UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

Solubilidade de Equações Algébricas por Radicais

Alan Uchôa Pellejero

Dissertação de Mestrado do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT)

ICMC USP
SÃO CARLOS

Alan Uchôa Pellejero

Solubilidade de Equações Algébricas por Radicais

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências – Mestrado Profissional em Matemática em Rede Nacional. *EXEMPLAR DE DEFESA*

Área de Concentração: Mestrado Profissional em Matemática em Rede Nacional

Orientador: Prof. Dr. Antônio Calixto de Souza Filho

USP – São Carlos
Dezembro de 2023

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

Uchôa Pellejero, Alan
U386s Solubilidade de Equações Algébricas por Radicais / Alan Uchôa Pellejero; orientador Antônio Calixto de Souza Filho. -- São Carlos, 2023.
96 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Matemática) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2023.

1. Álgebra. 2. Teoria de Galois. 3. Equações Algébricas. 4. Solubilidade por Radicais. I. Calixto de Souza Filho, Antônio, orient. II. Título.

Bibliotecários responsáveis pela estrutura de catalogação da publicação de acordo com a AACR2:
Gláucia Maria Saia Cristianini - CRB - 8/4938
Juliana de Souza Moraes - CRB - 8/6176

Alan Uchôa Pellejero

Solubility of Algebraic Equations by Radicals

Master dissertation submitted to the Institute of Mathematics and Computer Sciences – ICMC-USP, in partial fulfillment of the requirements for the degree of Mathematics Professional Master's Program. *EXAMINATION BOARD PRESENTATION COPY*

Concentration Area: Professional Master Degree Program in Mathematics in National Network

Advisor: Prof. Dr. Antônio Calixto de Souza Filho

USP – São Carlos
December 2023

Este trabalho é dedicado à minha esposa Fernanda e à minha filha Brenda.

AGRADECIMENTOS

Ao meu orientador, Prof. Dr. Antônio Calixto de Souza Filho, por ter me apoiado incondicionalmente durante a realização desta dissertação. Sem a sua valorosa contribuição este trabalho jamais teria sido concluído.

À minha amada esposa Fernanda, por ser especial em minha vida, por acreditar em mim e por me incentivar diariamente a querer ser uma pessoa melhor.

À minha amada filha Brenda, por trazer um novo significado à minha vida.

À Sociedade Brasileira de Matemática (SBM), pela oportunidade de fazer parte do PROFMAT — Mestrado Profissional em Matemática em Rede Nacional, programa que tem elevado sobremaneira a qualidade do ensino de Matemática e, por conseguinte, da educação básica brasileira.

À Universidade de São Paulo (USP), pela oportunidade de realizar o sonho de concluir um curso de pós-graduação *stricto sensu* de excelência, nesta que é uma das cem melhores universidades do mundo.

Ao Instituto de Matemática e Estatística (IME/USP), pela oportunidade de participar de tantos Cursos de Verão, os quais foram fundamentais para suprimir muitas lacunas de minha formação matemática básica.

À equipe do Instituto de Ciências Matemáticas e de Computação (ICMC/USP), tanto por terem desenvolvido e disponibilizado um *template* de LaTeXde alta qualidade — a partir do qual esta dissertação foi escrita — quanto pela atenção e cordialidade sempre presentes.

À Faculdade Estadual de Filosofia, Ciências e Letras de Jacarezinho (FAFIJA), da Universidade Estadual do Norte Pioneiro do Paraná (UENP), pela oportunidade de me graduar em Matemática. Em especial, agradeço ao Prof. Luiz Clemente Viana Franco (Prof. Kiko), pelo privilégio de ter sido seu aluno, ocasião em que pude apreciar um pouco mais da beleza desta, que é a rainha das ciências, por meio de seus ensinamentos.

Por fim, registro meus sinceros agradecimentos a todos aqueles que contribuíram de alguma forma para a realização deste trabalho.

