) = 2$.

Exemplo 6. Em S_3 há subgrupos que não são normais, por exemplo o subgrupo gerado por $\langle(12)\rangle = \{1, (12)\}$. Observe que

$$\begin{aligned} (13) \circ (12) &= (123) \Rightarrow (13)\langle(12)\rangle = \{(13), (123)\} \\ (12) \circ (13) &= (132) \Rightarrow \langle(12)\rangle(13) = \{(13), (132)\}, \end{aligned}$$

como dissemos inicialmente.

Observação 4. Seja H um subgrupo de G tal que $(G : H) = 2$. Então H é um subgrupo normal de G. De fato, nesse caso, as classes laterais à esquerda, com relação a H, são duas: H e aH, em que a é um elemento qualquer do grupo que não pertence a H, e, portanto, $aH = H^c$ (o complementar de H em G), pois as duas classes formam uma partição de G. As classes laterais à direita em relação a H, também são duas: H e Ha, em que a é um elemento qualquer do grupo que não pertence a H, e, portanto, $Ha = H^c$. Logo

$$aH = H^c = Ha$$

e pela arbitrariedade de a, temos que $xH = Hx$, qualquer que seja $x \in G$. Como havíamos afirmado.

Proposição 11. *Para todo $n > 1$, o conjunto A_n é um subgrupo, de ordem $\frac{n!}{2}$ e índice 2, de S_n.*

A demonstração pode ser encontrada em Hygino e Iezzi (2003).

Agora vamos entender como operar elementos do conjunto quociente. Dado um grupo G e um subgrupo normal N, definimos a operação entre dois elementos $aN, bN \in G/N$ como

$$(aN)(bN) = (ab)N.$$

Com essa operação, caso N seja normal a G, então G/N será um grupo que denominamos por grupo quociente. De fato,

- $[(aN)(bN)](cN) = (aN)[(bN)(cN)]$;
- $(aN)(eN) = (ae)N = aN = (ea)N = (eN)(aN)$;
- $(aN)(a^{-1}N) = (aa^{-1})N = (eN) = (a^{-1}a)N = (a^{-1}N)(aN)$. Portanto, o conjunto quociente G/N, com a multiplicação de subconjuntos, restrita aos seus elementos, é um grupo cujo elemento neutro é $eN = N$ e no qual $(aN)^{-1} = a^{-1}N$.

Exemplo 7. Considere o subgrupo de D_4 de S_4. Pelo Exemplo 5, temos que C_4 é um subgrupo normal de D_4, com

$$G/C_4 = \{H, XH\}.$$

Sua tábua de operações será:

Tabela 1.2: Tábua de D_4/C_4

$\circ$	H	XH
H	H	XH
XH	XH	H

Pela Tábua, G/C_4 é um grupo.

Se compararmos o grupo G/C_4 com o grupo $\mathbb{Z}_2$ veremos que suas tábuas de operações possuem o mesmo "comportamento". Na verdade é possível estabelecer uma função que preserva as operações envolvidas entre os dois grupos. No decorrer do trabalho veremos as condições necessárias para que seja possível estabelecer esse tipo de relação.

1.4.4 Grupos solúveis

Definição 9. *Um grupo G é solúvel se este tem uma sequência finita de subgrupos,*

$$1 \subseteq G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

tais que,

i) $G_i \lhd G_{i+1}$, *para* $i = 0, \cdots n-1$;

ii) G_{i+1}/G_i *é abeliano para* $i = 0, \cdots n-1$.

Exemplos

1. Todo grupo abeliano G é solúvel com $1 \lhd G$.

2. O grupo diedral D_4 de ordem 8 é solúvel. Pois vimos que ele tem um subgrupo normal C_4 de ordem 4, cujo quociente tem ordem 2, e C_4 é abeliano, então

$$1 \lhd C_4 \lhd D_4.$$

3. S_3 é solúvel! De fato, considere $U = \langle(123)\rangle = \{1, (123), (132)\}$ de S_3. Como S_3 possui 6 elementos e U possui 3 elementos então pelo Teorema de Lagrange temos que $(S_3 : U) = 2$. Logo, pela observação 4, $U \lhd S_3$ e S_3/U é abeliano e, como U também é abeliano, S_3 é solúvel.

4. O grupo simétrico S_4 é solúvel, com a sequência

$$1 \lhd V \lhd A_4 \lhd S_4,$$

em que, $A_4 = \langle a, b; a^3, b^2, (ab)^3\rangle$ onde $a = (234)$ e $b = (12)(34)$ é o grupo Alternado de ordem 12, e V é o grupo de Klein, grupo consistido das permutações $1, (12)(34), (13)(24), (14)(23)$. Vejamos.

Inicialmente $(S_4 : A_4) = 2$, pela Observaçao 4, $A_4 \lhd S_4$.

Agora, por definição, V é nomal a A_4 se $\forall\, x \in A_4$ temos $x^{-1}Vx = V$. Como A_4 é gerado por $(234), (12)(34)$, é suficiente analisarmos apenas os geradores. Assim, para $x = (234)$

$$\begin{aligned}(243) \circ (12)(34) \circ (234) &= (14)(23)\\ (243) \circ (13)(24) \circ (234) &= (12)(34)\\ (243) \circ (14)(23) \circ (234) &= (13)(24).\end{aligned}$$

Agora, $x = (12)(34)$. Como x também é um elemento de V então sua operação com qualquer elemento de V está em V. Isso mostra que $V \lhd A_4$. A ordem dos conjuntos quocientes são: $|V/1| = 4, |V/A_4| = 3, |S_4/A_4| = 2$ que pela Proposição 10 são abelianos.

Agora, para $n \geq 5$, S_n não é solúvel. Mostraremos que S_5 não é solúvel e para isso, é suficiente mostrar que $A_5 \subset S_5$ não é solúvel. Para isso, é necessário o seguinte resultado:

Teorema 12. *Sejam G um grupo, H um subgrupo de G e N um subgrupo normal de G, assim,*

i) Se G é solúvel, então H é solúvel.

ii) Se G é solúvel, então G/N é solúvel.

iii) Se N e G/N são solúveis, então G é solúvel.

A demonstração pode ser encontrada em Gonçalves (2006).

Definição 10. *Um grupo G é simples se seus subgrupos normais são 1 e G.*

Exemplo 8. O grupo $\mathbb{Z}_5$ é simples, pois os únicos subgrupos são $\{1\}$ e $\mathbb{Z}_5$ que são normais e abelianos, portanto, solúveis. Ainda mais, $\mathbb{Z}_p$ é simples para todo p primo.

Teorema 13. *Seja G um grupo solúvel de ordem finita. Então, G é simples se, e somente se, é cíclico e de ordem prima.*

Demonstração. ($\Rightarrow$) Suponhamos que G é um grupo solúvel, então, este tem uma sequência

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G,$$

na qual devemos assumir $G_{i+1} \neq G_i$. Assim, G_{n-1} é um subgrupo normal próprio de G. Entretanto, G é simples, logo $G_{n-1} = 1$ e $G/G_{n-1} = G$, então, pela definição de solubilidade, G é abeliano. Assim G é abeliano e simples, o que significa que os únicos subgrupos de G são os triviais. Como G é finito, pelo Teorema de Lagrange, dado um primo p que divide $|G|$, existe $g \in G$, $g \neq 1$, com ordem p. Assim, $\langle g \rangle = 1$ ou $\langle g \rangle = G$. Vale a última igualdade, pois $G \neq 1$. Logo, G é cíclico de ordem p.

($\Leftarrow$) Como G é de ordem prima então os únicos subgrupos são os triviais, logo, simples. Por ser cíclico, será abeliano, ou seja, solúvel. □

Teorema 14. *O grupo A_n, $n \geq 3$, é gerado pelo conjunto de todos os $3-$cíclos de S_n.*

Para a demonstração veja Gonçalves (2006).

Teorema 15. *Se $n \geq 5$, então, o grupo alternado A_n é simples.*

Demonstração. Suponhamos que $1 \neq N \lhd A_n$. Nossa estratégia será a seguinte: observemos, primeiramente, que se N contém um 3-ciclo, da forma (abc), então contém todos os 3-ciclos. E como os 3-ciclos geram o A_n, devemos ter $N = A_n$. Segundo, mostraremos que N deve conter um 3-ciclo. Neste momento, é que temos como essencial, o fato de que $n \geq 5$.

Suponhamos, então, que N contenha um 3-ciclo. Sem perda de generalidade, N, contenha (123). Assim, para qualquer $k > 3$, o ciclo $(32k)$ é uma permutação par, e, portanto, pertence a A_n. Logo,

$$(32k)^{-1}(123)(32k) = (1k2),$$

pertence a N. Portanto, N contém $(1k2)^2 = (12k)$ para todo $k \geq 3$. Afirmamos que N é gerado por todos os 3-ciclos da forma $(12k)$.

De fato! Se $n = 3$, temos a afirmação verdadeira. Caso, $n > 3$, temos que para todos $a, b > 2$, a permutação $(1a)(2b)$ é par, portanto, pertence a A_n. Assim, N contém

$$((1a)(2b))^{-1}(12k)(1a)(2b) = (abk),$$

se $k \neq a, b$. Como, A_n é gerado por todos os 3-ciclos, segue que $N = A_n$.

Resta mostrarmos que N contém ao menos um 3-ciclo. Faremos isto pela análise dos casos:

i) Suponhamos que N contenha um elemento $x = abc\cdots$, em que $a, b, c, \cdots$ sejam ciclos disjuntos e,

$$a = (a_1 \cdots a_m)(m \geq 4).$$

Consideremos $t = (a_1 a_2 a_3)$. Então, N contém $t^{-1}xt$. Como, t comuta com $b, c, \cdots$ (ciclos disjuntos), segue que,

$$t^{-1}xt = (t^{-1}at)bc\cdots = z(digamos).$$

Então, N contém,

$$zx^{-1} = (a_1 a_3 a_m),$$

que é um 3-ciclo.

ii) Suponhamos, agora, que N contenha um elemento envolvendo ao menos dois 3-ciclos. Sem perda de generalidade, N contém,

$$x = (123)(456)y,$$

y é uma permutação fixando $1, 2, 3, 4, 5, 6$. Consideremos $t = (234)$. Então, N contém,

$$(t^{-1}xt)x^{-1} = (12436).$$

Assim, pelo caso anterior, N contém um 3-ciclo.

iii) Suponhamos que N contenha um elemento de x da forma $(ijk)p$, em que, p é um produto de 2-ciclos disjuntos de (ijk). Então, N contém $x^2 = (ijk)$, que é um 3-ciclo.

iv) Resta apenas, o caso em que todo elemento de N é um produto disjunto de 2-ciclos. (Isto ocorre na verdade quando $n = 4$, dado pelo grupo de Klein V). Mas, como $n \geq 5$, podemos assumir que N contém,

$$x = (12)(34)p,$$

em que p fixa $1, 2, 3, 4$. Se considerarmos, $t = (234)$, teremos que N contém

$$(t^{-1}xt)^{-1}x^{-1} = (14)(23),$$

e se $u = (145)$, N contém,

$$u^{-1}(t^{-1}xtx^{-1})u = (45)(23),$$

assim, N contém,

$$(45)(23)(14)(23) = (145),$$

contradizendo o fato de termos assumido que todo elemento de N é um produto de 2-ciclos disjuntos. Portanto, A_n é simples se $n \geq 5$. □

Na verdade, A_5 é o "menor"grupo simples, não abeliano, resultado provado primeiramente por Galois.

Corolário 16. *O grupo simétrico S_n é não solúvel para $n \geq 5$.*

Demonstração. Se S_n fosse solúvel, teríamos que A_n seria solúvel (Teorema 12) e simples (Teorema 15), e portanto, de ordem prima pelo Teorema 13. Mas, $|A_n| = \frac{1}{2}(n!)$, e não é primo se $n \geq 5$. □

1.5 Homomorfismo e isomorfismo de grupos

O principal objetivo deste tópico é a compreensão do conceito de isomorfismo de grupos. Veremos que a partir do isomorfismo as propriedades entre grupos classificados em uma mesma classe são preservadas e será de grande utilidade para o estudo de solubilidade dos polinômios.

Definição 11. *Dá-se o nome de homomorfismo de um grupo $(G, *)$ num grupo $(J, \cdot)$ a toda aplicação $f : G \to J$, tais que quaisquer que sejam $x, y \in G$:*

$$f(x * y) = f(x) \cdot f(y).$$

Exemplo 9. Sejam os grupos $G = (\mathbb{R}_+^*, \cdot)$ e $H = (\mathbb{R}, +)$. Defina a aplicação $f : G \to H$ por $f(x) = log(x)$. A aplicação f assim definida é um homomorfismo. De fato, para todos $x, y \in \mathbb{R}_+^*$ temos:

$$f(xy) = log(xy) = log(x) + log(y) = f(x) + f(y).$$

Definição 12. *Se a aplicação $f : G \to H$ é injetora, então é chamado de homomorfismo injetor (monomorfismo).*

Definição 13. *Se a aplicação $f : G \to H$ é sobrejetora, então é chamado de homomorfismo sobrejetor.*

Exemplo 10. Existe um homomorfismo bijetor entre os grupos $G = (\mathbb{R}, +)$ e $H = (\mathbb{R}_+^*, \cdot)$. De fato, a aplicação $f : G \to H$ definida por $f(x) = 3^x$ é um homomorfismo bijetor, pois:

i) A aplicação é um homomorfismo,

$$f(x, y) = 3^{x+y} = 3^x \cdot 3^y = f(x) \cdot f(y), \quad \forall\, x, y \in \mathbb{R}.$$

ii) A aplicação é injetora,

$$\forall \;\; x, y \in \mathbb{R}, \quad f(x) = f(y) \Rightarrow 3^x = 3^y \Rightarrow x = y.$$

iii) A aplicação f é sobrejetora, $\forall\, y \in H$, temos que existe $x = log_3(y) \in G$ tal que

$$f(x) = 3^{log_3(y)} = y.$$

Definição 14. *Se a aplicação $f : G \to H$ é um homomorfismo bijetor, então é chamado de isomorfismo. Se dois grupos G, J são isomorfos, denotamos por $G \cong J$.*

No Exemplo 7 construímos o grupo quociente D_4/C_4. Trabalhar com esses quocientes, às vezes, pode ser uma tarefa um pouco complicada. Afim de melhorar ou simplesmente tornar esses grupos mais tratáveis podemos associá-los a grupos conhecidos.

Seja $f : D_4/C_4 \to (\mathbb{Z}_2, +)$ um homomorfismo tal que

$$f(H) = \overline{0} \;\; e \;\; f(xH) = \overline{1},$$

com $x \in D_4$. Temos que f é bijetora e preserva operações, no sentido;

$$\overline{0} = \overline{1} + \overline{1} = f(xH) + f(xH) = f[(xH)(xH)] = f(H)$$

$$\overline{1} = \overline{1} + \overline{0} = f(xH) + f(H) = f[(xH)(H)] = f(xH).$$

Logo, os dois grupos são isoformos, $D_4/C_4 \cong \mathbb{Z}_2$. Em álgebra, grupos isomorfos são considerados "iguais", sendo possível substituir um pelo outro convenientemente.

Definição 15. *Um homomorfismo $f : G \to G$ é chamado também de endomorfismo de*

G, já os isomorfismos de G sobre si mesmo são chamados de automorfismos de G.

Seguindo a ideia de associar um grupo qualquer a um grupo conhecido mais tratável, segue:

Teorema 17 (Teorema de Cayley)**.** *Todo grupo finito é isomorfo a um subgrupo de um grupo de permutações.*

A demonstração pode ser encontrada em Gonçalves (2006).

1.5.1 Proposições sobre homomorfismos de grupos

Sejam G e J grupos cujos elementos neutros indicaremos por e e u, respectivamente, e $f : G \to J$ um homomorfismo de grupos.

Proposição 18. $f(e) = u$.

Demonstração. Como e é o elemento neutro de G então $ee = e$ e $uf(e) = f(e)$, pois $f(e) \in J$ e u é o elemento neutro de J. Levando-se em conta isso e a hipótese de que f é um homomorfismo:

$$f(e)f(e) = f(ee) = f(e) = uf(e) \text{ implicando } f(e) = u.$$

□

Proposição 19. *Se a é um elemento qualquer de G então* $f(a^{-1}) = [f(a)]^{-1}$.

Demonstração. Usando a proposição anterior,

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = u = f(a)[f(a)]^{-1} \text{ implicando } f(a^{-1}) = [f(a)]^{-1}.$$

□

Corolário 20. $f(ab^{-1}) = f(a)[f(b)]^{-1}$.

Proposição 21. *Se H é um subgrupo de G, então* $f(H)$ *é um subgrupo de J.*

Demonstração. Lembremos primeiro que $f(H) = \{f(x); x \in H\}$.

i) Como $e \in H$, pois H é um subgrupo de G, então $f(e) = u \in f(H)$ e, portanto, $f(H) \neq \emptyset$.

ii) Sejam $c, d \in f(H)$. Então $c = f(a)$ e $d = f(b)$, para convenientes elementos $a, b \in H$. Logo, $cd^{-1} = f(a)[f(b)]^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$. Como $ab^{-1} \in H$, pois, por hipótese, H é um subgrupo de G, então $cd^{-1} \in f(H)$. □

Definição 16. *Seja $f : G \to J$ um homomorfismo de grupos. O seguinte subconjunto de G será chamado núcleo de f e denotado por $N(f)$.*

$$N(f) = \{x \in G; f(x) = u\}.$$

Exemplo 11. Seja $f : \mathbb{Q}^* \to \mathbb{R}^*$ definida por $f(x) = x^2$. O elemento neutro de $\mathbb{R}^*$ é 1. Se $x \in N(f)$, então devemos ter $f(x) = 1$, ou seja, $x^2 = 1$ então $x = \pm 1$. Logo, o $N(f) = \{-1, +1\}$.

Proposição 22. *Seja $f : G \to J$ um homomorfismo de grupos. Então:*

i) $N(f)$ é um subgrupo normal de G;

ii) f é um homomorfismo injetor se, e somente se, $N(f) = \{e\}$.