"Quando tudo está sob controle é sinal
de que não estamos indo suficientemente rápido."
(Mario Andretti)

RESUMO

PELLEJERO, A. U. **Solubilidade de Equações Algébricas por Radicais**. 2023. 96 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2023.

A Teoria de Galois é considerada um dos principais resultados de Álgebra do século XIX. Sua importância não se resume à beleza da solução encontrada para o problema de resolução de equações algébricas por radicais reais, mas também por introduzir conceitos inovadores que deram origem ao que se conhece hoje por "Álgebra Moderna". A partir de uma contextualização histórica que busca situar o desenvolvimento da matemática em cada época, são apresentados conceitos relacionados à evolução do pensamento matemático e alguns de seus principais resultados. No estudo das equações do primeiro ao quarto grau, são apresentadas as respectivas deduções de suas fórmulas resolutivas. Para equações com grau igual ou superior a cinco, são apresentados conceitos como Grupos, Anéis e Corpos, assim como alguns de seus principais resultados, com o objetivo de provar a insolubilidade de uma equação polinomial de grau $n \geq 5$ por meio de uma abordagem alternativa — na qual não se utilizam conceitos como extensões normais, polinômios irredutíveis ou corpos de decomposição. Como exemplos de aplicação da teoria, são apresentados ao final três problemas clássicos da Geometria — duplicação do cubo, trisseção de um ângulo e quadratura do círculo —, cuja impossibilidade de resolução com régua e compasso somente foi demonstrada a partir da Teoria de Galois.

Palavras-chave: Equações Algébricas, Solubilidade por Radicais, Teoria de Galois.

ABSTRACT

PELLEJERO, A. U. **Solubility of Algebraic Equations by Radicals**. 2023. 96 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2023.

Galois Theory is considered one of the main Algebra results of the 19th century. Its importance is not limited to the beauty of the solution found to the problem of solving algebraic equations using real radicals, but also for introducing innovative concepts that gave rise to what is known today as "Modern Algebra". Based on a historical contextualization that aims to situate the development of mathematics in each era, concepts related to the evolution of mathematical thinking and some of its main results are presented. In the study of equations from the first to the fourth degree, the respective deductions of their solving formulas are presented. For equations with a degree equal to or greater than five, concepts such as Groups, Rings and Fields are presented, as well as some of their main results, with the aim of proving the insolubility of a polynomial equation of degree $n \geq 5$ by means of an alternative approach — in which concepts such as normal extensions, irreducible polynomials or decomposition fields are not used. As examples of the application of the theory, three classic Geometry problems are presented at the end — doubling the cube, trisection of an angle and squaring the circle —, whose impossibility of solving with a ruler and compass was only demonstrated from the Theory of Galois.

Keywords: Algebraic Equations, Solubility by Radicals, Galois Theory.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

CAPÍTULO

1

INTRODUÇÃO

Segundo Highfield (2010), ao fim de sua apresentação em 1860 na *Royal Society*[1] sobre suas recentes descobertas envolvendo a *Eletricidade*, Faraday[2] teria sido interpelado pela rainha Vitória[3] com a seguinte questão:

— *Tudo isto é muito interessante, Sr. Faraday, mas para que serve?*

Faraday então teria respondido:

— *Majestade, para que serve um recém-nascido?*

No âmbito do Ensino Básico, é bastante provável que a maioria dos professores de Matemática já tenha se deparado com uma pergunta do tipo "Para que serve isso, professor?"

Geralmente motivado pela dificuldade que muitos alunos têm de compreender de que forma a Matemática poderá ser útil em suas vidas, esse tipo de questionamento é motivado, em parte, pela pouca aplicabilidade da teoria vista em sala de aula às necessidades práticas do dia a dia. Isso decorre do fato de que o ensino da Matemática nem sempre é contextualizado, tendo pouca ou nenhuma relação com a vivência dos alunos.

No decorrer do estudo da Matemática, é natural que a capacidade de abstração dos alunos seja cada vez mais incentivada — e exigida. Um divisor de águas na vida escolar de qualquer um é quando "os números são substituídos por letras" — uma forma sutil de se referir à álgebra[4].