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

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

Isso mostra que $ab^{-1} \in N(f)$. Agora, se $n \in N(f)$ e $g \in G$ temos,

$$f(g^{-1}ng) = f(g)^{-1}f(n)f(g) = f(g)^{-1}uf(g) = u,$$

ou seja, $g^{-1}ng \in N(f)$ para todo $n \in N(f)$ e todo $g \in G$. Assim, $N(f)$ é um subgrupo normal de G

ii) ($\Rightarrow$) Por hipótese f é injetora. Vamos mostrar que o único elemento de $N(f)$ é e (elemento neutro de G). Para isso, vamos tomar $a \in N(f)$ e demonstrar que necessariamente $a = e$. De fato, como $a \in N(f)$ então $f(a) = u$. Mas, devido a proposição, $f(e) = u$. Portanto, $f(a) = f(e)$. Como, porém, f é injetora, por hipótese, então $a = e$.

($\Leftarrow$) Sejam $x_1, x_2 \in G$ elementos tais que $f(x_1) = f(x_2)$. Multiplicando cada membro dessa igualdade por $f[(x_2)]^{-1}$, obtemos $f(x_1)f[(x_2)]^{-1} = u$. Mas, devido ao corolário da proposição, $f(x_1)f[(x_2)]^{-1} = u = f(x_1x_2^{-1})$. Portanto, $f(x_1x_2^{-1}) = u$, o que mostra que $x_1x_2^{-1} \in N(f) = e$. Então $x_1x_2^{-1} = e$ e, portanto, $x_1 = x_2$. De onde, f é injetora, como queríamos provar. □

Teorema 23 (Teorema do homomorfismo para grupos)**.** *Seja $f : G \to J$ um homormofismo sobrejetor de grupos. Se $N = N(f)$, então o grupo quociente G/N é isomorfo ao grupo J .*

Demonstração. Seja $\overline{G} = G/N$ e $N \triangleleft G$. Vamos definir

$$\widehat{f}: \quad \overline{G} \to Im(f), \quad \widehat{f}(xN) := f(x).$$

Mostraremos que $\widehat{f}$ é um isomorfismo de grupos.

- $\widehat{f}$ é uma função bem definida. De fato, se $xN = yN$ então, $y^{-1}x \in N$, isto é, $f(y^{-1}x) = u$, que pode ser escrito $f(y^{-1})f(x) = u$ e multiplicando a esquerda por $f(y)$ obtemos $f(x) = f(y)$, em outras palavras $\widehat{f}(xN) = \widehat{f}(yN)$.
- $\widehat{f}$ é um homomorfismo. Se $xN, yN \in \overline{G}$, temos

$$\widehat{f}(xNyN) = \widehat{f}(xyN) = f(xy) = f(x)f(y) = \widehat{f}(xN)\widehat{f}(yN),$$

- $\widehat{f}$ é sobrejetivo. Se $b \in Im(f)$ então $b = f(x)$ para algum $x \in \overline{G}$. Logo, $b = f(x) = \widehat{f}(xN)$.
- $\widehat{f}$ é injetivo. Se $\widehat{f}(xN) = u$ então, $f(x) = u$, isto é, $x \in N$, ou seja, $xN = N$. Isso mostra que $N(\widehat{f}) = \{N\}$ e portanto $\widehat{f}$ é injetivo. □

Exemplo 12. Dado um inteiro $m > 1$, consideremos $f_m : \mathbb{Z} \to \mathbb{Z}_m$ definido por $f_m(a) = \overline{a}$. Este é um homomorfismo sobrejetor de grupos, pois

$$f_m(a + b) = \overline{a + b} = \overline{a} + \overline{b} = f_m(a) + f_m(b).$$

Dado $y \in \mathbb{Z}_m$, então $y = \overline{a}$, para algum $a \in \{0, 1, 2, \cdots, m - 1\}$, e, portanto, $f_m(a) = \overline{a} = y$, ou seja, f é sobrejetiva. Seu núcleo é o conjunto dos inteiros a tais que $\overline{a} = 0$,

de forma equivalente, é o conjunto dos inteiros a tais que $a \equiv 0 \mod m$. Portanto, $N(f) = m\mathbb{Z} = \{0, \pm m, \pm 2m, \cdots\}$. O Teorema do Homomorfismo nos garante que os grupos $\mathbb{Z}/m\mathbb{Z}$ e $\mathbb{Z}_m$ são isomorfos.

Exemplo 13. Seja G o conjunto das funções $\mathbb{R}$ em $\mathbb{R}$. G é um grupo munido da operação: se $f, g \in G$ define

$$(f+g)(x) = f(x) + g(x), \quad \forall\, x \in \mathbb{R}.$$

Com essa operação, G é um grupo abeliano. O elemento neutro é a função constante 0 e o inverso de f é $-f$ definido por $(-f)(x) = -f(x)$ para todo $x \in \mathbb{R}$. Seja

$$N = \{g \in G : g(1) = 0\}.$$

Mostraremos que N é um subgrupo normal de G e que $G/N \cong \mathbb{R}$ (sendo que $\mathbb{R}$ é visto como grupo aditivo). Para fazer isso, queremos construir um homomorfismo sobrejetivo $\phi : G \to \mathbb{R}$ com a propriedade que $N(\phi) = N$. A definição de N sugere o seguinte: definimos $\phi : G \to \mathbb{R}$ por $\phi(g) = g(1)$. Se trata de um homomorfismo de grupos:

$$\phi(g_1 + g_2) = (g_1 + g_2)(1) = g_1(1) + g_2(1) = \phi(g_1) + \phi(g_2).$$

O núcleo de ϕ é igual a N. Além disso, ϕ é sobrejetiva: se $\alpha \in \mathbb{R}$ então a função constante $g(x) = \alpha$ pertence a G, e $\phi(g) = g(1) = \alpha$. Pelo Teorema de Homomorfismo temos então G/N é isomorfo a $\mathbb{R}$.

Observação 5. *Pela Proposição 22 e o Teorema do homomorfismo. Dado $f : G \to L$ sobrejetora se o núcleo $N(f) = 1_G$ então G será isomorfo a L.*

Capítulo 2

Anéis, corpos e extensão de corpos

O estudo de anéis é necessário para entendermos a necessidade de certas propriedades em operações usuais (como soma e produto de números reais ou polinômios) para encontrar soluções de equações polinomiais e também para o estudo do conjunto de polinômios. Este último é objeto importante no nosso trabalho, bem como o estudo de corpo, uma vez que é nesse conjunto que se encontram as soluções das equações polinomiais.

Definição 17. *Um sistema matemático constituído de um conjunto não vazio A e um par de operações sobre A, respectivamente uma adição $(x, y) \to x + y$ e uma multiplicação $(x, y) \to x \cdot y$ é denominado anel (denotamos por $(A, +, \cdot)$) se as operações satisfazem:*

i) $(A, +)$ *é um grupo abeliano;*

ii) A multiplicação é associativa, ou seja, $\forall\, a, b, c \in A$*;*

$$(ab)c = a(bc);$$

iii) a multiplicação é distributiva em relação a adição, ou seja, $\forall\, a, b, c \in A$*;*

$$a(b + c) = ab + ac \quad \text{e} \quad (a + b)c = ac + bc.$$

Para facilitar a notação representaremos um anel apenas por A.

Abaixo veremos algumas propriedades de anéis.

1. Se o anel possui o elemento neutro da multiplicação, a saber 1, chamamos de anel

com unidade, ou seja, $\exists\, 1 \in A, 0 \neq 1$, tal que;

$$a \cdot 1 = 1 \cdot a = a, \quad \forall\, x \in A.$$

2. Se o anel é comutativo para a multiplicação, chamamos de anel comutativo, ou seja,

$$\forall\, a, b \in A,\ a \cdot b = b \cdot a.$$

3. Diremos que o anel não tem divisores de zero, se satisfaz, $\forall\, a, b \in A,\ a \cdot b = 0 \Rightarrow a = 0$ ou $b = 0$.

4. Se $(A, +, \cdot)$ é um anel comutativo, com unidade e sem divisores de zero, dizemos que $(A, +, \cdot)$ é um anel de integridade.

   Finalmente, se um anel de integridade satisfaz: para todo $a \in A^*$, $\exists\ \ b \in A$, tal que, $a \cdot b = b \cdot a = 1$, dizemos que $(A, +, \cdot)$ é um Corpo.

Exemplo 14. Seguem alguns exemplos para visualizar os conceitos definidos acima:

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são anéis de integridade, consequentemente, anéis. Destes, $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são corpos.

2. $\mathbb{Z}(\sqrt{p}) = \{a + b\sqrt{p}; a, b \in \mathbb{Z}\}$, com p primo, é um anel de integridade.

3. $\mathbb{Z}_p$, com p primo é um corpo.

4. $GL_n(\mathbb{R})$, o conjunto das matrizes invertíveis de ordem n com coeficientes reais apesar de todo elemento possuir inverso multiplicativo não é um anel pois, não é fechado com relação a soma.

2.1 Solução para equações do tipo $a \cdot x + b = c$

Retornando a soluções de equações. Agora, podemos trabalhar com mais de uma operação entre os elementos de um determinado conjunto. Nesse sentido, consideremos a equação:

$$a \cdot x + b \ = \ c \tag{2.1}$$

onde a, b, c pertencem a um conjunto U qualquer. A ideia inicial era de encontrar soluções para a equação do tipo $a * x = b$ e procuramos propriedades na operação do conjunto para garantir a solução da equação. Aqui não será diferente.

Vimos que $a * x = b$ possui solução desde que a operação $*$ nos dê uma estrutura de grupo no conjunto onde se encontram os coeficientes da equação. Então refazemos a mesma pergunta: em quais condições sempre podemos garantir solução da equação (2.1)?

Se consideramos a equação sobre o anel dos inteiros, $(\mathbb{Z}, +, \cdot)$. É de fácil visualização que nem sempre a Equação (2.1) tem solução. Basta tomar $a = 3$, $b = -4$ e $c = 1$;

$$\begin{aligned} 3 \cdot x - 4 &= 1 \\ 3 \cdot x &= 5 \end{aligned}$$

e bem sabemos que não existe nenhum número inteiro que multiplicado por 3 nos dê 5. Mas agora, se consideramos a Equação (2.1) sobre o corpo $(\mathbb{U}, +, \cdot)$ qualquer, temos:

$$a \cdot x + b = c.$$

Somando $-b$ em ambos os membros

$$(a \cdot x + b) + (-b) = c + (-b).$$

Usando a associatividade da adição

$$a \cdot x + (b - b) = c - b.$$

Multiplicando por a^{-1}

$$a^{-1} \cdot (a \cdot x) = a^{-1} \cdot (c - b).$$

Agora, pela associatividade da multiplicação

$$(a^{-1} \cdot a) \cdot x = a^{-1} \cdot (c - b) \quad \Rightarrow \quad x = a^{-1} \cdot (c - b).$$

O que vemos aqui é a necessidade de existência de inversos aditivos e multipli-

cativos dos elementos da equação. Mas vale observar que o termo constante b não necessariamente precisa possuir um inverso multiplicativo, apenas o termo linear a. Podemos então pensar, assim como anteriormente, na Equação (2.1) com coeficientes matriciais.

$$A \cdot X + B = C \tag{2.2}$$

onde A, B e $C \in M_{n\times n}(\mathbb{R})$. Como o conjunto das matrizes é um grupo abeliano com relação a adição de matrizes, podemos considerar apenas o problema

$$A \cdot X = C - B.$$

Sendo assim, este tipo de esquação em um anel pode ser vista como uma equação multiplicativa: se em um anel A tivermos que $(A - \{0\}, \cdot)$ for um grupo multiplicativo se, e somente se, a equação tem solução.

2.2 Equação do segundo grau

Assim como na equação anterior, aqui a estrutura de grupo não é sempre suficiente para garantir a solução das equações do segundo grau devido a necessidade de duas operações bem definidas no conjunto. Se os coeficientes da equação pertencem a um anel U, teremos equações onde não está bem definido o conceito de solução, por exemplo $f(x) = x^2 - 1$, para determinar as soluções, ou raízes, do polinômio f temos:

$$x^2 - 1 = 0 \Leftrightarrow (x-1)(x+1) = 0,$$

claramente vemos que ± 1 são raízes em um anel de integridade, como por exemplo o anel dos inteiros. Nestes, quando temos um produto igual a zero, um dos fatores deve ser zero. Mas se os coeficientes do polinômio estiverem, por exemplo, em $\mathbb{Z}_8$ teremos outras soluções pois:

$$\begin{aligned} f(x) &= (x-\overline{1})(x+\overline{1}) \\ f(\overline{3}) &= (\overline{3}-\overline{1})(\overline{3}+\overline{1}) \\ &= \overline{2}\cdot\overline{4} = \overline{0}. \end{aligned}$$

Observe que $f(\overline{1}) = f(\overline{3}) = f(\overline{5}) = f(\overline{7}) = 0$. Com isso, as raízes de um polinômio não satisfazem o Teorema Fundamental da Álgebra quando procuramos em conjuntos que possuem divisores de zero. Sendo assim, sempre iremos procurar as soluções de equações polinomiais em corpos.

Determinar as raízes de um polinômio é um problema antigo e que só começou a ser resolvido a partir de 1700, com Euler, Goldbach, Bernoulli e outros. Em 1742, Euler, sem provar, disse que todo polinômio real poderia ser decomposto em fatores lineares ou quadráticos com coeficientes reais. Anos depois Euler e Jean Le Rond d'Alembert deram provas completas para essa afirmação. Lagrange clamou pelo preenchimento dos buracos na prova de Euler, mas cometeu o erro de assumir que as raízes existiam. A primeira prova genuína foi dada por Gauss na sua tese de doutorado em 1799. Gerando o famoso teorema:

Teorema 24 (Teorema Fundamental da Álgebra)**.** *Seja $p(x)$ um polinômio sobre $\mathbb{C}$, com $\partial p \geq 1$. Então existe pelo menos um $z \in \mathbb{C}$ tal que $p(z) = 0$.*

Este teorema possui aplicações em diferentes áreas da matemática e inúmeras demonstrações sendo algumas analíticas, topológicas ou algébricas. Gauss, logo após apresentar a prova total do teorema ainda fez outras três diferentes.

2.2.1 Radiciação

A radiciação é uma operação matemática inversa à potenciação, assim como a divisão é o inverso da multiplicação.

Para um número real a, a expressão $\sqrt[n]{a}$ representa o único número real x que satisfaz $x^n = a$. Quando n é omisso, significa que $n = 2$ e o símbolo de radicais refere-se à raiz quadrada. Neste caso, x é raiz da equação, n o índice, a o radicando e $\sqrt{\ }$ o radical.

Um erro comum é achar que a raiz par de um número, em especial a raiz quadrada, tem duas soluções, uma positiva e outra negativa, por exemplo, $\sqrt{4} = \pm 2$. Isso advém do fato que os estudantes quando aprendem a resolver equações quadráticas como $x^2 = 25$, acham ser equivalente a encontrar a raiz, mas não é. De fato, existem dois valores ± 5 que satisfazem $x^2 = 25$. No entanto, existe apenas uma resposta para $\sqrt{25}$ que é 5. Se trata de uma definição que a raiz de índice par de um número positivo será o número positivo.

Definição 18. *Se x é um número real, o módulo de x (ou valor absoluto de x) é o número*

$|x|$ *definido por*

$$\begin{cases} |x| = x, & se \quad x \geq 0 \\ |x| = -x, & se \quad x < 0. \end{cases}$$

Proposição 25. *Para qualquer $x \in \mathbb{R}$, temos que $|x| = \sqrt{x^2}$.*

Demonstração. Inicialmente vamos mostrar que:

$$|x|^2 = |x^2| = x^2, \quad \forall\, x \in \mathbb{R}.$$

Sendo $x^2 \geq 0$, $\forall\, x \in \mathbb{R}$, temos que:

$$|x^2| = x^2,$$

pela definição de módulo. Resta mostrar que:

$$|x|^2 = x^2.$$

Se $x \geq 0$, temos $|x| = x$ e, portanto,

$$|x|^2 = (x)^2 = x^2,$$

se $x < 0$,

$$|x| = -x$$

e,

$$|x|^2 = (-x)^2 = x^2.$$

Agora vamos mostrar que $|x| = \sqrt{x^2}$. Seja $\sqrt{x^2}$ a raiz quadrada de x^2, isto é, o número não negativo cujo quadrado é x^2. O número $|x|$ satisfaz tais condições, ou seja,

$$|x| \geq 0 \;\text{ e }\; |x|^2 = x^2.$$

Logo,

$$\sqrt{x^2} = \sqrt{|x|^2} = |x|.$$

□

Faremos agora alguns exemplos para mostrar a necessidade de introduzir certas

propriedades nas operações em anéis de integridade.

Exemplo 15.

1. Considere a equação $x^2 - 1 = 0$, onde seus coeficientes encontram-se no corpo $\mathbb{Q}$. Para desenvolver esse tipo de equação se faz necessário trabalharmos com anéis de integridade ou corpos, devido a utilização das operações: soma e produto. Resolvendo a equação, temos:

$$\begin{aligned} x^2 - 1 &= 0 \\ (x^2 - 1) + 1 &= 1 \ \text{(Somando o simétrico aditivo de -1);} \\ x^2 &= 1; \\ \sqrt{x^2} &= \sqrt{1} \ \text{(Extraindo a raiz quadrada em ambos os membros);} \\ |x| &= 1 \ \text{(Proposição 25).} \end{aligned}$$

   Portanto, pela definição de módulo $x = \pm 1$. Logo, os zeros da equação são $x = 1$ ou $x = -1$.

2. Vamos encontrar os zeros da equação $ix^2 - 2i = 0$, em que seus coeficientes estão em $\mathbb{C}$ e $i^2 = -1$.

$$\begin{aligned} ix^2 - 2i &= 0 \\ (ix^2 - 2i) + 2i &= 2i \ \text{(Simétrico aditivo);} \\ ix^2 + (-2i + 2i) &= 2i \ \text{(Associatividade);} \\ ix^2 &= 2i \ \text{(Multiplicando por } -i\text{);} \\ x &= \pm\sqrt{2} \in \mathbb{R}. \end{aligned}$$

Definição 19. *Uma equação polinomial quadrática ou de grau 2 é toda equação da forma*

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

onde a, b *e* $c \in \mathbb{C}$*, com* $a \neq 0$.

Aqui os coeficientes já estão em um corpo, sendo assim as operações são amplamente conhecidas. Vamos determinar a solução para uma equação do segundo grau

conhecida como a fórmula de Bhaskara. Demonstraremos a fórmula pelo método de completar quadrados (Peruzzo, 2013). Para isso, inicialmente podemos dividir a equação por a, reescrevendo

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

Isolando o termo independente $\frac{c}{a}$ e completando o quadrado de forma conveniente, temos:

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

Daí,

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

reescrevendo o primeiro termo

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

Extraindo a raiz quadrada dos dois lados da igualdade e usando a Proposição 25,

$$\begin{aligned} \sqrt{\left(x + \frac{b}{2a}\right)^2} &= \sqrt{\frac{b^2 - 4ac}{4a^2}} \\ \left|x + \frac{b}{2a}\right| = \sqrt{\frac{b^2 - 4ac}{4a^2}} &\Leftrightarrow x + \frac{b}{2a} = \pm\frac{\sqrt{b^2 - 4ac}}{2a}. \end{aligned}$$

Subtraindo $-\frac{b}{2a}$ em ambos os lados da igualdade

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

Fazendo $\Delta = b^2 - 4ac$, observe que, se $a, b, c \in \mathbb{R}$, então:

- Se $\Delta < 0$, então a equação não possui raíz reais.
- Se $\Delta = 0$, a equação possui apenas uma raíz real.
- Se $\Delta > 0$, a equação possui duas raízes reais.

Se consideramos a equação do segundo grau sobre os números Racionais temos

que nem todas as raízes serão números racionais, nem mesmo reais. Por exemplo:

$$x^2 + 1 = 0 \quad \Leftrightarrow \quad x = \pm i.$$

A teoria de Galois que veremos no trabalho tem início na obtenção do menor corpo onde o polinômio possui todas as raízes, isso nos fornecerá informações importantes sobre a forma de determinar as raízes de um polinômio de grau maior ou igual a cinco.

2.3 Anel de polinômios

Seja $\mathbb{K}$ um corpo. Chamamos de anel de polinômios sobre $\mathbb{K}$ na indeterminada x, e representamos por $\mathbb{K}[x]$, o conjunto de todos os polinômios com coeficientes em $\mathbb{K}$ na indeterminada x.

Definição 20. *Sejam $a_1, a_2, \cdots, a_n \in \mathbb{K}$, $n \in \mathbb{N}$, onde $\mathbb{K}$ é um corpo. Chamamos de polinômio sobre $\mathbb{K}$ em uma indeterminada x a expressão:*

$$p(x) = \sum_{i=0}^{n} a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

Considere os polinômios: $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ e $q(x) = b_m x^m + b_{b-1} x^{m-1} + \cdots + b_1 x + b_0$. Eles são ditos iguais, se $m = n$ e seus coeficientes são iguais, ou seja, $a_i = b_i$; $\forall\, i = 1, \ldots, n$. Se todos os coeficientes de um polinômio forem iguais a 0, chamamos de polinômio nulo ou identicamente nulo.

Se $a \in \mathbb{K}$, o polinômio $p(x)$ definido por $p(x) = a$, é chamado de polinômio constante determinado por a. Dessa forma, qualquer elemento $a \in \mathbb{K}$ pode ser expresso como um polinômio constante. E com isso, $\mathbb{K} \subset \mathbb{K}[x]$.

Definição 21. *Seja $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$. Se $a_n \neq 0$, dizemos que o grau do polinômio $p(x)$ é n, e denotamos por $\partial p(x) = n$, ou seja, o grau de um polinômio é dado pela maior potência de sua indeterminada. E o grau será zero se o polinômio for constante. Dizemos que um polinômio $g(x)$ é mônico, se o coeficiente do termo de maior grau de $g(x)$ é igual a 1.*

É importante destacar, ainda, que a soma e produtos de polinômios estão bem definidas:

Sejam p e q dois polinômios pertencentes a $\mathbb{K}[x]$, temos que:

i) para adição:

$$p(x) + q(x) = c_k x^k + c_{k-1} x^{k-1} + \cdots + c_1 x + c_0,$$

onde $c_i = (a_i + b_i) \in \mathbb{K}$, com $k \in \mathbb{N}$ e com

$$\partial(p(x) + q(x)) \leq \max\{\partial p(x), \partial q(x)\} = \max(m, n).$$

ii) Para multiplicação:

$$p(x) \cdot q(x) = c_j x^j + c_{j-1} j x^{j-1} + \cdots + c_1 x + c_0,$$

onde $c_0 = a_0 b_0$, $c_1 = a_0 b_1 + a_1 b_0$, $c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0, \cdots, cj = a_0 b_j + a_1 b_{j-1} + \cdots + a_{j-1} b_1 + a_j b_0$, $j \in \mathbb{N}$ e grau

$$\partial(p(x) \cdot q(x)) = \partial p(x) + \partial q(x) = n + m.$$

É de facíl verificação que $\mathbb{K}[x]$ é um anel com a soma e o produto de polinômios definidos acima. Por ser um anel, temos todas as propriedades da sessão anterior satisfeitas, além disso, $\mathbb{K}[x]$ é um anel de integridade. Mas não é um corpo por não ter todos seus elementos invertíveis. Observe que os únicos polinômios invertíveis de $\mathbb{K}[x]$ são os polinômios constantes não nulos. Por exemplo o polinômio $f(x) = x^2$ não possui inverso já que $f^{-1}(x) = \dfrac{1}{x^2}$ não está definido no zero.

Definição 22. *Sejam $p(x), q(x) \in \mathbb{K}[x]$. Dizemos que $p(x)$ divide $q(x)$ se existe $h(x) \in \mathbb{K}[x]$ tal que,*

$$q(x) = p(x) \cdot h(x).$$

Denotamos por $p(x)|q(x)$. Dizemos também que $p(x)$ é divisor de $q(x)$ ou que $q(x)$ é divisível por $p(x)$. Caso contrário, teremos $p(x) \nmid q(x)$.

Exemplo 16. Em $\mathbb{Z}[x]$, o polinômio $p(x) = x+4$ divide o polinômio $q(x) = 2x^2+2x-24$.

De fato. Temos pela definição que as raízes de um polinômio (zeros de um polinômio) $q(x)$ sobre $\mathbb{K}$ é dado por um elemento $r \in \mathbb{K}$ tal que $q(r) = 0$, onde o

número de raízes é determinado pelo grau de $q(x)$. Dessa forma, no exemplo acima $q(x) = p(x) \cdot h(x) = a(x - r_1)(x - r_2)$, onde r_1 e r_2 são raízes do polinômio e $a \neq 0$.

Logo, as raízes de $q(x)$ são $r_1 = -4$, $r_2 = 3$ e $a = 2$. Concluímos que $p(x)|q(x)$, pois $q(x) = 2(x + 4)(x - 3)$ e são únicas pelo Teorema Fundamental da Álgebra.

Porém nem sempre podemos conseguir uma divisão exata dos polinômios. Veremos então, que sob certas condições, é possível conseguir uma "divisão aproximada"de um polinômio por outro, assim como acontece no anel $\mathbb{Z}$.

Teorema 26 (Algoritmo Euclidiano)**.** *Sejam $\mathbb{K}$ um corpo e $f(x)$ e $g(x)$ polinômios em $\mathbb{K}[x]$. Suponhamos que $f(x)$ é não nulo. Então existem únicos polinômios $q(x)$ e $r(x)$ em $\mathbb{K}[x]$, tal que $g(x) = f(x)q(x) + r(x)$ e $r(x)$ tem grau estritamente menor do que $f(x)$.*

A demonstração pode ser encontrada em Biazzi (2014).

Exemplo 17. Vamos determinar o quociente e o resto da divisão de $p(x) = 12x^3 - 4x + 9$ por $q(x) = 2x^2 + x + 3$, ambos em $\mathbb{Z}[x]$.

$$\begin{array}{r|l} 12x^3 - 4x + 9 & 2x^2 + x + 3 \\ \cline{2-2} -12x^3 - 6x^2 - 18x & 6x - 3 \\ \cline{1-1} -6x^2 - 22x + 9 & \\ 6x^2 + 3x + 9 & \\ \cline{1-1} -19x + 18 & \end{array}$$

Com isso,

$$12x^3 - 4x + 9 = (2x^2 + x + 3)(6x - 3) - 19x + 18$$

Definição 23. *Seja $p(x)$ um polinômio sobre $\mathbb{K}$ e r um elemento de $\mathbb{K}$. Se existe um número natural n positivo tal que:*

$$p(x) = (x - r)^n q(x),$$

em que $q(x)$ é um polinômio com coeficientes em $\mathbb{K}$ e r não é raiz de $q(x)$, então dizemos que r é uma raiz de multiplicidade n de $p(x)$. Se a raiz tem multiplicidade 1, é chamada de raíz simples.

2.3.1 Irredutibilidade de polinômios

Definição 24. *Um polinômio sobre $\mathbb{K} = \mathbb{R}, \mathbb{Q}$ ou $\mathbb{Z}$ é redutível se é o produto de dois polinômios sobre $\mathbb{R}$ de graus menores. Caso contrário, dizemos que é irredutível.*

Exemplo 18.

1. Todos os polinômios de graus 0 e 1 são irredutíveis, pois não podem ser expressos como um produto de polinômios de graus menores.

2. No Exemplo 16, temos que $q(x) = 2x^2 + 2x - 24$ é redutível sobre $\mathbb{Z}$, já que $q(x) = 2(x+4)(x-3)$.

3. O polinômio $q(x) = x^2 - 2$ é irredutível sobre $\mathbb{Q}$. Pois, caso não fosse, teríamos

$$x^2 - 2 = (ax + b)(cx + d),$$

com $a, b, c, d \in \mathbb{Q}$. Dividindo se necessário, podemos assumir $a = c = 1$. Então,

$$\begin{aligned} x^2 - 2 &= (ax + b)(cx + d) \\ &= x^2 + dx + bx + bd \\ &= x^2 + (b + d)x + bd. \end{aligned}$$

Segue pela definição de igualdade de polinômios que:

$$\begin{cases} b + d &= 0 \\ bd &= -2. \end{cases}$$

Isolando d na primeira equação, conseguimos $d = -b$. Substituindo na segunda equação, ficamos com $b^2 = 2$. Mas, não há número racional tal que sua raiz quadrada seja 2.

Observe que o polinômio pode ser irredutível sobre um subcorpo dos complexos, porém, redutível, se considerarmos um subcorpo maior. Por exemplo, o polinômio $x^2+1 \in \mathbb{Q}[x]$ é irredutível sobre $\mathbb{Q}$ mas é redutível sobre o subcorpo $\mathbb{Q}(i) = \{a + bi; a, b \in \mathbb{Q}\}$ de $\mathbb{C}$. Veremos com mais detalhes no decorrer do trabalho.

Teorema 27. *Qualquer polinômio $f(x)$ pode ser escrito de uma única maneira como produto de polinômios irredutíveis em $\mathbb{K}[x]$, a menos de ordem dos fatores e constantes.*

Demonstração. Seja $f(x) \in \mathbb{K}[x]$ um polinômio de grau n maior ou igual a 1, vamos provar por indução sobre $\partial(f(x))$.

O caso $\partial(f(x)) = 1$, já está fatorado como produto de irredutíveis. Além disso, a unicidade segue da identidade de polinômios.

Se $\partial(f(x)) = n > 1$, podemos escrever $f(x) = f_1(x)f_2(x)$, onde $f_1(x)$ e $f_2(x)$ possuem grau menor que n. Se $f_1(x)$ e $f_2(x)$ forem irredutíveis, a fatoração está concluída. Caso contrário, devemos repetir o processo até obtermos uma fatoração de $f(x)$ como produto de irredutíveis. Suponha que $f(x)$ seja o produto de m polinômios irredutíveis, assim vamos mostrar a unicidade da fatoração. Suponhamos que

$$f(x) = f_1(x)f_2(x)\cdots f_m(x) = g_1(x)g_2(x)\cdots g_k(x)$$

sejam duas possíveis fatorações de $f(x)$ como produto de polinômios irredutíveis, onde $m \leq k$. Então, $f_1(x) \,|\, g_1(x)g_2(x)\cdots g_k(x)$ onde, $f_1(x)|g_j(x)$ para alguma $j \in 1, \cdots, k$. Podemos assumir, sem perda de generalidade, que $j = 1$, então $f_1(x) \,|\, g_1(x)$. No entanto, $g_1(x)$ é irredutível, assim $g_1(x) = \alpha_1 f_1(x)$, com $\alpha_1 \in \mathbb{K}$. Substituindo $g_1(x)$ na equação destacada anteriormente e cancelando, ficamos com

$$f_1(x)f_2(x)\cdots f_m(x) = \alpha_1 f_1(x)g_2(x)\cdots g_k(x)$$

$$f_2(x)\cdots f_m(x) = \alpha_1 g_2(x)\cdots g_k(x).$$

Repetindo o argumento, obtemos

$$1 = \alpha_1 \cdots \alpha_m g_{m+1}(x)\cdots g_k(x),$$

o que só é possível se $m = n$. Portanto, concluímos que os fatores irredutíveis $f_i(x)$ e $g_i(x)$ são os mesmos. □

Em geral, a verificação da irredutibilidade de um polinômio sobre um corpo nem sempre é uma tarefa fácil. Sendo assim, mostraremos dois mecanismos que nos ajudam a fazer tal verificação, sendo eles: Critério de Eisenstein e Redução Módulo p, com p primo. Mas antes, enunciaremos o Lema de Gauss, que nos diz que irredutibilidade sobre $\mathbb{Z}$ implica a irredutibilidade sobre $\mathbb{Q}$.

Teorema 28 (Lema de Gauss)**.** *Seja f um polinômio sobre $\mathbb{Z}$ que é irredutível sobre $\mathbb{Z}$. Então f, considerado como um polinômio sobre $\mathbb{Q}$, é também irredutível sobre $\mathbb{Q}$.*

A demonstração pode ser encontrada em Gonçalves (2006).

Teorema 29 (Critério de Eisenstein)**.** *Seja* $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ *um polinômio sobre* $\mathbb{Z}$*. Suponha que exista um primo* p *tal que,*

i) $p \nmid a_n$*;*

ii) $p|a_i\,(i = 0, 1, \cdots, n-1)$*;*

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

Então f *é irredutível sobre* $\mathbb{Q}$*.*

Demonstração. Pelo Lema de Gauss, é suficiente mostrar que f é irredutível sobre $\mathbb{Z}$. Suponhamos por contradição que $f = gh$, em que,

$$g(x) = b_0 + b_1x + \cdots + b_rx^r \qquad \text{e} \qquad h(x) = c_0 + c_1x + \cdots c_sx^s$$

são polinômios de graus menores do que o grau de f sobre $\mathbb{Z}$. Então, $r \geq 1, s \geq 1, r+s = n$. Agora, $b_0c_0 = a_0$ e, pelo $item(ii)$, $p|a_0$. Como p é primo, $p|b_0$ ou $p|c_0$. Já pelo $item(iii)$, temos que p não pode dividir ambos b_0 e c_0, assim, sem perda de generalidade, podemos assumir que $p|b_0$ e $p \nmid c_0$. Se todos os b_j forem divisíveis por p, então a_n é divisível por p, o que contraria o $item(i)$. Consideremos b_j o primeiro coeficiente de g que não é divisível por p. Então

$$a_j = b_jc_0 + \cdots + b_0c_j,$$

com $j < n$. Deste modo, concluímos que $p|c_0$, pois p divide $a_j, b_0, \cdots b_{j-1}$, mas não b_j . O que é uma contradição. Portanto, f é irredutível. □

Exemplo 19. *O polinômio* $f(x) = 5x^{17} + 6x^{13} + 15x^4 + 3x^2 + 9x + 12$ *é irredutível sobre* $\mathbb{Q}$*. De fato, aplicando o critério de Eisenstein para* $p = 3$ *temos que* $p \nmid 5$*,* $p \mid 12, 9, 3, 15, 6$ *e* $p^2 = 9 \nmid 12$*, que mostra que* $f(x)$ *irredutível sobre* $\mathbb{Q}$*.*

Exemplo 20. Agora, para o polinômio $g(x) = x^4 + x^3 - 7x^2 - x + 6$ não é possível encontrar um número primo p que satisfaça o Teorema de Eisenstein. Mas de fato, $g(x)$ é redutível sobre $\mathbb{Q}$. Basta observar que $g(-1) = 0$.

Para simplificar a notação, dado um polinômio $f(x) \in \mathbb{Z}[x]$, com $f(x) = a_n x^n + \cdots + a_0$, usaremos $\overline{f}(x)$ para denotar o polinômio com coeficientes em $\mathbb{Z}_p$, para algum $p \in \mathbb{N}$.

Proposição 30. *(Redução Módulo p). Sejam $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ e um número primo p, tal que $p \nmid a_n$. Caso $\overline{f}(x)$ seja irredutível sobre $\mathbb{Z}_p$, temos que $f(x)$ é irredutível sobre $\mathbb{Q}$.*

A demonstração pode ser encontrada em Biazzi (2014).

Exemplo 21. Vamos verificar que $f(x) = x^4 + 10x^3 + 15x^2 + 5x + 12 \in \mathbb{Z}[x]$ é irredutível sobre $\mathbb{Q}$.