---

1 Instituição fundada em 1660, em Londres, que se destina à promoção do conhecimento científico.

2 Michael Faraday(1791 - 1867), foi um físico e químico britânico conhecido por suas contribuições em eletromagnetismo e eletroquímica, tendo se notabilizado pela descoberta da indução eletromagnética, a lei da eletrólise, a invenção do motor elétrico e a introdução de conceitos como campo elétrico e linhas de força magnética. É considerado um dos cientistas mais influentes do século XIX.

3 Alexandrina Victoria (1819 - 1901), foi uma monarca do Reino Unido, cujo reinado, conhecido como a Era Vitoriana, foi marcado por uma expansão significativa do Império Britânico, avanços industriais, científicos e culturais, além de mudanças sociais e políticas.

4 Vocábulo derivado do termo árabe *al-jabr*, utilizado pela primeira vez entre os anos de 813 e 833 E.C. pelo matemático persa al-Khwarizmi, personalidade sobre a qual discorreremos mais adiante.

Nesse contexto, consta nos Parâmetros Curriculares Nacionais (PCN) de Matemática a seguinte consideração:

> "Embora nas séries iniciais já se possa desenvolver uma pré-álgebra, é especialmente nas séries finais do ensino fundamental que os trabalhos algébricos serão ampliados, trabalhando com situações-problema, o aluno reconhecerá diferentes funções da álgebra (como modelizar, resolver problemas aritmeticamente insolúveis, demonstrar), representando problemas por meio de equações (identificando parâmetros, variáveis e relações e tomando contato com fórmulas, equações, variáveis e incógnitas) e conhecendo a 'sintaxe' (regras para resolução) de uma equação." (BRASIL., 1997, p. 39)

A apresentação de temas históricos e culturais no processo de ensino e aprendizagem consiste em uma estratégia educacional que possibilita ao aluno vislumbrar outros dimensões do saber matemático além dos aspectos meramente técnicos. Isso contribui não apenas para uma melhor compreensão do assunto, mas também para a formação geral do estudante, haja vista que possibilita relacionar fatos, datas, locais, pessoas e instituições, por exemplo, ampliando assim a sua visão de mundo e, por conseguinte, a sua capacidade de extrair e analisar dados, transformá-los em informações e obter suas próprias conclusões a respeito dos mais variados temas.

O objetivo de tal abordagem é auxiliar os alunos a desmistificar a visão de que a ciência seja algo "pronto", estimulando assim o desenvolvimento de espírito crítico e da criatividade, além da perspicácia e busca por novas descobertas, predicados indispensáveis não apenas àqueles que se dedicam à ciência, mas também para que os alunos possam, agora ou no futuro, saber como identificar os problemas da vida real e buscar meios de resolvê-los. E certamente a Matemática cumpre um papel fundamental nesse propósito.

No que se refere ao desenvolvimento de competências cognitivas, Vygotsky[5] explica:

> "O aprendizado adequadamente organizado resulta em desenvolvimento mental e põe em movimento vários processos de desenvolvimento que, de outra forma, seriam impossíveis de acontecer." (VYGOTSKY, 2002)

[5] Lev Vygotsky (1896 - 1934) foi um psicólogo soviético e uma das figuras mais influentes na psicologia do desenvolvimento do século XX. Conhecido por suas teorias sobre o desenvolvimento cognitivo das crianças, Vygotsky enfatizou a importância crucial das interações sociais e do contexto cultural no desenvolvimento da cognição, introduzindo conceitos fundamentais como a "Zona de Desenvolvimento Proximal", que descreve a diferença entre o que uma criança pode fazer com e sem ajuda, e o processo de "internalização", pelo qual as habilidades sociais são transformadas em funções mentais internas. Suas teorias têm sido amplamente aplicadas na educação, formando a base para novas abordagens no ensino e aprendizagem. Embora suas ideias tenham sido inicialmente censuradas na União Soviética, elas ganharam reconhecimento internacional após sua morte e continuam a influenciar a educação e a psicologia contemporâneas.