Considere $p = 5$ e $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ então $\overline{f}(x) = x^4 + \overline{2} \in \mathbb{Z}_5[x]$. Observe que $5 \nmid 1$ e pela proposição acima é suficiente provarmos que $\overline{f}(x) = x^4 + \overline{2}$ é irredutível sobre $\mathbb{Z}_5$. Se este for redutível sobre $\mathbb{Z}_5$, então este tem um fator de grau 1, ou é produto de dois fatores de grau 2. Mas observe que $\overline{f}(x)$ não possui raízes em $\mathbb{Z}_5$. Assim a única forma possível de fatorarmos $\overline{f}(x)$ seria a seguinte:

$$x^4 + \overline{2} = (ax^2 + bx + c)(a'x^2 + b'x + c'),$$

onde $a, b, c, a', b', c' \in \mathbb{Z}_5$. Podemos considerar $a = a' = 1$, caso não sejam, basta dividir o polinômio por seus respectivos inversos.

$$x^4 + \overline{2} = (x^2 + bx + c)(x^2 + b'x + c').$$

Desenvolvendo o produto e igualando os polinômios obtemos: $b + b' = 0$, $bb' + c + c' = 0$, $cc' = 2$. Assim, $c + c' = b^2$ que pode apenas assumir os valores, $\overline{0}, \overline{1}, \overline{4}$, que são os quadrados perfeitos em $\mathbb{Z}_5$. Logo,

i) para $b^2 = 0$ temos: $c + c' = \overline{0} \Rightarrow c(-c) = 2 \Rightarrow -c^2 = \overline{2}$;

ii) para $b^2 = 1$ temos: $c + c' = \overline{1} \Rightarrow c' = 1 - c \Rightarrow c(1 - c) = \overline{2}$;

iii) para $b^2 = 4$ temos: $c + c' = \overline{4} \Rightarrow c' = 4 - c \Rightarrow c(4 - c) = \overline{2}$.

Note que testando todas as possibilidades para c, nenhuma satisfaz estas equações. Daí, temos que $x^4 + \overline{2}$ é irredutível sobre $\mathbb{Z}_5$ e, por consequência, $f(x)$ é irredutível sobre $\mathbb{Q}$.

2.3.2 Extensão de corpos

O polinômio $x^2 + 1 \in \mathbb{Q}[x]$ é irredutível sobre $\mathbb{Q}$. Deste modo como podemos adicionar elementos a $\mathbb{Q}$ para que o polinômio passe a ter raízes nesse novo conjunto. Como veremos, essa adjunção deve ser feita de modo a preservar as propriedades e axiomas que definem um corpo. Chamaremos tal adjunção de "extensão de corpos". Como foi visto, ao adicionarmos todas as combinações lineares de 1 e de i sobre $\mathbb{Q}(i) = \{a + bi; a, b \in \mathbb{Q}\}$ é gerado um novo corpo onde o polinômio $x^2 + 1$ é redutível. Neste tópico iremos abordar a parte da teoria de corpos que engloba extensões e raízes de polinômios.

Definição 25. *Uma Extensão de um corpo $\mathbb{K} \subset \mathbb{C}$ é um monomorfismo $\iota : \mathbb{K} \to \mathbb{L}$, em que $\mathbb{L}$ é um subcorpo dos complexos. Diremos que $\mathbb{K}$ é o corpo menor e $\mathbb{L}$ é o corpo maior.*

Definição 26. *Seja X um subconjunto de $\mathbb{C}$. Então o subcorpo de $\mathbb{C}$ gerado por X é a interseção de todos os subcorpos de $\mathbb{C}$ que contém X. Equivalentemente, este é o subcorpo $\mathbb{K}(X)$ que satisfaz alguma das seguintes condições,*

i) O único menor subcorpo de $\mathbb{C}$ que contém X;

ii) O conjunto de todos os elementos de $\mathbb{C}$ que podem ser obtidos a partir de elementos de X por uma sequência de finitas operações.

Usaremos a notação $\mathbb{L} : \mathbb{K}$ para representar que $\mathbb{L}$ é uma extensão de $\mathbb{K}$. Como $\mathbb{K} \subset \mathbb{L}$, então $\mathbb{L}$ é um espaço vetorial sobre $\mathbb{K}$, uma vez que as relações de definição de um corpo são justamente as relações de definição de um espaço vetorial se o escalar está em $\mathbb{L}$.

Definição 27. *O grau, $[\mathbb{L} : \mathbb{K}]$, de uma extensão $\mathbb{L} : \mathbb{K}$ é a dimensão do espaço vetorial de $\mathbb{L}$ sobre $\mathbb{K}$.*

Por definição, uma extensão $\mathbb{L} : \mathbb{K}$ é dita finita se seu grau é finito, caso contrário é chamada extensão infinita. Nestre trabalho focaremos nas extensões finitas.

Exemplos

1. A função inclusão $\iota : \mathbb{R} \to \mathbb{C}$ é uma extensão de corpo onde $[\mathbb{C} : \mathbb{R}] = 2$. De fato, basta notar que

$$\mathbb{C} = \{a + bi; a, b \in \mathbb{R} \ \ e \ \ i^2 = -1\}$$

2. Seja $\mathbb{Q}(\sqrt{2}) = \{p + q\sqrt{2};\, p, q \in \mathbb{Q}\}$. Então $\mathbb{Q}(\sqrt{2})$ é um corpo e uma extensão de $\mathbb{Q}$, onde $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Para verificar que $\mathbb{Q}(\sqrt{2})$ é um corpo, é suficiente mostrar que todo elemento $0 \neq \alpha = p+q\sqrt{2}$ possui simétrico multiplicativo, pois a soma e o produto são as operações usuais e com isso seu simétrico aditivo é $-\alpha$.

Considere $\beta = p - q\sqrt{2}$, então

$$\alpha\beta = (p + q\sqrt{2})(p - q\sqrt{2}) = p^2 - 2q^2 = \omega \in \mathbb{Q}.$$

Com $w \neq 0$ pois $\mathbb{Q}(\sqrt{2})$ é anel de integridade. Logo, $\dfrac{\beta}{\omega} \in \mathbb{Q}(\sqrt{2})$. E então,

$$\alpha \cdot \frac{\beta}{\omega} = 1$$

3. Considere o polinômio $f(x) = x^4 - 2x^2 - 3 \in \mathbb{Q}[x]$. Fatorando $f(x)$ como produto de irredutíveis sobre $\mathbb{Q}$ temos,

$$f(x) = (x^2 + 1)(x^2 - 3),$$

note que $f(x)$ é irredutível (fatores lineares) sobre $\mathbb{Q}$, pois suas raízes são: $\pm i$ e $\pm\sqrt{3}$. Porém é redutível sobre $\mathbb{Q}(i, -i, \sqrt{3}, -\sqrt{3})$. É de fácil verificação que $\mathbb{Q}(i, -i, \sqrt{3}, -\sqrt{3}) = \mathbb{Q}(i, \sqrt{3})$, uma vez que estes conjuntos são também espaços vetoriais. Observe que se $\alpha\mathbb{Q}(i, -i, \sqrt{3}, -\sqrt{3})$ então existem $p, q, r, s, t \in \mathbb{Q}$ tais que:

$$\begin{aligned} \alpha &= p + qi - ri + s\sqrt{3} - t\sqrt{3} \\ &= p + (q - r)i + (s - t)\sqrt{3} \in \mathbb{Q}(i, \sqrt{3}). \end{aligned}$$

Agora, vamos considerar $\mathbb{K} = \mathbb{Q}$ e $X = \{i, \sqrt{3}\}$. Então $\mathbb{K}(X)$ deve conter $\mathbb{K}$ e X. Este também deve conter o produto $i\sqrt{3}$. O subcorpo $\mathbb{K}(X)$ deve conter todo elemento da forma:

$$\alpha = p + qi + r\sqrt{3} + si\sqrt{3};\ com\ \ p, q, r, s \in \mathbb{Q}.$$

Seja $L \subseteq \mathbb{C}$ o conjunto de todos os números α como acima. Se conseguirmos provar que L é um subcorpo de $\mathbb{C}$, sabendo que $\mathbb{K}(X) \subseteq L$, por definição, e $\mathbb{K}(X)$ ser o menor subcorpo de $\mathbb{C}$ com esta propriedade, segue que $\mathbb{K}(X) = L$. Para L ser um subcorpo de $\mathbb{C}$ resta provarmos que qualquer que seja $\alpha \neq 0$, encontramos o seu inverso

α^{-1} pertencente a L, uma vez que temos de forma nítida o fechamento de L com respeito as operações de soma e multiplicação. De fato, temos que provar que para (p, q, r, s), nem todos nulos, teremos

$$(p + qi + r\sqrt{3} + si\sqrt{3})^{-1} \in L.$$

Primeiro, suponhamos que $p + qi + r\sqrt{3} + si\sqrt{3} = 0$. Então,

$$p + r\sqrt{3} = -i(q + s\sqrt{3}).$$

Notemos que o lado esquerdo, $p + r\sqrt{3}$, é um número real, enquanto que o lado direito, $-i(q + s\sqrt{3})$, é um número complexo. Portanto, $p + r\sqrt{3} = 0$ e $q + s\sqrt{3} = 0$. Se $r \neq 0$, então $\sqrt{3} = \dfrac{-p}{r} \in \mathbb{Q}$, mas $\sqrt{3}$ é irracional. Logo, devemos ter $r = 0$, donde $p = 0$. De modo análogo, $q = s = 0$.

Provaremos agora a existência de α^{-1}. Seja M um subconjunto de L contendo todos $p + qi\,(p, q \in \mathbb{Q})$. Então escrevemos,

$$\alpha = x + y\sqrt{3},$$

com $x = p + iq$ e $y = r + is \in M$. Seja

$$\beta = p + qi - r\sqrt{3} - si\sqrt{3} = x - y\sqrt{3} \in L.$$

Então,

$$\alpha\beta = (x + y\sqrt{3})(x - y\sqrt{3}) = x^2 - 3y^2 = z$$

onde $z \in M$. Como $\alpha \neq 0$ e $\beta \neq 0$, temos que $z \neq 0$ e, portanto, $\alpha^{-1} = \beta z^{-1}$. Com isso, concluímos que $\alpha^{-1} = \beta z^{-1} \in L$.

Pela propriedade de espaço vetorial, temos $[\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}] = 4$. Porém nem sempre conseguimos determinar o grau de um extensão com tanta facilidade, dessa forma, segue abaixo o teorema que auxilia nesse cálculo pois nos permite usar outras extensões com graus conhecidos.

Sejam $\mathbb{K} \subset \mathbb{C}$ é um corpo e $X = \{k_1, k_2, \cdots, k_n\}$ um conjunto finito de elementos de $\mathbb{C}$. Denotaremos por $\mathbb{K}(X)$ o conjunto de todas as combinações lineares de $\mathbb{K}$ com

elementos de X. Se $\alpha \in \mathbb{K}(X)$, então

$$\alpha = p_0 + p_1k_1 + \cdots + p_nk_n,$$

onde, $p_0, p_1, \cdots, p_n \in \mathbb{K}$.

Teorema 31 (Lei da Torre)**.** *Se* $\mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \cdots \subseteq \mathbb{K}_n$ *são subcorpos de* $\mathbb{C}$*, então*

$$[\mathbb{K}_n : \mathbb{K}_0] = [\mathbb{K}_n : \mathbb{K}_{n-1}][\mathbb{K}_{n-1} : \mathbb{K}_{n-2}] \cdots [\mathbb{K}_1 : \mathbb{K}_0].$$

A demonstração pode ser encontrada em Cruz (2014).

Exemplo 22. Vamos determinar $[\mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{13}) : \mathbb{Q}]$.

Aplicando a Lei da Torre, onde $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\sqrt{5}, \sqrt{7}) \subseteq \mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{13})$, temos

$$[\mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{13}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{13}) : \mathbb{Q}(\sqrt{5}, \sqrt{7})][\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}].$$

Note que,

i) $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$;

ii) $[\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{5})] = 2$. De fato, seja $\alpha \in \mathbb{Q}(\sqrt{5}, \sqrt{7})$ então $\alpha = p + q\sqrt{7}$ com $p, q \in \mathbb{Q}(\sqrt{5})$. Agora, $[\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}] = 4$, pois, dado $\alpha' \in \mathbb{Q}(\sqrt{5}, \sqrt{7})$

$$\begin{aligned} \alpha' &= p + q\sqrt{7} \text{ com } p, q \in \mathbb{Q}(\sqrt{5}) \\ &= p_1 + q_1\sqrt{5} + (p_2 + q_2\sqrt{5})\sqrt{7} \\ &= p_1 + q_1\sqrt{5} + p_2\sqrt{7} + q_2\sqrt{35} \end{aligned}$$

com $p = p_1 + q_1\sqrt{5}$, $q = p_2 + q_2\sqrt{5}$ e $p_1, p_2, q_1, q_2 \in \mathbb{Q}$. Pelo teorema da torre verificamos

$$4 = [\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{5})] \cdot [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

ii) De modo análogo ao item anterior obtemos que

$[\mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{13}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{13}) : \mathbb{Q}(\sqrt{5}, \sqrt{7})] \cdot [\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{5})] \cdot [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 8$.

Observação 6. *Vimos que para algumas extensões é suficiente anexar apenas um número ao corpo, que chamamos de extensão simples. Por exemplo,* $\mathbb{Q}(\sqrt{2})$ *e* $\mathbb{R}(i)$.

Definição 28. *Considere* $\widehat{\mathbb{K}}$ *e* $\widehat{\mathbb{L}}$ *extenções dos corpos de* $\mathbb{K}$ *e* $\mathbb{L}$*, respectivamente. Um isomorfismo entre duas extensões de corpos* $\iota : \mathbb{K} \to \widehat{\mathbb{K}}$ *e* $\jmath : \mathbb{L} \to \widehat{\mathbb{L}}$ *é um par* (λ, μ) *de isomorfismos* $\lambda : \mathbb{K} \to \mathbb{L}$*,* $\mu : \widehat{\mathbb{K}} \to \widehat{\mathbb{L}}$*, tal que para todo* $k \in \mathbb{K}$*,*

$$\jmath(\lambda(k)) = \mu(\iota(k)).$$

Para melhor visualização, pode-se considerar o seguinte diagrama comutativo:

$$\begin{array}{ccc} \mathbb{K} & \xrightarrow{i} & \widehat{\mathbb{K}} \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\mu} \\ \mathbb{L} & \xrightarrow[\jmath]{} & \widehat{\mathbb{L}}. \end{array}$$

Dessa forma, os dois possíveis caminhos de $\mathbb{K}$ *a* $\widehat{\mathbb{L}}$ *originam a mesma função.*

A ideia de equivalência expressada por isomorfismo é válida, pois estes, preservam propriedades do corpo domínio no corpo imagem.

Várias identificações podem ser feitas a partir desta definição. Se identificarmos $\mathbb{K}$ e $\iota(\mathbb{K})$, e $\mathbb{L}$ e $\jmath(\mathbb{L})$, então ι e $\jmath$ são inclusões, e a condição de comutatividade agora torna:

$$\mu|_{\mathbb{K}} = \lambda,$$

em que $\mu|_{\mathbb{K}}$ denota a restrição de μ sobre $\mathbb{K}$. Se identificarmos $\mathbb{K}$ e $\mathbb{L}$, então λ torna-se a identidade, e $\mu|_{\mathbb{K}}$ é a identidade. Usaremos sempre que possível esta identificação entre os corpos que são isomorfos.

2.3.3 Extensões algébricas

Definição 29. *Seja* $\mathbb{K}$ *um subcorpo de* $\mathbb{C}$*, e seja* $\alpha \in \mathbb{C}$*. Então* α *é algébrico sobre* $\mathbb{K}$ *se existe um polinômio não nulo* f *sobre* $\mathbb{K}$*, tal que,* $f(\alpha) = 0$*. Caso contrário, dizemos que* α *é transcendente sobre* $\mathbb{K}$*.*

Definição 30. *Seja* $\mathbb{L}$ *uma extensão do corpo* $\mathbb{K}$*. Se todo* $\alpha \in \mathbb{L}$ *é algébrico sobre* $\mathbb{K}$*, diremos que* $\mathbb{L} : \mathbb{K}$ *é uma extensão algébrica.*

Exemplo 23. O elemento $\sqrt{5}$ é algébrico sobre $\mathbb{Q}$ uma vez que é raiz de $f(x) = x^2 - 5$ e $f(x) \in \mathbb{Q}[x]$. Já π é transcendente sobre $\mathbb{Q}$, pois não existe um polinômio $f(x) \in \mathbb{Q}[x]$ tal que $f(\pi) = 0$. Assim como o número π, o número de Euler "e", também é transcendente, para demonstração veja Figueiredo (2011).

Definição 31. *Seja $\mathbb{L} : \mathbb{K}$ uma extensão de corpos, e suponhamos que $\alpha \in \mathbb{L}$ é algébrico sobre $\mathbb{K}$. O polinômio minimal de α sobre $\mathbb{K}$, é o polinômio mônico m sobre $\mathbb{K}$ de menor grau tal que $m(\alpha) = 0$.*

Exemplo 24. Sabemos que $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ é uma extensão simples e algébrica sobre $\mathbb{Q}$, pois $m(x) = x^2 - 2 \in \mathbb{Q}[x]$ é um polinômio tal que $m(\sqrt{2}) = 0$. Notemos que o polinômio m é mônico. Afirmamos que este é o polinômio minimal de $\sqrt{2}$ sobre $\mathbb{Q}$. De fato, se este não fosse, os polinômios de menor grau em $\mathbb{Q}$ seriam da forma $x - q$ para algum $q \in \mathbb{Q}$, ou o polinômio constante igual a 1. Ora, $\sqrt{2}$ não pode ser zero de nenhum destes, pois se fosse, teríamos $\sqrt{2} \in \mathbb{Q}$. Portanto, o polinômio minimal de $\sqrt{2}$ sobre $\mathbb{Q}$, é mesmo o $m(x) = x^2 - 2$.

Teorema 32. *Se $\mathbb{K}$ é um subcorpo de $\mathbb{C}$ e m é qualquer polinômio mônico irredutível sobre $\mathbb{K}$, então existe um $\alpha \in \mathbb{C}$, algébrico sobre $\mathbb{K}$, tal que α tem m como polinômio minimal sobre $\mathbb{K}$.*

Demonstração. Pelo teorema fundamental da Álgebra, existe pelo menos um α em $\mathbb{C}$, zero de m. Então, $m(\alpha) = 0$, e portanto, o polinômio minimal f de α sobre $\mathbb{K}$, divide m. Ora, m é irredutível sobre $\mathbb{K}$, e ambos f e m são mônicos, logo $f = m$. □

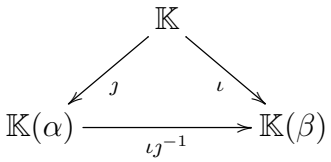
Proposição 33. *Se a extensão é algébrica, então $[\mathbb{K}(\alpha) : \mathbb{K}] = \partial m$, em que ∂m é o grau do polinômio minimal de α sobre $\mathbb{K}$.*

A demonstração pode ser encontrada em Cruz (2014).