Com esse propósito, esta dissertação foi estruturada em três partes:

1. A primeira parte — capítulo dois (Um Pouco de História da Matemática) — é voltada ao público geral, podendo ser lida por alunos de ensino fundamental, médio e superior, e demais interessados no assunto. No capítulo dois, trataremos um pouco da História da Matemática, desde os primórdios da humanidade até o século XIX.

2. A segunda parte — capítulo três (Equações Algébricas) — é voltada para alunos de ensino médio, superior, docentes da educação básica e demais interessados em se aprofundar um pouco mais no assunto. É desejável possuir familiaridade com técnicas matemáticas básicas, sobretudo no que diz respeito às manipulações algébricas que se farão necessárias. Nesse capítulo, abordaremos o contexto histórico das equações e introduziremos as equações de grau um até quatro, apresentando os cálculos para encontrar as respectivas fórmulas resolutivas. Nesse capítulo, a apresentação dos conceitos buscou utilizar uma linguagem mais simples e objetiva, dando ênfase às técnicas empregadas em cada situação considerando-se a época e respectivas ferramentas matemáticas disponíveis.

3. A terceira parte — capítulos 4 (Noções Gerais) e 5 (Solubilidade por Radicais) — é destinada a alunos do ensino superior, docentes da educação básica e demais interessados no assunto. É desejável que o leitor possua familiaridade com técnicas matemáticas mais avançadas, em especial, referentes a demonstração de teoremas e conhecimentos sobre a estrutura axiomática da Matemática. Nesses capítulos, o objetivo é apresentar conceitos e resultados de Álgebra — em especial sobre Grupos, Anéis e Corpos — a fim de preparar o leitor para a compreensão da demonstração de que equações algébricas de grau maior ou igual a cinco não são solúveis por radicais. A abordagem escolhida busca equilibrar os conceitos e resultados que podem ser compreendidos de forma intuitiva com o rigor matemático necessário ao desenvolvimento do assunto, sobretudo no que tange às definições, teoremas e demonstrações.

A apresentação dos tópicos de forma contextualizada à História da Matemática tem por finalidade conduzir o leitor através de uma fascinante viagem no tempo, a qual se inicia nos primórdios da humanidade — com as primeiras evidências de contagem e realização de cálculos[6] — até o desenvolvimento de poderosas teorias matemáticas no século XIX, tais como a Teoria de Galois.

[6] De origem latina, a palavra *calculus* significa *pequena pedra*. Essa denominação decorre da utilização histórica de pedras pequenas (ou seixos) para contar e realizar operações aritméticas, uma prática comum nas antigas civilizações romana e grega. Ainda hoje se utiliza a palavra "cálculo" com esse significado, por exemplo, quando se diz "cálculo renal", popularmente conhecido por "pedra no rim".

CAPÍTULO

2

UM POUCO DE HISTÓRIA DA MATEMÁTICA

Para que possamos entender a condição humana à época dos primeiros registros matemáticos de que se tem notícia, iremos considerar a abordagem da questão dada por Struik (2012):

> "As primeiras concepções de número e forma remontam ao Paleolítico Superior, quando os homens viviam em pequenos grupos, sob condições pouco diferentes das que viviam os animais, e seu sustento era obtido sobretudo pela coleta de alimentos. Eram grupos de nômades que, com o passar do tempo, criaram ferramentas básicas, inclusive artigos para pescar e caçar, e desenvolveram processos rudimentares para se comunicarem uns com os outros. Mais adiante, passaram a transmitir seu legado e sua cultura através de estátuas e pinturas em cavernas". (STRUIK, 2012, p. 9)

Alguns desses registros em cavernas[1] datam de mais de 15 mil anos e sugerem pinturas rupestres com motivação cerimonial. O que interessa, do ponto de vista matemático, é que já nessas figuras se observa a capacidade de reproduzir formas planas e espaciais, o que evidencia habilidades cognitivas e de abstração.