Exemplo 25. Vimos que o polinômio minimal de $\sqrt{2}$ é $m(x) = x^2 - 2$, com isso, segue diretamente da proposição que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Teorema 34. *Suponha $\mathbb{K}(\alpha) : \mathbb{K}$ e $\mathbb{K}(\beta) : \mathbb{K}$ extensões algébricas simples, tais que α e β tenham o mesmo polinômio minimal m sobre $\mathbb{K}$. Então, estas duas extensões são isomorfas, e o isomorfismo de corpos maiores, pode ser entendido como uma função de α para β (e como a identidade sobre $\mathbb{K}$).*

Este teorema só é possível por existir o isomorfismo entre o corpo $\mathbb{K}$ e as extensões $\mathbb{K}(\alpha)$ e $\mathbb{K}(\beta)$. Então, considerando $\jmath$ e ι os respectivos isomorfismos. O diagrama ilustra o isomorfismo entre os corpos, sempre que o polinômio minimal for o mesmo, a demonstração pode ser encontrada em Cruz (2014).



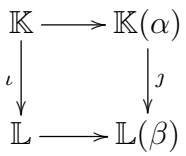
Lema 35. *Seja $\mathbb{K}(\alpha) : \mathbb{K}$ uma extensão algébrica simples, e seja m o polinômio minimal de α sobre $\mathbb{K}$, e ainda $\partial m = n$. Então, $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ é uma base para $\mathbb{K}(\alpha)$ sobre $\mathbb{K}$. Em particular, $[\mathbb{K}(\alpha) : \mathbb{K}] = n$.*

A demonstração pode ser encontrada em Gonçalves (2006).

Exemplo 26. Como já visto anteriormente, $\{1, i, \sqrt{3}, i\sqrt{3}\}$ forma uma base para o espaço vetorial $\mathbb{Q}(i, \sqrt{3})$ sobre $\mathbb{Q}$, assim, $[\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}] = 4$.

Teorema 36. *Suponha que $\mathbb{K}$ e $\mathbb{L}$ sejam subcorpos de $\mathbb{C}$ e que $\iota : \mathbb{K} \to \mathbb{L}$ é um isomorfismo. Sejam $\mathbb{K}(\alpha)$ e $\mathbb{L}(\beta)$ extensões algébricas simples de $\mathbb{K}$ e $\mathbb{L}$, respectivamente, tais que $m_\alpha(t)$ é o polinômio minimal de α sobre $\mathbb{K}$, e $m_\beta(t)$, o polinômio minimal de β sobre $\mathbb{L}$. Além disso, suponha que $m_\beta(t) = \iota(m_\alpha(t))$. Então, existe um isomorfismo $j : \mathbb{K}(\alpha) \to \mathbb{L}(\beta)$ tal que $j|_{\mathbb{K}} = \iota$ e $j(\alpha) = \beta$.*

A existência de um isomorfismo entre $\mathbb{K}$ e $\mathbb{L}$ nos dá a partir de agora a existência de um isomorfismo entre as extensões, de modo que as raízes são levadas em raízes, ilustrada pelo diagrama abaixo.



No próximo capítulo faremos uma aplicação de toda teoria desenvolvida neste capítulo. Veremos que a garantia de existência destes isomorfismos entre as extensões é essencial para gerarmos o grupo de Galois, e assim, permite-nos aplicar a teoria de grupos em problemas de polinômios em $\mathbb{C}$.

Capítulo 3

Teoria de Galois

Veremos neste capítulo alguns elementos da Teoria de Galois que nos mostram em quais circunstâncias um polinômio de qualquer grau pode ou não apresentar soluções por meio de radicais.

3.1 Corpo de decomposição

Definição 32. *Seja $f(x) \in \mathbb{K}[x]$. O menor subcorpo de $\mathbb{C}$ que contém $\mathbb{K}$ e todas as raízes de $f(x)$, é chamado corpo de decomposição do polinômio $f(x)$, e denotaremos por $L = Gal(f, \mathbb{K})$.*

Quando falamos em corpo de decomposição de um polinômio, este é o menor corpo tal que é escrito como produto de fatores de polinômios de grau 1 (polinômios lineares).

Antes de ver mais um exemplo, vamos relembrar sobre raiz n-ésima da unidade. Pois alguns exemplos de extensões podem ser obtidas considerando as raízes da unidade. Considere a equação $z^n - 1 = 0$, queremos determinar todas os valores $\omega \in \mathbb{C}$ tais que $\omega^n = 1$. Os valores que satisfazem essa equação são da forma:

$$w_k = \sqrt[n]{|1|}\left(\cos\frac{2k\pi}{n} + i\,\mathrm{sen}\frac{2k\pi}{n}\right);\ 0 \leq k \leq n-1.$$

A partir da fórmula de De Moivre obtemos $\omega = (\cos\frac{2\pi}{n} + i\,\mathrm{sen}\frac{2\pi}{n})$, assim, para

$$\begin{aligned} k &= 0 \Rightarrow w_0 = (\cos 0 + i\,\mathrm{sen}0) = 1 = \omega^0; \\ k &= 1 \Rightarrow w_1 = (\cos\frac{2\pi}{n} + i\,\mathrm{sen}\frac{2\pi}{n}) = \omega; \\ k &= 2 \Rightarrow w_2 = (\cos\frac{4\pi}{n} + i\,\mathrm{sen}\frac{4\pi}{n}) = \omega^2; \\ k &= 3 \Rightarrow w_3 = (\cos\frac{6\pi}{n} + i\,\mathrm{sen}\frac{6\pi}{n}) = \omega^3; \\ &\vdots \end{aligned}$$

$$k = n-1 \Rightarrow w_{n-1} = (\cos\frac{2(n-1)\pi}{n} + i\,\mathrm{sen}\frac{2(n-1)\pi}{n}) = \omega^{n-1}.$$

Observe que $\omega^n = 1$, sendo assim, se consideramos o conjunto formado por todas as raízes n-ésimas da unidade com a operação multiplicação, será um grupo cíclico gerado por ω.

$$C_n = \left\{1, \omega, \cdots, \omega^{n-1}\right\} = \langle\omega\rangle \cong \mathbb{Z}_n$$

Uma raiz n-ésima da unidade é chamada de primitiva (ou seja, uma raiz primitiva n-ésima da unidade) quando ela não é também uma raiz m-ésima da unidade para $m < n$. Com isso, vemos que as raízes primitivas da unidade também geram o grupo C_n composto das raízes n-ésimas da unidade. Logo, uma raiz ω^m é primitiva se, e somente se, $mdc(m,n) = 1$. Se n for primo, então toda raiz da unidade é primitiva.

Exemplo 27. Vamos determinar o corpo de decomposição do polinômio $f(x) = x^5 - 3 \in \mathbb{Q}[x]$.

Como o polinômio é irredutível sobre $\mathbb{Q}$ devemos estender esse corpo de modo que $f(x)$ se decomponha linearmente. O polinômio $f(x)$ se decompõe sobre $\mathbb{Q}(\sqrt[5]{3}, \omega)$, onde $\omega = \cos\frac{2\pi}{5} + i\,\mathrm{sen}\frac{2\pi}{5}$, raiz quinta da unidade. De fato, temos que $\sqrt[5]{3}$ e $\sqrt[5]{3}\omega = \sqrt[5]{3}(\cos\frac{2\pi}{5} + i\,\mathrm{sen}\frac{2\pi}{5})$ são raízes de $f(x)$, então pela fórmula de Moivre

$$w_k = \sqrt[5]{3}\left(\cos\frac{2k\pi}{5} + i\,\mathrm{sen}\frac{2k\pi}{5}\right) = \sqrt[5]{3}\left(\cos\frac{2\pi}{5} + i\,\mathrm{sen}\frac{2\pi}{5}\right)^k = \sqrt[5]{3}\omega^k, \quad \forall \;\; 0 \leq k \leq 4.$$

Observe a semelhança com as raízes da unidade. O polinômio é redutível sobre a extensão $\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}$, porém, não de forma linear. Sendo assim, é necessário uma nova extensão.

Como vimos acima, as raizes do polinômio são $\sqrt[5]{3}$ e $\sqrt[5]{3}\omega$, $\sqrt[5]{3}\omega^2$, $\sqrt[5]{3}\omega^3$, $\sqrt[5]{3}\omega^4$. Logo a extensão $\mathbb{Q}(\sqrt[5]{3}, \omega) : \mathbb{Q}(\sqrt[5]{3})$ nos dará as raízes que faltam para fatoração linear. Pela Definição 32, $Gal(x^5 - 3, \mathbb{Q}) = \mathbb{Q}(\sqrt[5]{3}, \omega)$ é o corpo de decomposição do polinômio

$f(x)$.

3.2 Normalidade e separabilidade

Definição 33. *Uma extensão $\mathbb{L} : \mathbb{K}$ é normal se todo polinômio irredutível f sobre $\mathbb{K}$ que tem ao menos um zero em $\mathbb{L}$ se decompõe linearmente em $\mathbb{L}$.*

Exemplo 28. No exemplo anterior $\mathbb{Q}(\sqrt[5]{3}, \omega) : \mathbb{Q}$ é uma extensão normal, enquanto a extensão $\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}$ não é normal, uma vez que o polinômio $f(x) = x^5 - 3$ possui um zero em $\mathbb{Q}(\sqrt[5]{3})$, mas este não se decompõe linearmente em $\mathbb{Q}(\sqrt[5]{3})$, já que as demais raízes são complexas.

Teorema 37. *Uma extensão de corpo é normal se, e somente se, é o corpo de decomposição para algum polinômio.*

A demonstração pode ser encontrada em Cruz (2014).

Definição 34. *Um polinômio irredutível f sobre um subcorpo $\mathbb{K}$ de $\mathbb{C}$ é separável sobre $\mathbb{K}$ se tem apenas zeros simples em $\mathbb{C}$.*

Veremos ferramentas que irão nos auxiliar na construção do grupo de Galois de um polinômio.

Definição 35. *Suponhamos que $\mathbb{K}$ seja um subcorpo de $\mathbb{C}$, e*

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{K}[x].$$

Então, a derivada de f é o polinômio

$$f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \in \mathbb{K}[x].$$

Se $\mathbb{K} = \mathbb{R}$ (ou $\mathbb{K} = \mathbb{C}$), não há, em geral, razão para pensarmos em $f'(x)$ como a taxa de variação de f, mas as propriedades de derivação são preservadas. Em particular, para todo polinômio f e g sobre $\mathbb{K}[x]$,

$$(f + g)' = f' + g' \text{ e}$$

$$(fg)' = (f')g + f(g').$$

Também, se $\lambda \in \mathbb{K}$, então $(\lambda)' = 0$, e assim,

$$(\lambda f)' = \lambda(f').$$

Estas propriedades da derivada permitem estabelecermos critérios para existência de zeros múltiplos de um polinômio.

Proposição 38. *Seja $f(x) \in \mathbb{K}[x]$, onde $\mathbb{K} \subset \mathbb{C}$, $\partial f \geq 1$. Então,*

i) $f(x)$ é separável $\Leftrightarrow mdc(f(x), f'(x)) = 1$;

ii) se $f(x)$ é irredutível sobre $\mathbb{K}$, então todas as raízes de $f(x)$ são simples.

Demonstração. i) ($\Rightarrow$) Seja $f(x) = (x-\alpha)^k g(x)$, onde $g(x)$ é um polinômio tal que $\partial g < \partial f$ e k é a multiplicidade de α. A derivada de $f(x)$ é

$$f'(x) = k(x-\alpha)^{k-1} g(x) + (x-\alpha)^k g'(x).$$

Para $k = 1$,

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

e, para $k > 1$, temos

$$\begin{aligned} f'(x) &= k(x-\alpha)^{k-1} g(x) + (x-\alpha)^k g'(x) \\ f'(x) &= (x-\alpha)[k(x-\alpha)^{k-2} g(x) + (x-\alpha)^{k-1} g'(x)]. \end{aligned}$$

Ou seja, se $k > 1$, $f(x)$ e $f'(x)$ tem um fator em comum, logo $mdc(f(x), f'(x)) \neq 1$. Diferentemente, se $k = 1$, $f(x)$ é separável e $f'(\alpha) \neq 0$. Logo, $mdc(f(x), f'(x)) = 1$.

($\Leftarrow$) Suponhamos que $f(x) = (x-\alpha)g(x)$ e $f'(x) = (x-\alpha)h(x)$, ou seja, que α é raiz de multiplicidade 1 dos polinômios $f(x)$ e $f'(x)$. Veja que,

$$f'(x) = g(x) + (x-\alpha)g'(x) = (x-\alpha)h(x).$$

Como $f'(\alpha) = 0$, temos

$$0 = f'(\alpha) = g(\alpha) + (\alpha - \alpha)g'(\alpha) \Rightarrow g(\alpha) = 0.$$

E portanto α possui multiplicidade $n \geq 1$. Podemos então escrever $g(x) = (x - \alpha)^n p(x)$. Agora, substituindo em $f(x) = (x - \alpha)g(x)$, obtemos que

$$f(x) = (x - \alpha)[(x - \alpha)^n p(x)] = (x - \alpha)^{n+1} p(x).$$

Assim, α possui multiplicidade no mínimo 2. Logo, se $f(x)$ e $f'(x)$ forem coprimos, ou seja, $mdc(f(x), f'(x)) = 1$, teremos que α é uma raiz simples.

ii) Como $f(x)$ é irredutível, então a menos de constante, seus divisores são apenas $f(x)$ e 1, não possuindo fator comum com $f'(x)$ e portanto $mdc(f(x), f'(x)) = 1$. Pelo item anterior segue que todas as raízes de $f(x)$ são simples. □

Definição 36. *Dizemos que uma extensão $\mathbb{L} : \mathbb{K}$ é separável se todo elemento de $\mathbb{L}$ for raiz de um polinômio separável com coeficientes em $\mathbb{K}$.*

Definição 37. *Dizemos que uma extensão $\mathbb{L} : \mathbb{K}$ é um corpo de decomposição, denotado por $Gal(f, \mathbb{K})$, se ela for normal e separável.*

Observação 7. Como trabalhamos com extensões que são subcorpos de $\mathbb{C}$, então elas serão sempre separáveis. Sendo assim uma extensão será corpo de decomposição se, e somente se, for normal.

3.3 Automorfismos de corpos

Vimos que automorfismo de um grupo é um isomorfismo do grupo nele mesmo. Podemos estender esse conceito para corpo, como abaixo

Definição 38. *Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos. Uma aplicação $f : \mathbb{K} \to \mathbb{L}$ é um homomorfismo de corpos se preserva a soma e o produto de modo que, $\forall\, a, b \in \mathbb{K}$*

$$\begin{aligned} f(a + b) &= f(a) + f(b) \\ f(a \cdot b) &= f(a) \cdot f(b). \end{aligned}$$

Se f é bijetora dizemos que é um isomorfismo de corpos. O isomorfismo $f : \mathbb{L} \to \mathbb{L}$ é chamado de automorfismo. Os automorfismos de $\mathbb{L}$ que fixam $\mathbb{K}$ são chamados de $\mathbb{K}$-automorfismos de $\mathbb{L}$.

Complementando o Teorema 34.

Proposição 39. *Sejam σ um $\mathbb{K}$-automorfismo de $\mathbb{L}$ e $f(x) \in \mathbb{K}[x]$. Se $\alpha \in \mathbb{L}$ é raiz de $f(x)$, então $\sigma(\alpha)$ também é uma raiz de $f(x)$.*

Demonstração. Inicialmente, mostraremos que $\sigma(f(\alpha)) = f(\sigma(\alpha))$. Considerando $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, aplicando σ em $f(x)$, teremos

$$\begin{aligned}
\sigma(f(\alpha)) &= \sigma(a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) \\
&= \sigma(a_n\alpha^n) + \sigma(a_{n-1}\alpha^{n-1}) + \cdots + \sigma(a_1\alpha) + \sigma(a_0) \\
&= \sigma(a_n)\sigma(\alpha^n) + \sigma(a_{n-1})\sigma(\alpha^{n-1}) + \cdots + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) \\
&= f(\sigma(\alpha)).
\end{aligned}$$

Portanto,

$$\sigma(f(\alpha)) = f(\sigma(\alpha)).$$

Como $f(\alpha) = 0$, segue que

$$f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0.$$

Dessa forma, $\sigma(\alpha)$ é uma raiz de $f(x)$, e fazendo $\sigma(\alpha) = \beta$:

$$\sigma(f(\alpha)) = f(\beta) = 0.$$

Portanto, o automorfismo leva uma raiz de $f(x)$ em outra raiz, ou seja, permuta as raízes de f. □

Seja $\mathbb{L} = \mathbb{Q}(\sqrt{2})$. O elemento $\sqrt{2}$ tem como polinômio minimal $x^2 - 2$. Pelo Teorema 32 qualquer $\mathbb{Q}$-automorfismo $\sigma : \mathbb{L} \to \mathbb{L}$ transforma raízes deste polinômio em raízes do mesmo. Existem, pois, precisamente dois $\mathbb{Q}$-automorfismos:

$$\begin{array}{rccc}
\sigma_1 : & \mathbb{Q}(\sqrt{2}) & \longrightarrow & \mathbb{Q}(\sqrt{2}) \\
& a \in \mathbb{Q} & \longmapsto & a \\
& \sqrt{2} & \longmapsto & \sqrt{2}
\end{array}
\qquad \text{e} \qquad
\begin{array}{rccc}
\sigma_2 : & \mathbb{Q}(\sqrt{2}) & \longrightarrow & \mathbb{Q}(\sqrt{2}) \\
& a \in \mathbb{Q} & \longmapsto & a \\
& \sqrt{2} & \longmapsto & -\sqrt{2}.
\end{array}$$

O primeiro é a identidade e o segundo aplica cada elemento $a+b\sqrt{2}$ de $\mathbb{Q}(\sqrt{2})$ em $a-b\sqrt{2}$. Agora estamos prontos para definir o Grupo de Galois de um polinômio.

Definição 39. *Sejam $f(x)$ um polinômio em $\mathbb{K}[x]$ e $\mathbb{L}$ seu corpo de decomposição sobre $\mathbb{K}$. O conjunto $Gal(\mathbb{L}:\mathbb{K})$ formado por todos os automorfismos de $\mathbb{L}$ que fixam $\mathbb{K}$ é o grupo de Galois de $f(x)$.*

Do exemplo anterior, $Gal(\mathbb{L}:\mathbb{Q}) = \{id, \sigma_2\}$, que é isomorfo a $\mathbb{Z}_2$.

Teorema 40. *Seja $\mathbb{F}:\mathbb{K}$ uma extensão normal e finita, com grupo de Galois $Gal(\mathbb{F}:\mathbb{K})$. Então $\mathbb{L}$ é uma extensão normal de $\mathbb{K}$ se, e somente se, $Gal(\mathbb{F}:\mathbb{L})$ é um subgrupo normal de $Gal(\mathbb{F}:\mathbb{K})$, e neste caso $Gal(\mathbb{L}:\mathbb{K}) \cong Gal(\mathbb{F}:\mathbb{K})/Gal(\mathbb{F}:\mathbb{L})$.*

Uma demonstração pode ser encontrado em Santos (2019).

Teorema 41. *Seja $\mathbb{L}:\mathbb{K}$ uma extensão finita. Então as seguintes condições são equivalentes:*

i) $\mathbb{L}$ *é corpo de decomposição;*

ii) $\mathbb{L}:\mathbb{K}$ *é normal;*

iii) $|Gal(\mathbb{L}:\mathbb{K})| = [\mathbb{L}:\mathbb{K}]$.

Demonstração. $(i) \Rightarrow (ii)$ Segue da Definição 37 e da Observação 7.

$(ii) \Rightarrow (iii)$ Seja $p(x) \in \mathbb{K}[x]$ o polinômio minimal de α, tal que $\mathbb{L} = \mathbb{K}(\alpha)$, e seja σ um $\mathbb{K}$-automorfismo de $\mathbb{L}$. Como sabemos, $\sigma(\alpha) = \alpha'$, onde α' também é raiz de $p(x)$ e $\alpha' \in \mathbb{L}$. Logo $\mathbb{K}(\alpha') \subset \mathbb{L}$ e $[\mathbb{K}(\alpha'):\mathbb{K}] = [\mathbb{L}:\mathbb{K}] = \partial p(x)$ então $\mathbb{L} = \mathbb{K}(\alpha) = \mathbb{K}(\alpha')$. Como σ fica determinado com o que faz com α então $|Gal(\mathbb{L}:\mathbb{K})|$ é no máximo a quantidade de raízes de $p(x)$, que é no máximo $\partial p(x) = [\mathbb{L}:\mathbb{K}]$, logo $|Gal(\mathbb{L}:\mathbb{K})| \leq [\mathbb{L}:\mathbb{K}]$.

O leitor encontrará em Gonçalves (2006) a prova de que $|Gal(\mathbb{L}:\mathbb{K})| \geq [\mathbb{L}:\mathbb{K}]$, e então $|Gal(\mathbb{L}:\mathbb{K})| = [\mathbb{L}:\mathbb{K}]$.

$(iii) \Rightarrow (i)$ Supondo que $|Gal(\mathbb{L}:\mathbb{K})| = [\mathbb{L}:\mathbb{K}]$, mostremos que $\mathbb{L}$ é corpo de decomposição de $p(x) \in \mathbb{K}[x]$. Seja $p(x)$ o polinômio separável e minimal de α, e $\mathbb{L} = \mathbb{K}(\alpha)$. Seja ainda σ um $\mathbb{K}$-automorfismo de $\mathbb{L}$, tem-se que $\sigma(\alpha) \in \mathbb{L}$ e é outra raiz de $p(x)$. Assim $|Gal(\mathbb{L}:\mathbb{K})|$ é menor ou igual ao número de raízes de $p(x)$. Agora, como $|Gal(\mathbb{L}:\mathbb{K})| = [\mathbb{L}:\mathbb{K}]$, teremos $|Gal(\mathbb{L}:\mathbb{K})| = \partial p(x)$ que é igual ao número de raízes de $p(x)$ em $\mathbb{L}$. Segue que $\mathbb{L}$ contém todas as raízes de $p(x)$, e portanto $\mathbb{L} = Gal(p(x), \mathbb{K})$, e $\mathbb{L}:\mathbb{K}$ é um corpo de decomposição. □

Para uma melhor compreensão do que foi visto até aqui vejamos um exemplo:

Exemplo 29. Vamos determinar o grupo de Galois da extensão $Gal(x^4 - 3, \mathbb{Q})$.

De modo análogo ao Exemplo 27 temos que as raízes do polinômio $p(x) = x^4 - 3$ são: $\sqrt[4]{3}, -\sqrt[4]{3}, i\sqrt[4]{3}, -i\sqrt[4]{3}$. O polinômio p pode ser fatorado da seguinte forma:

$$p(x) = (x - \varepsilon)(x + \varepsilon)(x - i\varepsilon)(x + i\varepsilon),$$

onde $\varepsilon = \sqrt[4]{3}$. Portanto todas as raízes estão na extensão $\mathbb{Q}(\varepsilon, i)$. Como ela é normal e separável então pela Definição 37 e pela Observação 7 temos que $Gal(x^4 - 5, \mathbb{Q}) = \mathbb{Q}(\varepsilon, i)$. Usando a Lei da Torre, temos que:

$$[\mathbb{Q}(\varepsilon, i) : \mathbb{Q}] = [\mathbb{Q}(\varepsilon, i) : \mathbb{Q}(\varepsilon)] \cdot [\mathbb{Q}(\varepsilon) : \mathbb{Q}].$$

Observe que ε é um zero de um polinômio sobre $\mathbb{Q}$ e pelo Critério de Eisenstein, $p(x)$ é irredutível. Temos ainda, que $p(x)$ é o polinômio minimal de ε sobre $\mathbb{Q}$. Segue pela Proposição 33, que $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = 4$. Temos que $[\mathbb{Q}(\varepsilon, i) : \mathbb{Q}(\varepsilon)] = 2$, pois o polinômio minimal de i sobre $\mathbb{Q}(\varepsilon)$ é $x^2 + 1 = 0$, mas $i \notin \mathbb{R} \supseteq \mathbb{Q}(\varepsilon)$. Logo,

$$[\mathbb{Q}(\varepsilon, i) : \mathbb{Q}] = 8.$$

Pelo Teorema 41, temos que $|Gal(\mathbb{Q}(\varepsilon, i) : \mathbb{Q})| = 8$.

Agora devemos encontrar os elementos do Grupo de Galois de $\mathbb{Q}(\varepsilon, i) : \mathbb{Q}$. Pelo Teorema 34, há um $\mathbb{Q}$-automorfismo σ de $\mathbb{Q}(\varepsilon, i)$ tal que,

$$\sigma(i) = i \quad \text{e} \quad \sigma(\varepsilon) = i\varepsilon,$$

e por outro τ, tal que

$$\tau(i) = -i \quad \text{e} \quad \tau(\varepsilon) = \varepsilon$$

Produtos destes geram 8 distintos $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\varepsilon, i)$, como seguem:
Observe que:

$$\sigma^4(\varepsilon) = \sigma^2(\sigma^2(\varepsilon)) = \sigma^2(-\varepsilon) = \varepsilon, \qquad \sigma^4(i) = i,$$

$$\tau^2(\varepsilon) = \varepsilon \quad \text{e} \quad \tau^2(i) = \tau(\tau(i)) = -\tau(i) = i.$$

Automorfismos	Aplicados em ε	Aplicados em i
1	ε	i
σ	$i\varepsilon$	i
$\sigma^2 = \sigma \circ \sigma$	$-\varepsilon$	i
σ^3	$-i\varepsilon$	i
τ	ε	$-i$
$\sigma\tau$	$i\varepsilon$	$-i$
$\sigma^2\tau$	$-\varepsilon$	$-i$
$\sigma^3\tau$	$-i\varepsilon$	$-i$

Tabela 3.1: $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\varepsilon, i)$

Com isso, $\sigma^4 = \tau^2 = 1$. E também, usando a tabela,

$$\sigma^3\tau(\varepsilon) = \sigma^3(\tau(\varepsilon)) = \sigma^3(\varepsilon) = -i\varepsilon = \tau\sigma(\varepsilon) \text{ e } \sigma^3\tau(i) = \sigma^3(-i) = -i = \tau\sigma(i),$$

ou seja, $\sigma^3\tau = \tau\sigma$. De maneira análoga temos $\tau\sigma^2 = \sigma^2\tau$ e $\tau\sigma^3 = \sigma\tau$.

Dessa forma a estrutura do grupo de Galois para este polinômio será

$$G = \langle \sigma, \tau : \sigma^4, \tau^2, \tau\sigma = \sigma^3\tau \rangle,$$

isto é, G é o grupo diedral de ordem 8.

Agora veremos como associar o grupo de Galois de um polinômio com a sua solubilidade.

3.4 Solubilidade por radicais

Veremos nesta sessão as condições necessárias para que um polinômio seja solúvel por radicais, ou seja, para que suas raízes sejam expressas apenas por operações elementares e radicais. Usaremos a teoria de Galois para mostrar que se o grupo associado as raízes de um polinômio for solúvel então o polinômio será solúvel por radicais.

Definição 40. *Um corpo $\mathbb{L}$ é dito ser uma extensão radical de um corpo $\mathbb{K}$ se existe uma cadeia de corpos*

$$\mathbb{K} = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \mathbb{K}_2 \subseteq \cdots \subseteq \mathbb{K}_r = \mathbb{L}$$

na qual para cada $i = 1, 2, \cdots, r$, tem-se $\mathbb{K}_i = \mathbb{K}_{i-1}(\alpha_i)$ com $\alpha_i^m \in \mathbb{K}_{i-1}$ para algum inteiro m.

Exemplo 30. Considere o polinômio $f(x) = x^3 - 2 \in \mathbb{Q}[x]$.

Os zeros desse polinômio são: $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2}\omega$, $\alpha_3 = \sqrt[3]{2}\omega^2$, onde $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ (raiz primitiva da unidade). Assim a cadeia correspondente é

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

Como encontramos uma extensão radical de $\mathbb{Q}$ que contém todas as raízes de $f(x)$, diremos que este polinômio é solúvel por radicais.

Definição 41. *Seja f um polinômio sobre um subcorpo $\mathbb{K}$ de $\mathbb{C}$, e seja $Gal(f, \mathbb{K})$ o corpo de decomposição de f sobre $\mathbb{K}$. Dizemos que f é solúvel por radicais se existe um corpo $\mathbb{M}$ contendo $Gal(f, \mathbb{K})$, tal que $\mathbb{M} : \mathbb{K}$ seja uma extensão radical.*

Lema 42. *Seja $\mathbb{K}$ um subcorpo de $\mathbb{C}$ e seja $\mathbb{L}$ o corpo de decomposição para $t^p - 1$ sobre $\mathbb{K}$, onde p é primo. Então, o Grupo de Galois $Gal(\mathbb{L} : \mathbb{K})$ é abeliano.*

Demonstração. A derivada de $t^p - 1$ é pt^{p-1} que são coprimos. Logo, pela Proposição 38, o polinômio não tem zeros múltiplos em $\mathbb{L}$. Claramente, seus zeros formam um grupo sob multiplicação; este grupo tem ordem prima p, e como os zeros são distintos, ele é cíclico.

Seja ξ um gerador deste grupo. Então, $\mathbb{L} = \mathbb{K}(\xi)$, e qualquer $\mathbb{K}$-automorfismo de $\mathbb{L}$ é determinado por seu efeito em ξ.

Além disso, $\mathbb{K}$-automorfismos permutam os zeros de $t^p - 1$. Portanto, qualquer $\mathbb{K}$-automorfismo de $\mathbb{L}$ é da forma,

$$\alpha_j : \xi \to \xi^j,$$

e é unicamente determinado por esta condição. Mas, então $\alpha_i\alpha_j$ e $\alpha_j\alpha_i$ levam, ambos, ξ em ξ^{ij} , portanto, o Grupo de Galois associado a $t^p - 1$ é abeliano. □

Lema 43. *Seja $\mathbb{K}$ um subcorpo de $\mathbb{C}$ em que $t^n - 1$ se decompõe linearmente. Sejam $a \in \mathbb{K}$ e $\mathbb{L}$ um corpo de decomposição para $t^n - a$ sobre $\mathbb{K}$. Então, o Grupo de Galois de $\mathbb{L} : \mathbb{K}$ é abeliano.*

Demonstração. Seja α um zero qualquer de $t^n - a$. Como $t^n - 1$ se decompõe linearmente em $\mathbb{K}$, o zero geral de $t^n - a$ é ξ_a onde ξ é um zero de $t^n - 1$ em $\mathbb{K}$. Como $\mathbb{L} = \mathbb{K}(\alpha)$, qualquer $\mathbb{K}$-automorfismo de $\mathbb{L}$ é determinado por seu efeito em α. Dados dois $\mathbb{K}$-automorfismos:

$$\Phi : \alpha \longmapsto \xi\alpha \quad e \quad \Psi : \alpha \longmapsto \eta\alpha,$$

onde ξ e η são raizes da unidade, então

$$\Phi\Psi(\alpha) = \xi\eta\alpha = \eta\xi\alpha = \Psi\Phi(\alpha).$$

E, como anteriormente, o Grupo de Galois associado a $t^n - a$ é abeliano. □

Definição 42. *Seja f um polinômio sobre $\mathbb{K}$ (um subcorpo de $\mathbb{C}$), com corpo de decomposição $Gal(f, \mathbb{K})$ sobre $\mathbb{K}$. O Grupo de Galois de f sobre $\mathbb{K}$ é o grupo $Gal(Gal(f, \mathbb{K}) : \mathbb{K})$.*

Teorema 44 (Galois)**.** *Seja $f(x) \in \mathbb{K}[x]$, com $\mathbb{K} \subset \mathbb{C}$, e $\mathbb{L} = Gal(f, \mathbb{K})$ o corpo de decomposição de $f(x)$ sobre $\mathbb{K}$. O polinômio $f(x)$ é solúvel por radicais sobre $\mathbb{K}$ se, e somente se, $Gal(\mathbb{L} : \mathbb{K})$ é um grupo solúvel.*

Demonstração. ($\Rightarrow$) Suponhamos que $f(x) = 0$ seja solúvel por radicais, e $\mathbb{L} : \mathbb{K}$ seja seu corpo de decomposição. Da definição 41, $\exists\, \mathbb{M}$ com $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$, tal que a extensão $\mathbb{M} : \mathbb{K}$ é radical. Então:

$$\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 = \mathbb{K}_0(\alpha_1) \subset \cdots \subset \mathbb{K}_t = \mathbb{K}_{t-1}(\alpha_t) = \mathbb{M},$$

onde para cada $i \in \{1, 2, \cdots, t\}$, $\exists\, m_i \in \mathbb{Z}$ tais que $\alpha_i^{m_i} \in \mathbb{K}_{i-1}$. Por conveniência os m_i's são positivos e mínimos.

Tome $n = mmc(m_1, m_2, \cdots, m_t)$, e seja $\omega_n \in \mathbb{C}$ uma raíz n-ésima primitiva da unidade. Fazendo $\mathbb{M}' = \mathbb{M}(\omega_n)$, onde $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M} \subset \mathbb{M}'$, temos que $\mathbb{M}' = \mathbb{K}(\alpha_1, \alpha_2, \cdots, \alpha_t, \omega_n)$, que é equivalente a $\mathbb{M}' = \mathbb{K}(\omega_n, \alpha_1, \alpha_2, \cdots, \alpha_t)$, e $\mathbb{M}'(\omega_n) : \mathbb{K}$ é uma extensão radical, uma vez que $\omega_n^n = 1$, de acordo com a Definição 40. Temos então a seguinte cadeia:

$$\mathbb{M}_0 = \mathbb{K} \subset \mathbb{M}_1 = \mathbb{M}_0(\omega_n) \subset \mathbb{M}_2 = \mathbb{M}_1(\alpha_1) \subset \cdots \subset \mathbb{M}_{t+1} = \mathbb{M}_t(\alpha_t) = \mathbb{M}'.$$

Onde para cada $i \in \{1, 2, \cdots, t\}$, temos que $\alpha_i^{m_i} \in \mathbb{M}_{i-1}$. Notemos que tanto $\mathbb{L}$ quanto $\mathbb{M}'$ são corpos de decomposição de f sobre $\mathbb{K}$. Seja $G_i = Aut_{\mathbb{M}_i}\mathbb{M}' = \{\sigma : \mathbb{M}' \to \mathbb{M}'; \sigma(k) = k, \forall\, k \in \mathbb{M}_i\}$, com $i \in \{0, 1, \cdots, t+1\}$ ($Aut_{\mathbb{M}_i}\mathbb{M}'$ é o conjunto dos $\mathbb{M}_i$-automorfismo de

$\mathbb{M}'$), do Teorema 40 obtemos a seguinte subsérie normal:

$$\{e\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_{t+1} = G.$$

Ainda do Teorema 40, segue que:

$$\frac{G_i}{G_{i-1}} = \frac{Aut_{\mathbb{M}_i}\mathbb{M}'}{Aut_{\mathbb{M}_{i-1}}\mathbb{M}'} \cong Aut_{\mathbb{M}_i}\mathbb{M}_{i-1}.$$

Analisando $Aut_{\mathbb{M}_i}\mathbb{M}_{i-1}$, temos que, para $i = 1$, $Aut_{\mathbb{M}_1}\mathbb{M}_0 = Aut_{\mathbb{K}}\mathbb{K}[\omega_n]$, que de acordo com o Lema 43 é abeliano.

Para $n \geq 2$, segue ainda do Lema 43 que $Aut_{\mathbb{M}_i}\mathbb{M}_{i-1}$ é abeliano. Portanto $G = Aut_{\mathbb{K}}\mathbb{M}'$ é solúvel. Novamente pelo Teorema 40 temos que,

$$Aut_{\mathbb{K}}\mathbb{L} \cong \frac{Aut_{\mathbb{K}}\mathbb{M}'}{Aut_{\mathbb{L}}\mathbb{M}'}$$

E portanto, pelo Teorema 12 seque que $Aut_{\mathbb{K}}\mathbb{L}$ é solúvel.