A despeito da dificuldade que existe em precisar quando os seres humanos começaram a utilizar conscientemente a Matemática em seu benefício próprio, é indiscutível que o seu domínio permitiu atingir patamares cada vez mais elevados de desenvolvimento e cognição.

[1] As mais famosas são *Chauvet* e *Lascaux*, na França, e *Altamira*, na Espanha.

Adicionalmente, Courant e Robbins (2000) [2,3] mencionam:

> "Matemática, como expressão da mente humana, reflete a vontade ativa, a razão contemplativa, e o desejo da perfeição estética. Seus elementos básicos são a lógica e a intuição, a análise e a construção, a generalidade e a individualidade. Embora diferentes tradições possam enfatizar diferentes aspectos, é somente a influência recíproca destas forças antitéticas e a luta por sua síntese que constituem a vida, a utilidade e o supremo valor da Ciência Matemática."(COURANT; ROBBINS, 2000)

2.1 África

Osso de Lebombo

Segundo Darling (2004), o "Osso de Lebombo" é um dos mais antigos artefatos matemáticos de que se tem notícia. Descoberto na década de 1970, nos Montes Libombos, na Suazilândia, e datado de mais de 30 mil anos atrás.

Trata-se de uma fíbula de babuíno, na qual se observa vinte e nove entalhes feitos para representação de um calendário lunar, que ainda hoje é utilizado por alguns clãs de bosquímanos da Namíbia.

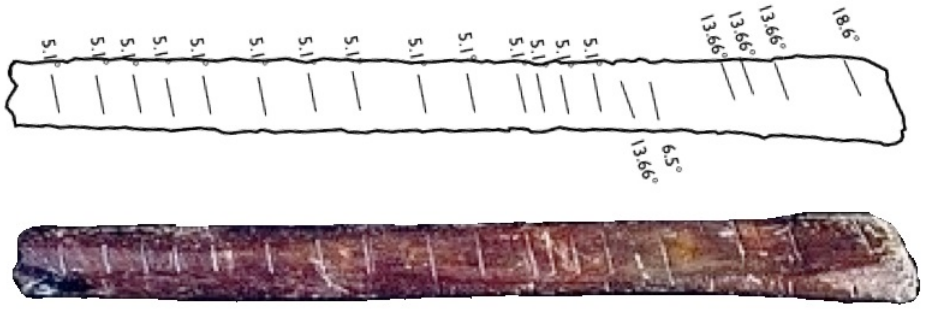


Figura 1 – Osso de Lebombo.

Fonte: Darling (2004, p. 184)

Osso de Ishango

Datado do Paleolítico Superior, o Osso de Ishango consiste em uma fíbula de babuíno com um pedaço de quartzo incrustado na ponta, o qual se supõe ter sido utilizado para gravar ou escrever.

[2] Richard Courant (1888 – 1972), matemático teuto-americano autor de diversos livros didáticos, tais como o *Métodos da Física Matemática*, em coautoria com David Hilbert.

[3] Herbert Ellis Robbins (1915 - 2001) matemático e estatístico estadunidense, conhecido por suas contribuições em estatística, teoria da decisão e teoria dos jogos.

Encontrado em Ishango, na atual República Democrática do Congo, na década de 1960 pelo geólogo Jean de Heinzelin de Braucourt (1920 - 1998), acredita-se que tenha mais de 11 mil anos, sendo considerado um dos mais antigos objetos matemáticos de que se tem notícia.

Como se pode observar na imagem a seguir, foram feitos entalhes em linhas, sendo que a primeira consistente com um sistema numérico com base decimal; a segunda, constando de uma lista de números primos entre dez e vinte; e a terceira contendo entalhes assemelhados a um método de multiplicação por dois, o qual coincide com um posteriormente utilizado pelos egípcios. Marcações adicionais sugerem que o osso também foi usado como um contador de fases lunares.

Figura 2 – Osso de Ishango.