($\Leftarrow$) Pode ser encontrada em Bewersdorff (2006).

De modo a exemplificar o teorema acima, observe que a seguinte equação $x^n - a = 0$. Facilmente podemos notar que trata-se de uma equação solúvel por radicais, uma vez que diante do que já vimos, suas n soluções serão $\{\sqrt[n]{a}, \sqrt[n]{a}\omega_n, \sqrt[n]{a}\omega_n^2, \cdots, \sqrt[n]{a}\omega_n^{n-1}\}$, com $\omega_n = \cos\left(\frac{2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2k\pi}{n}\right)$, com $k = 0, \cdots, n-1$.

Concluímos que as raízes de um polinômio podem ser escritas a partir de seus coeficientes se o Grupo de Galois associado ao polinômio é solúvel. O problema em determinar a solubilidade por radicais de polinômios foi resolvido, mas da forma como vimos, é preciso ter acesso as raízes para que possamos decidir sobre a solubilidade. No próximo capítulo mostraremos ferramentas que irão nos auxiliar sem termos as raízes de forma explícita.

Capítulo 4

Equações polinomiais

Neste capítulo veremos deduções das fórmulas por radicais para resolução de polinômios de grau 3 e 4 e a não solubilidade por radicais para um polinômio de grau 5. Como já foi dito no capítulo 1, para polinômios com estes graus existe a necessidade de trabalharmos em corpos para garantir a existências de raízes.

Como vimos no Teorema 44, uma equação polinomial será solúvel por radicais se o grupo de Galois associado ao corpo de decomposição do polinômio for solúvel. E também pelo Teorema 17 que o grupo de Galois é isomorfo a um subgrupo de S_n, que, de acordo com o Corolário 16 e pelos Exemplos $1, 3$ e 4 de 1.4.4, será sempre solúvel para $n \leq 4$. Assim, como toda equação de grau n tem seu grupo de Galois isomorfo a um subgrupo de S_n, então teremos sempre que o grupo de Galois será solúvel para $n \leq 4$ e portanto toda equação de grau ≤ 4 será solúvel por radicais.

Agora, no Exemplo 27 temos que a equação polinomial, apesar de ter grau 5, é solúvel por radicais e esse fato ocorre apenas pelo fato do grupo de Galois do polinômio ser solúvel. Veremos um exemplo onde a solubilidade por radicais não é possível para um polinômio de quinto grau.

4.1 Equação de grau 3

Definição 43. *Uma equação cúbica ou de grau* 3 *é toda equação da forma*

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

onde a, b, c *e* $d \in \mathbb{C}$*, com* $a \neq 0$.

Para determinar sua solução utilizaremos um método conhecido como Fórmula de Cardano - Tartaglia. Para isso, inicialmente podemos dividir toda equação por a, de modo à torná-la mônica,

$$x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a} = 0.$$

Logo, basta considerar equações em que o coeficiente de x^3 é igual 1.

Dada a equação $x^3 + ax^2 + bx + c = 0$, a substituição $x = y - \frac{a}{3}$ a trasforma em

$$\begin{aligned}
\left(y - \frac{a}{3}\right)^3 + a\left(y - \frac{a}{3}\right)^2 + b\left(y - \frac{a}{3}\right) + c &= 0 \\
y^3 - ay^2 + \frac{a^2}{3}y - \frac{a^3}{27} + a\left(y^2 - \frac{2a}{3}y + \frac{a^2}{9}\right) + b\left(y - \frac{a}{3}\right) + c &= 0 \\
y^3 + \left(b - \frac{a^2}{3}\right)y + \frac{2a^3}{27} - \frac{ab}{3} + c &= 0,
\end{aligned}$$

que é uma equação desprovida de termo de grau 2. Portanto, é suficiente estudar as equações do grau 3 do tipo

$$y^3 + py + q = 0,$$

onde $p = b - \frac{a^2}{3}$ e $q = \frac{2a^3}{27} - \frac{ab}{3} + c$.

Para encontrar as raízes, escremos $y = u + v$. Substituindo, obtemos

$$u^3 + v^3 + 3u^2v + 3uv^2 + p(u + v) + q = 0,$$

isto é,

$$u^3 + v^3 + (3uv + p)(u + v) + q = 0.$$

Portanto, se existem números u, v tais que

$$u^3 + v^3 + q = 0, \qquad uv + \frac{p}{3} = 0,$$

ou seja, elevando ao cubo a segunda equação, ficamos com

$$u^3 + v^3 = -q, \qquad u^3v^3 = -\frac{p^3}{27},$$

então $y = u + v$ será raiz da equação $y^3 + py + q = 0$.

Ora, o problema de achar u^3 e v^3 conhecendo sua soma e o produto é, como

sabemos, de fácil solução: u^3 e v^3 são as raízes da equação do segundo grau

$$w^2 + qw - \frac{p^3}{27} = 0.$$

Utilizando a fómula de Bhaskara obtemos

$$\begin{cases} u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} &= z_1 \\ v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} &= z_2. \end{cases}$$

Escolhendo uma das raízes cúbicas de z_1, temos que as soluções são $\sqrt[3]{z_1}, \omega\sqrt[3]{z_1}$ e $\omega^2\sqrt[3]{z_1}$ em que $\omega = \frac{-1+i\sqrt{3}}{2}$ é uma das raízes cúbicas da unidade. Denotando agora por $\sqrt[3]{z_2}$ a raiz cúbica de z_2, de forma que a segunda equação do sistema seja satisfeita, admitimos as seguintes soluções:

$$\begin{aligned} u_1 &= \sqrt[3]{z_1}, & v_1 &= \sqrt[3]{z_2}, \\ u_2 &= \omega\sqrt[3]{z_1}, & v_2 &= \omega^2\sqrt[3]{z_2}, \\ u_3 &= \omega^2\sqrt[3]{z_1}, & v_3 &= \omega\sqrt[3]{z_2}. \end{aligned}$$

Logo, o polinômio $y^3 + py + q = 0$ possue como solução as chamadas fórmulas de Cardano - Tartaglia:

$$\begin{aligned} y_1 &= u_1 + v_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \\ y_2 &= u_2 + v_2 = \omega\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \omega^2\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \\ y_3 &= u_3 + v_3 = \omega^2\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \omega\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}. \end{aligned}$$

Finalmente, lembrando que as raízes são da forma $x_i = y_i - \frac{a}{3}$ com $i = 1, 2$ e 3, resolvemos o problema.

Algumas observações podem ser feitas em relação ao radicando

$$\Delta = \frac{q^2}{4} + \frac{p^3}{27}.$$

Se os coeficientes do polinômio de grau 3 são reais, são válidas as seguintes observações, conforme Lima (2006):

- Se $\Delta > 0$, então a equação terá uma raiz real e duas raízes complexas conjugadas;
- Se $\Delta = 0$, então a equação terá três raízes reais, sendo uma repetida;
- Se $\Delta < 0$, então a equação terá três raízes reais e distintas.

Exemplo 31. Vamos determinar as raízes de $y^3 - 6y - 9 = 0$.

Como a equação cúbica já está na forma $y^3 + py + q = 0$, basta aplicarmos a fómula de Cardano - Tartaglia. Veja que,

$$\Delta = \frac{q^2}{4} + \frac{p^3}{27} = \frac{(-9)^2}{4} + \frac{(-6)^3}{27} = \frac{49}{4},$$

como $\Delta > 0$ então $\sqrt{\Delta} = \frac{7}{2}$ e a equação terá uma raiz real e duas raízes complexas conjugadas. Logo suas raízes são:

$$\begin{aligned} y_1 &= \sqrt[3]{\frac{9}{2} + \frac{7}{2}} + \sqrt[3]{\frac{9}{2} - \frac{7}{2}} \\ y_1 &= \sqrt[3]{8} + 1 \\ y_1 &= 3. \end{aligned}$$

Agora vamos encontrar as duas raízes complexas conjugadas

$$\begin{aligned} y_2 &= \omega\sqrt[3]{\frac{9}{2} + \frac{7}{2}} + \omega^2\sqrt[3]{\frac{9}{2} - \frac{7}{2}} \\ y_2 &= \left(\frac{-1}{2} + \frac{\sqrt{3}i}{2}\right)2 + \left(\frac{-1}{2} - \frac{\sqrt{3}i}{2}\right) \\ y_2 &= -1 + \sqrt{3}i - \frac{1}{2} - \frac{\sqrt{3}i}{2} \\ y_2 &= -\frac{3}{2} + \frac{\sqrt{3}i}{2}. \end{aligned}$$

Como as raízes complexas são conjugadas então $y_3 = \overline{y_2} = -\frac{3}{2} - \frac{\sqrt{3}i}{2}$.

Observação 8. Sempre que tivermos uma raíz inteira, pelo algorítmo de Euclides, se 3 é raíz do polinômio $y^3 - 6y - 9 = 0$, então $y - 3$ divide o polinômio. Assim,

$$y^3 - 6y - 9 = (y - 3)(y^2 + 3y + 3).$$

Portanto, as outras duas raízes do polinômio são exatamente as raízes de $y^2 + 3y + 3$.

Exemplo 32. Vamos determinar as raízes do polinômio $x^3 - 6x^2 + 11x - 6 = 0$.

Como o polinômio possui todas as potências, precisamos aplicar o método de Cardano - Tartaglia para obtermos $y^3 + py + q$. Assim,

$$p = b - \frac{a^3}{3} = 11 - \frac{(-6)^2}{3} = -1$$

e

$$q = \frac{2(-6)^3}{27} - \frac{(-6)11}{3} + (-6) = 0.$$

Com isso,

$$y^3 - y = 0 \quad \Rightarrow \quad y(y^2 - 1) = 0,$$

e então $y_1 = 0, y_2 = 1$ e $y_3 = -1$ são raízes do polinômio acima. Logo, as raízes de $x^3 - 6x^2 + 11x - 6 = 0$ são dadas por $x_i = y_i - \frac{a}{3}$, $i = 1, 2, 3$. Substituindo,

$$\begin{aligned} x_1 &= y_1 - \frac{a}{3} = 0 - \frac{(-6)}{3} = 2 \\ x_2 &= y_2 - \frac{a}{3} = 1 - \frac{(-6)}{3} = 3 \\ x_3 &= y_3 - \frac{a}{3} = -1 - \frac{(-6)}{3} = 1. \end{aligned}$$

4.2 Equação de grau 4

Definição 44. *Uma equação quártica ou de grau 4 é toda equação da forma*

$$ax^4 + bx^3 + cx^2 + dx + e = 0,$$

onde $a, b, c, d, e \in \mathbb{C}$, *com* $a \neq 0$.

Para determinar sua resolução utilizaremos o método de Ferrari. Para isso, inicialmente podemos dividir toda equação por a, de modo à torná-la mônica, reescrevendo

$$x^4 + \frac{b}{a}x^3 + \frac{c}{a}x^2 + \frac{d}{a}x + \frac{e}{a}.$$

Logo, basta considerar equações em que o coeficiente do termo de quarto grau igual a 1.

Considere a equação $x^4 + ax^3 + bx^2 + cx + d = 0$, completando o quadrado de forma conveniente.

$$\begin{aligned} x^4 + ax^3 &= -(bx^2 + cx + d) \\ x^4 + ax^3 + \left(\frac{a}{2}x\right)^2 &= \left(\frac{a}{2}x\right)^2 - (bx^2 + cx + d) \\ \left(x^2 + \frac{a}{2}x\right)^2 &= \left(\frac{a^2 - 4b}{4}\right)x^2 - cx - d. \end{aligned} \tag{4.1}$$

Observamos que na equação seria interessante se aparecesse um quadrado perfeito no segundo membro, dessa forma poderíamos tratar o problema a partir de uma equação de grau 2. Para isso, basta somar um número y a $x^2 + \frac{a}{2}$ para aparecer os termos que somaremos na equação acima. Portanto,

$$\left(x^2 + \frac{a}{2}x + y\right)^2 = \left(x^2 + \frac{a}{2}x\right)^2 + 2\left(x^2 + \frac{a}{2}x\right)y + y^2.$$

Então, vamos somar a expressão $2yx^2 + axy + y^2$ a ambos os membros da equação 4.1 e agrupando os termos semelhantes, obtemos

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

Observe que o segundo membro da igualdade é um polinômio de grau 2 em x. Para que esta expressão seja um quadrado perfeito, basta que o delta seja igual a zero, $\Delta = 0$. Vamos analisar a equação:

$$\left[\left(\frac{a^2 - 4b}{4}\right) + 2y\right]x^2 + (ay - c)x + (y^2 - d) = 0.$$

Utilizando a fórmula de Δ para a solução da equação do segundo grau, temos:

$$\Delta = (ay - c)^2 - 4\left[\left(\frac{a^2 - 4b}{4}\right) + 2y\right](y^2 - d) = 0.$$

Se, e somente se,

$$\begin{aligned} (ay - c)^2 - (a^2 - 4b)y^2 + (a^2 - 4b)d - 8y^3 + 8dy &= 0 \\ -8y^3 + 4by^2 + (8d - 2ac)y + \left[c^2 + (a^2 - 4b)d\right] &= 0. \end{aligned}$$

Note que esta última é uma equação cúbica completa cujas raízes já sabemos determinar. Portanto as raízes da equação $x^4 + ax^3 + bx^2 + cx + d = 0$ são dadas pela solução da equação a seguir onde y_1 é uma das três soluções da cúbica acima.

$$\left(x^2 + \frac{a}{2}x + y_1\right)^2 = \left[\left(\frac{a^2 - 4b}{4}\right) + 2y_1\right]x^2 + (ay_1 - c)x + (y_1^2 - d).$$

Onde o segundo membro terá a seguinte forma $(\alpha + \beta)^2$, assim, temos:

$$\left(x^2 + \frac{a}{2}x + y_1\right)^2 = (\alpha + \beta)^2$$

$$x^2 + \frac{a}{2}x + y_1 = \pm(\alpha + \beta).$$

E da última equação saem as raízes da equação geral do 4º grau.

Exemplo 33. Vamos determinar as raízes do polinômio $p(x) = x^4 - 3x^3 - 11x^2 + 3x + 10$

Pelo método de Ferrari, temos:

$$\begin{aligned} x^4 - 3x^3 - 11x^2 + 3x + 10 &= 0 \\ x^4 - 3x^3 &= 11x^2 - 3x - 10, \end{aligned}$$

completando quadrado no primeiro membro,

$$\begin{aligned} \left(x^2 - \frac{3}{2}x\right)^2 &= \frac{9}{4}x^2 + 11x^2 - 3x - 10 \\ &= \frac{53}{4}x^2 - 3x - 10. \end{aligned}$$

Note que a expressão $\frac{53}{4}x^2 - 3x - 10$ não é um quadrado perfeito e portanto, precisaremos encontrar uma expressão de modo que ambos os membros sejam um quadrado perfeito, assim temos:

$$\begin{aligned} \left(x^2 - \frac{3}{2}x + y\right)^2 &= \left(x^2 - \frac{3}{2}x\right)^2 + 2\left(x^2 - \frac{3}{2}x\right)y + y^2 \\ &= \frac{53}{4}x^2 - 3x - 10 + 2x^2y - 3xy + y^2 \\ &= \left(\frac{53}{4} + 2y\right)x^2 - 3(1 + y)x + (y^2 - 10). \end{aligned} \tag{4.2}$$

Observando que o segundo membro é um polinômio quadrático em x, basta pedirmos que o delta seja igual a zero, $\Delta = 0$.

$$\begin{aligned} 0 = \Delta &= [-3(1+y)]^2 - 4\left(\frac{53}{4} + 2y\right)(y^2 - 10) \\ &= -8y^3 - 44y^2 + 98y + 539. \end{aligned}$$

Utilizando a fórmula de Cardano - Tartaglia, uma das raízes do polinômio cúbico acima é $y_1 = \frac{7}{2}$. Substituindo em (4.2), temos

$$\left(x^2 - \frac{3}{2}x + \frac{7}{2}\right)^2 = \frac{1}{4}(9x - 3)^2.$$

Assim, as raízes do polinômio de quarto grau serão as raízes dos polinômios quadráticos:

- $x^2 - 6x + 5 = 0$, com $\Delta = 6^2 - 4 \cdot 1 \cdot 5 = 16$, pela fórmula de Bhaskara:

$$x_1 = 1, \quad x_2 = 5;$$

- $x^2 + 3x + 2 = 0$ com $\Delta = 3^2 - 4 \cdot 1 \cdot 2 = 1$, pela fórmula de Bhaskara:

$$x_3 = -2, \quad x_4 = -1.$$

Com isso, as raízes são $x_1 = 1$, $x_2 = 5$, $x_3 = -2$, $x_4 = -1$.

Um método prático para obtenção de raízes inteiras de polinômios é observar que: **as possíveis raízes inteiras dividem o termo independente**. No polinômio em questão o termo independente é 10, e seus divisores são ± 1, ± 2, ± 5, ± 10. E é de fácil verificação que

$$p(1) = p(-1) = p(-2) = p(5) = 0,$$

como vimos.

4.3 Equação de grau ≥ 5

Vimos nas sessões anteriores que todo polinômio de grau ≤ 4 é solúvel por radicais, como também vimos que nem sempre um polinômio de grau ≥ 5 é solúvel por radicais, por isso não conseguimos uma fórmula generalizada para equações de grau ≥ 5. Mostraremos a seguir uma equação quíntica não solúvel por radicais.

Para melhor compreensão do exemplo, segue o seguinte teorema.

Teorema 45 (Teorema de Rolle)**.** *Dada uma função continua $f(x)$ definida em um intervalo fechado $[a, b]$ e diferenciável em (a, b). Se $f(a) = f(b)$ então existe um ponto c em (a, b) onde a tangente ao gráfico de $f(x)$ é horizontal, isto é,*

$$f'(c) = 0.$$

Exemplo 34. O polinômio $x^5 - 4x + 2 = 0 \in \mathbb{Q}[x]$ não é solúvel por radicais.

Chamaremos de $\mathbb{L} = Gal(f, \mathbb{Q})$, o corpo de decomposição de $f(x)$ e de G seu grupo de Galois. Observe que o critéio de Eisenstein é satisfeito para $q = 2$. Logo, $f(x)$ é irredutível em $\mathbb{Q}[x]$. Considere α uma das raízes de $f(x)$, temos pela Lei da Torre, que: $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$, onde, pela Proposição 33, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, logo $[\mathbb{L} : \mathbb{Q}]$ é múltiplo de 5. E como pelo Teorema 41 $[\mathbb{L} : \mathbb{Q}] = |G|$, então $|G|$ é múltiplo de 5, ou em outras palavras 5 divide $|G|$.

Pelo Teorema de Cauchy, temos que o grupo G possui um elemento de ordem 5. E como se sabe, no grupo S_5, os únicos elementos de ordem 5 de são os 5-ciclos. Logo, sabemos que G possui pelo menos um elemento 5-ciclo.

Como sabemos, $f(x)$ é irredutível sobre $\mathbb{Q}$ e temos ainda que sua primeira derivada é $f'(x) = 5x^4 - 4$. Com isso, como $mdc(f(x), f'(x)) = 1$ então pela Proposição 38 $f(x)$ é separável. Logo, só possui raízes simples.

Agora, fazendo $f(-2) = -38, f(-1) = -3, f(0) = 2, f(1) = -1$ e $f(2) = 18$, uma breve olhada no gráfico de $y = f(x)$ nos dá as posições de cada ponto. Assim, pelo Teorema de Rolle, os zeros de $f(x)$ são separados pelos zeros de $f'(x)$. Além disso, $f'(x)$ tem como zeros reais $\pm\sqrt[4]{\frac{4}{5}}$. Como $f(x)$ é separável, então, f tem no máximo três zeros reais. Mas, certamente f tem no mínimo três zeros reais, já que $f'(x)$ não muda de sinal para números maiores que $\sqrt[4]{\frac{4}{5}}$, ou menores que $-\sqrt[4]{\frac{4}{5}}$. Portanto, f tem precisamente

três zeros reais, logo as outras duas são complexas.

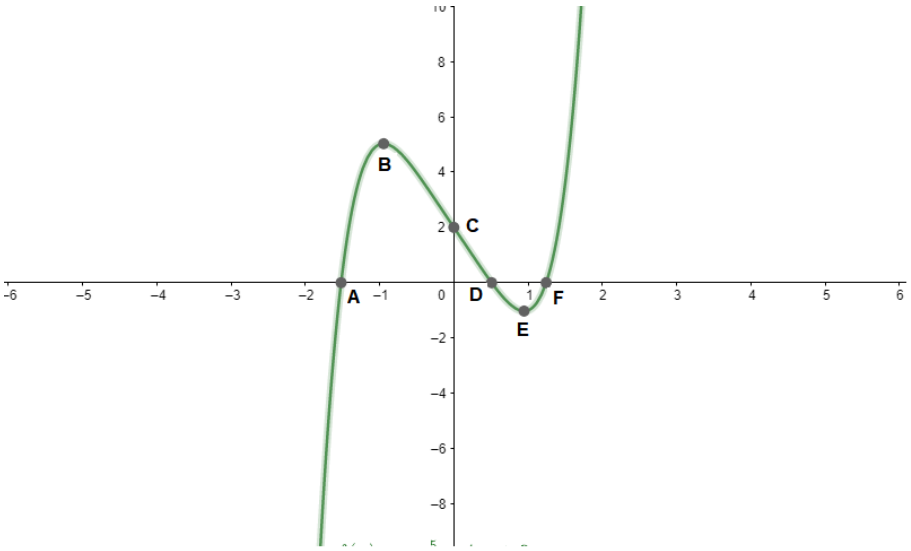


Figura 4.1: $f(x) = x^5 - 4x + 2$

Pelo Teorema 34 existe um automorfismo que leva a raíz complexa de $f(x)$ na outra raíz complexa conjugada e fixa todos os elementos de $\mathbb{L}$ menos as raízes complexas. Sendo assim, associamos este automorfismo a transposição $(12) \in S_5$. Com isso, pelo teorema 2 segue que $G \cong S_5$, que é não solúvel pelo Corolário 16. Logo, G não é solúvel e do Teorema 44 concluímos que $x^5 - 4x + 2 = 0$ não é solúvel por radicais.

Generalizando o exemplo acima, temos o seguinte lema.

Lema 46. *Sejam p um primo e f um polinômio irredutível de grau p sobre $\mathbb{Q}$. Suponhamos que f tenha precisamente dois zeros não reais em $\mathbb{C}$. Então, o Grupo de Galois de f sobre $\mathbb{Q}$ é isomorfo ao grupo simétrico S_p.*

Demonstração. Pelo Teorema Fundamental da Álgebra, $\mathbb{C}$ contém o corpo de decomposição $Gal(f, \mathbb{Q})$, digamos $\mathbb{L}$. Seja $Gal(\mathbb{L} : \mathbb{Q})$ o Grupo de Galois de f sobre $\mathbb{Q}$, considerado como o grupo de permutação nos zeros de f. Estes, são distintos pela Proposição 38, logo, $Gal(\mathbb{L} : \mathbb{Q})$ é isomorfo a um subgrupo de S_p. Seja $\alpha \in \mathbb{C}$ uma raíz qualquer de $f(x)$. Então, $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{L}$. Logo, $p = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ divide $[\mathbb{L} : \mathbb{Q}] = |Gal(\mathbb{L} : \mathbb{Q})|$. Pelo Teorema de Cauchy, $Gal(\mathbb{L} : \mathbb{K})$ tem um elemento de ordem p. Os elementos de ordem p de S_p são p-ciclos. A conjugação complexa é um $\mathbb{Q}$-automorfismo de $\mathbb{C}$ e restrita a $\mathbb{L}$ induz um $\mathbb{Q}$-automorfismo de $\mathbb{L}$, digamos σ. σ fixa as $p - 2$ raízes reais de $f(x)$ e permuta as duas raízes complexas não reais de $f(x)$. Portanto, $Gal(\mathbb{L} : \mathbb{Q})$ tem um 2-ciclo. Podemos supor,

após tomar uma potência do p-ciclo se necessário, que $(1,2),(1,2,\cdots,p) \in Gal(\mathbb{L}:\mathbb{Q})$. Logo, $Gal(\mathbb{L}:\mathbb{Q}) \supset \langle (1,2),(1,2,\cdots,p)\rangle = S_p$. Portanto, $Gal(\mathbb{L}:\mathbb{Q}) = S_p$. □

Exemplo 35. Vamos mostrar que o polinômio $p(x) = x^7 - 6x^6 + 11x^5 - 6x^4 - x^3 + 6x^2 - 12x + 5$ não é solúvel por radicais.

Assim como no Exemplo 34, podemos utilizar o Teorela de Rolle para determinar os intervalos onde se encontram as raízes do polinômio. É de fácil verificação que o polinômio possui exatamente uma raiz em cada um dos intervalos $(-2,0)$, $(0,1)$, $(1,1/2)$, $(1/2,2)$, $(5/3,7/9,4)$ e as raízes restantes devem ser complexas, pelo Teorema fundamental da Álgebra. Como segue o gráfico abaixo

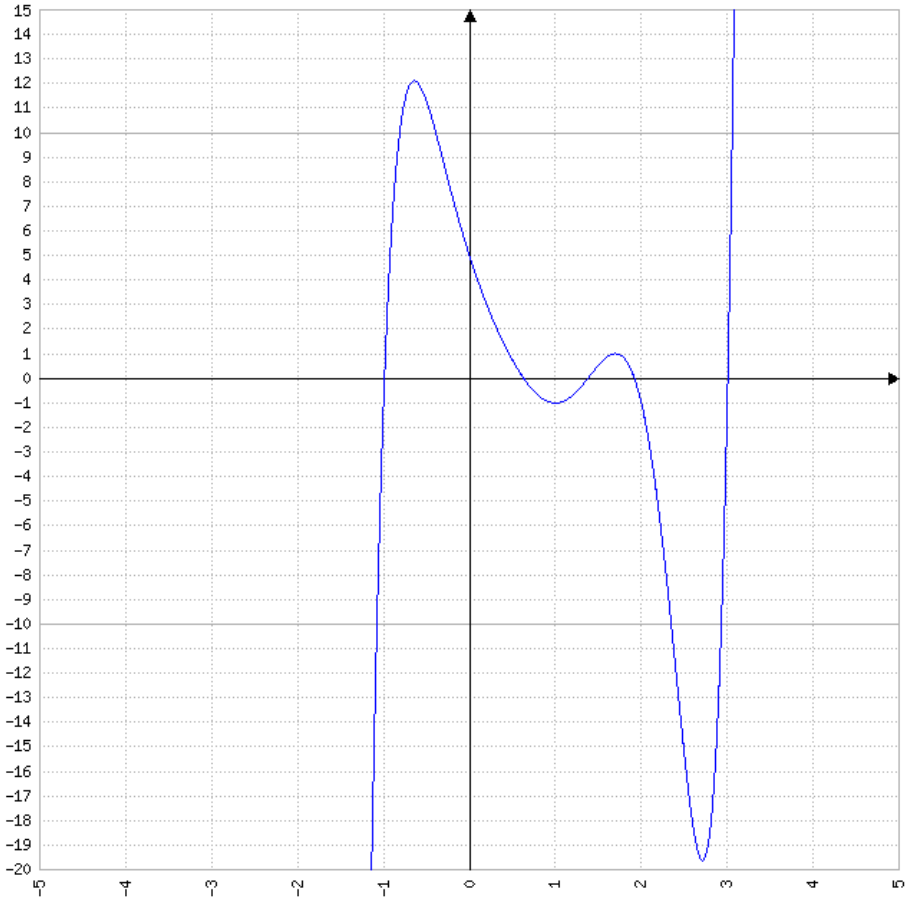


Figura 4.2: $p(x) = x^7 - 6x^6 + 11x^5 - 6x^4 - x^3 + 6x^2 - 12x + 5$

Então, pelo Lema 46 temos que o grupo de Galois associado as raízes do polinômio $p(x)$ é isomorfo a S_7. Portanto, $p(x)$ não é solúvel por radicais.

Exemplo 36. O polinômio $g(x) = x^5 - 5x^4 - 10x^3 - 10x^2 - 5x - 1$ é solúvel por radicais

De fato! Análogo ao Exemplo 34, verificamos que o polinômio $g(x)$ possui apenas

uma raiz real contida no intervalo aberto $(6, 7)$. Sendo assim, pelo Teorema Fundamental da Álgebra, $g(x)$ tem exatamente 4 raízes complexas e pelo Lema 46 o grupo de Galois G associado as raízes é um subgrupo solúvel do grupo de permutações S_5.

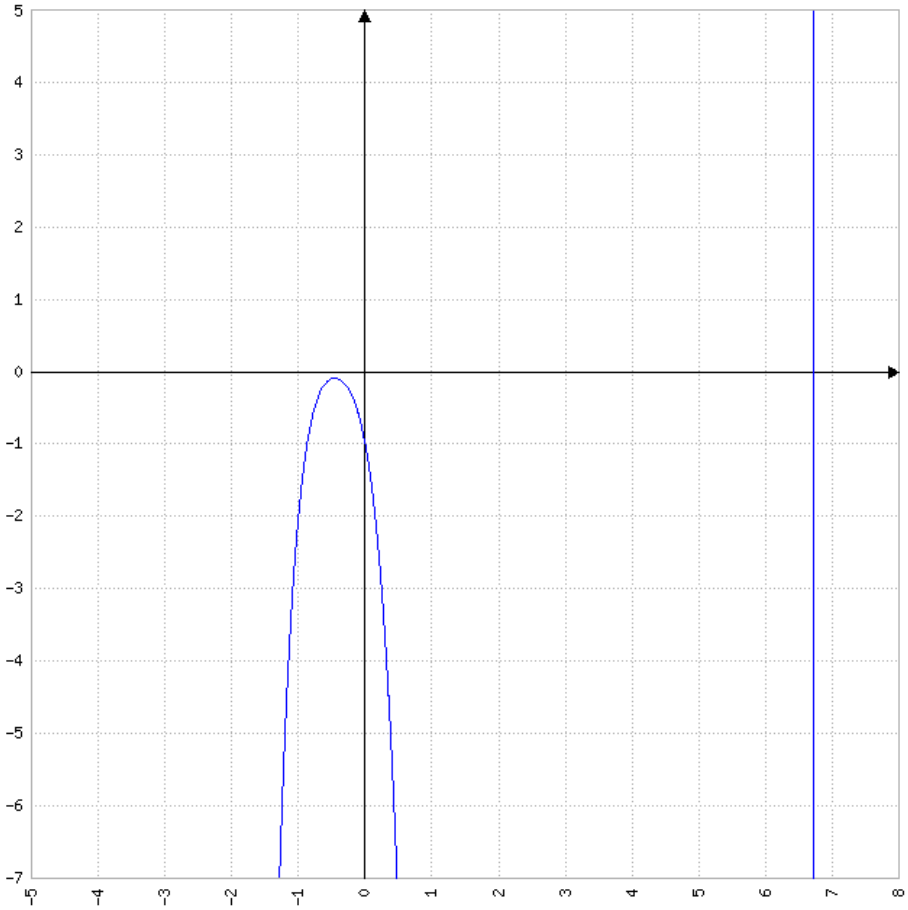


Figura 4.3: $g(x) = x^5 - 5x^4 - 10x^3 - 10x^2 - 5x - 1$

Para calcular o grupo de Galois do polinômio, uma ferramenta interessante é o site Magma, http://magma.maths.usyd.edu.au/calc/. Nele é possível, a partir do polinômio, determinar a ordem do grupo de Galois com o seguinte comando

$R < x >:=$ PolynomialRing (RationalField ());
$f := x\text{^}5 - 5 * x\text{^}4 - 10 * x\text{^}3 - 10 * x\text{^}2 - 5 * x - 1;$
$G :=$ GaloisGroup (f);
G;
IsSolvable (G);

que irá gerar como resposta

Permutation group G acting on a set of cardinality 5
Order = $20 = 2^2 * 5$
$(1, 2, 3, 4)$
$(1, 3)\ (2, 4)$
$(1, 2, 5, 4, 3)$
true

Temos a ordem do grupo de Galois, bem como os elementos que geram o grupo. E por fim a resposta de solubilidade "true", nos informando que tal grupo é solúvel, logo o polinômio é solúvel por radicais.

Concluímos nosso trabalho ressaltando que existem polinômios de grau ≥ 5 que são solúveis por radicais, equações triviais, como $x^5 - 15$ são solúveis por radicais, basta aplicar o Lema 43 para verificar esse fato. Para polinômios não triviais de grau 5 que são solúveis por radicais, suas raízes podem ser encontradas por um método chamada Transformação de Martinelli, este método está muito bem exposto no trabalho do professor Andrade (2019), onde utiliza um pouco das ideias de solubilidade das equações de graus 3 e 4.

Outros trabalhos exibem fórmulas mais gerais para determinação de raízes de polinômio de grau ímpar, por exemplo Cardoso (2016), nele é feito uma generalização do método de Cardano - Tartaglia para polinômios de grau ímpar maior que 3, sempre que solúvel por radicais. Uma abordagem diferente seria tentar determinar as raízes por aproximação e um método muito utilizado é o método de Newton, também mostrado em Cardoso (2016), que consiste em observar o comportamento das retas tangentes ao gráfico do polinômio a partir de um ponto inicial.

Finalizamos o trabalho reiterando a importância do estudo de equações polinomiais desde o ensino básico ao ensino superior. É claro que muito do que foi discutido no trabalho é de difícil aplicação no ensino básico, mas são grandes ferramentas para aprimorar o conhecimento do professor, dando diferentes direções na condução de suas aulas.

Considerações finais

Neste trabalho fizemos o estudo do conjunto solução de equação polinomial e sua solubilidade por radicais. Mostrando as estruturas algébricas adequadas para que uma equação polinomial sempre tenha solução e as condições necessárias para que suas raízes sejam dadas a partir de seus coeficientes.

O estudo de equações polinomiais é fundamental para o desenvolvimento da Matemática. É importante que os professores de Matemática tenham algum conhecimento sobre resolução de equações polinomiais. Pelo menos a parte histórica e os resultados sobre as possibilidades de haver uma fórmula para sua resolução. Isso reflete diretamente na postura do professor e traz mais informações para o aluno, tendo em vista a importância do tema. Diversos problemas do nosso cotidiano nos levam a equações que permitem fazer uma interpretação das possibilidades de tomada de decisão com a análise dos dados.

Durante praticamente toda a educação básica os alunos têm contato com equações polinomiais. Em virtude disso, resolvemos escrever sobre o tema com o objetivo de proporcionar aos professores mais uma ferramenta que possa auxiliar no processo de ensino e aprendizagem.

Referências Bibliográficas

Andrade, R. J. M. B. (2019). URL: https://www.fc.unesp.br/Home/Departamentos/Matematica/revistacqd2228/v16a12-resolucao-de-uma-equacao-do-quinto-grau.pdf. Acesso 26 de novembro de 2020.

Bewersdorff, J. (2006). *Galois Theory for Beginners*. AMS, Rhode Island.

Biazzi, R. N. (2014). Polinômios irredutíveis: Critérios e aplicações. Dissertação de Mestrado, UNESP, Rio Claro/MG.

Boldrini e Figueiredo (1980). *Álgebra Linear*. Harbra, UNICAMP - SP.

Cardoso, L. C. (2016). Solução por radicais de certas equações polinomiais de grau ímpar e método de Newton. Dissertação de Mestrado, UFMS, Três Lagoas/MS.

Cruz, K. B. (2014). Introdução à teoria de galois. trabalho de conclusão de curso. São Carlos: UFSCAR.

Figueiredo, D. G. (2011). *Números Irracionais e Transcendentes*. SBM, Rio de Janeiro.

Gonçalves, A. (2006). *Introdução à Álgebra*. IMPA - Projeto Euclides, Rio de Janeiro.

Hygino e Iezzi, G. (2003). *Álgebra Moderna*. Atual, S. Paulo.

Lima, E. L. (2006). *Meu Professor de Matemática e outras histórias - 2a Edição*. IMPA - Projeto Euclides, Rio de Janeiro.

Santos, A. N. J. (2019). Solução de equações polinomiais por meio de radicais. Dissertação de Mestrado, UFC, Sergipe/AL.

Singh, S. (2014). *O Último Teorema de Fermat*. BestBolso, Rio de Janeiro.