Fonte: Bangura (2011, p. 13)

2.2 Mesopotâmia

A região conhecida por *Mesopotâmia*[4], considerada o berço da civilização, designa mais uma extensão geográfica do que um povo ou uma unidade política. Foi lá que os povos sumérios, acádios, assírios e babilônios promoveram algumas das realizações mais importantes da História da Humanidade, tais como a invenção da roda (ANTHONY, 2010), o desenvolvimento da escrita (RUDGLEY, 2000) e da agricultura (GRANTHAM, 1998).

O crescimento da agricultura, em particular, cumpriu um papel fundamental para o desenvolvimento da Matemática, de tal forma que (GARBI, 2009, p. 7) considera, inclusive, que a Matemática seja fruto direto da Revolução Agrícola[5].

Isso porque, ao invés de caçar, pescar e coletar, o homem passou a cultivar seu próprio alimento, necessitando de mecanismos que propiciassem o melhor aproveitamento das terras.

[4] A *Mesopotâmia* — palavra que significa, em grego antigo, “entre rios”— é o nome dado à área do sistema fluvial Tigre-Eufrates, no atual território do Iraque.

[5] Revolução Agrícola, Revolução Neolítica ou Transição Demográfica Neolítica, foi a transição em grande escala de muitas culturas humanas, em torno de 10 mil anos atrás, o que alterou sobremaneira o estilo de vida de caçador-coletor e nômade adotado até então para agrícola e sedentário, tornando possível um aumento populacional sem precedentes na história da humanidade.

Muitos avanços observados nesse período encontram relação direta com a atividade agrícola: a criação de calendários lunares, o desenvolvimento de sistemas primitivos de numeração e o aperfeiçoamento de técnicas de administração da vida comum são alguns exemplos que fomentaram o uso de rudimentos matemáticos como importante ferramenta para planejamento, controle e execução de atividades quotidianas.

À medida que as populações começaram a se organizar em função desse novo estilo de vida sedentário, muitas cidades passaram a ter uma importância econômica fundamental, funcionando como entrepostos comerciais. Desse modo, novas necessidades foram surgindo, o que fomentou o desenvolvimento de conhecimentos matemáticos cada vez mais complexos (EVES, 2004, p. 52–56).

Eventualmente, a produção poderia se mostrar insuficiente em um determinado local, enquanto em outros poderia haver excedentes que poderiam ser negociados. Esse tipo de comércio primitivo, denominado "escambo", provavelmente já havia sido realizado pelos primeiros hominídeos, mas foi consideravelmente ampliado com o advento do comércio. Essa dinâmica promoveu um longo processo de urbanização da humanidade e intensificou o comércio entre as pessoas, as quais passaram a se relacionar com povos cada vez mais distantes e se concentrar em grandes cidades, onde seria, em teoria, mais fácil desenvolver atividades comerciais.

Nesse contexto, segundo Boyer e Merzbach (2019, p. 40), surgem as primeiras formas de escrita Matemática na Mesopotâmia, por volta do final do quarto milênio a.E.C.[6], na cidade de Uruk, no atual Iraque. Esta escrita primitiva evoluiu a partir de um sistema de símbolos usados para registrar quantidades para fins comerciais e administrativos, sendo que os primeiros registros matemáticos incluíam marcas feitas em tábuas de argila para contabilizar, por exemplo, mercadorias como grãos e gado.

Associar um mesmo número para expressar quantidades iguais de coisas distintas é uma habilidade que demonstra uma considerável capacidade de abstração, embora o ato de contar, por si só, possa ser considerado concreto (ROQUE, 2012, p. 39).

À medida que as civilizações mesopotâmicas — como os sumérios, acádios, babilônios e assírios — se desenvolviam, também evoluíam seus sistemas de escrita e de notação Matemática. Por volta de 3.000 a.E.C., os sumérios já tinham desenvolvido um sistema numérico sofisticado com base sexagesimal, o que influenciou profundamente a Matemática subsequente, de modo que ainda hoje contamos o tempo e medimos ângulos com base nesse sistema.

Os babilônios — que se seguiram aos sumérios — expandiram esse sistema e desenvolveram métodos avançados de aritmética e álgebra. Eram capazes de resolver equações, criaram tabelas de multiplicação para facilitar os cálculos e desenvolveram conceitos geométricos e trigonométricos inovadores para a época. Muitos de seus métodos e descobertas foram preserva-

[6] No decorrer deste texto, será utilizado "antes da Era Comum" e "depois da Era Comum", no lugar de "antes de Cristo" e "depois de Cristo".

dos em tábuas de argila e constituem alguns dos registros matemáticos mais antigos e valiosos, servindo de objeto de estudo para diversos pesquisadores que buscam compreender melhor a história daquele período.

Uma das principais contribuições dos mesopotâmios, segundo Roque (2012, p. 57), foi a criação do sistema sexagesimal, desenvolvido pelos sumérios por volta de 3.000 a.E.C. e adotado posteriormente pelos babilônios. Ainda hoje esse sistema é utilizado para medir tempo e ângulos.

Tabletes Numéricos Sumérios

Os sumérios habitaram a região da Mesopotâmia entre 6.500 e 2.000 a.E.C. e foram os responsáveis por vários avanços em Matemática, muitos dos quais registrados em tabletes de argila encontrados em excelente estado de conservação. Nesses tabletes, foram encontrados registros numéricos utilizando-se o sistema sexagesimal de contagem, além de diversos problemas de geometria e alguns considerados "algébricos" que — diferentemente do conceito atual, relacionado a equações — eram resolvidos por meio de uma série de instruções do tipo "faça isto", "faça aquilo" e "este é o resultado", sendo que tais instruções geralmente eram apresentadas sem qualquer justificativa (GARBI, 2011, p. 13).

Embora não haja um consenso com relação à motivação dos sumérios para desenvolver um sistema de numeração em base sexagesimal, especula-se que podem ter sido motivados pela quantidade de divisores de 60 [7] ou pela união de dois sistemas de contagens: o de base 5, em função da contagem dos dedos das mão; e o de base 12, que utilizava o método das três falanges[8].

Alguns dos principais tabletes numéricos sumérios são:

1. **Tablete Plimpton 322**: É um dos mais famosos tabletes utilizados no período babilônico. Catalogado sob o número 322 da coleção G.A. Plimpton, da Universidade Columbia, foi escrito no período babilônico antigo, provavelmente entre 1.900 e 1.600 a.E.C.

Figura 3 – Tablete Plimpton 322.

Fonte: Roque (2012, p. 57)

[7] São divisores positivos de 60 os números $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30$ e 60.

[8] Com exceção do polegar, as falanges dos dedos da mão direita eram utilizadas de modo a totalizar doze falanges e, com os dedos da mão esquerda, contavam-se as dúzias, totalizando 5 dúzias, ou seja, 60.

2. **Tablete YBC 7289**: É um pequeno tablete de argila, datado de cerca de 1800 a.E.C., famoso por conter um esboço aproximado de um quadrado junto com suas diagonais, mostrando um cálculo de $\sqrt{2}$ com precisão de quatro dígitos sexagesimais, o que equivale a seis dígitos decimais, sendo um feito bastante notável para a época.

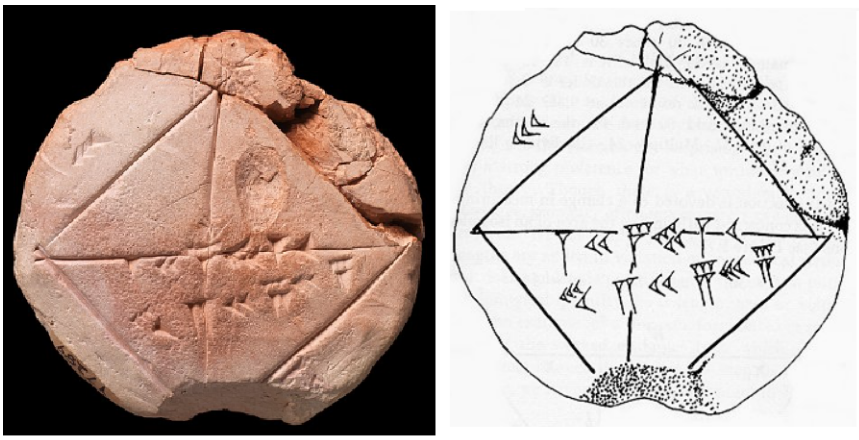


Figura 4 – Tablete YBC 7289 e ilustração.

Fonte: Roque (2012, p. 62)

3. **Tabletes da Série BM 15285 (Tabletes de Babilônia)**: Esses tabletes são uma coleção de 24 tabletes de argila que contêm listas de triângulos pitagóricos, ou seja, conjuntos de três números inteiros a, b e c que satisfazem a relação $a^2 + b^2 = c^2$.

4. **Tablete de Susa (Louvre Sb 29)**: Este tablete, encontrado em Susa, no atual Iraque, é importante por seu conteúdo relativo à álgebra, contendo problemas de equações quadráticas.

5. **Tablete AO 8862 (também conhecido como Tablete de Tell Harmal)**: Encontrado em Tell Harmal, em Bagdá, no Iraque, este tablete mostra problemas de álgebra e equações lineares, demonstrando o uso prático da Matemática para questões cotidianas e comerciais.

De acordo com Boyer e Merzbach (2019, p. 43-45), os babilônios possuíam uma tabulação para valores de $n^3 + n^2$ para valores inteiros de n. Com base nessa tabela, era possível resolver uma série de equações de terceiro ou quarto grau.

Um exemplo de problema pede o lado de um quadrado se a área menos o lado é igual a a 14,30. A solução desse problema equivale a resolver a equação $x^2 - x = 870$, por meio dos seguintes passos, que consideram a base sexagesimal:

1. Tome a metade de 1, que é 0;30
2. Multiplique 0;30 por 0;30, o que dá 0;15
3. Some isto a 14,30, o que dá 14,30;15
4. Isto é o quadrado de 29;30
5. Some 0;30 a 29;30
6. Obtenha 30 como resultado, que é o lado do quadrado

A solução apresentada equivale à fórmula $x = \sqrt{\left(\frac{p}{2}\right)^2 + q} + \frac{p}{2}$ para uma raiz da equação $x^2 - px = q$.

Igualmente surpreendente ao fato de que tudo isso foi feito sem utilizar a moderna notação algébrica é considerar que mesmo para equações de graus superiores tais como $ax^4 + bx^2 = c$ e $ax^8 + bx^4 = c$ eram reconhecidas como sendo apenas equações quadráticas em x^2 e x^4 sendo, portanto, passíveis de resolução por meio das técnicas usualmente empregadas.

2.3 Antigo Egito

Os primeiros assentamentos humanos no Antigo Egito datam de cerca de 6 mil anos a.E.C.. Já nos registros datados dessa época, se encontram estudos sobre estações do ano e fases lunares, com propósitos agrícolas e religiosos. Entretanto, segundo Roque (2012, p. 38), fontes indicam que, quando a Matemática começou a ser praticada no antigo Egito, estava associada sobretudo a necessidades administrativas.

Tal afirmação é corroborada por Garbi (2011, p. 12), que menciona que, no Egito Antigo, a Matemática era usada principalmente para fins práticos, como arquitetura e agrimensura. O famoso papiro de *Rhind*, datado de cerca de 1650 a.E.C., é um dos primeiros documentos conhecidos a mostrar o uso de operações aritméticas e equações lineares. Nesse documento, são apresentados 85 problemas de Aritmética e Geometria, mostrando as respectivas resoluções sem, no entanto, justificá-las.

Com as cheias do rio Nilo, as demarcações de terra para atividades agrícolas se perdiam, tendo sido necessário desenvolver formas de assegurar que as propriedades fossem devidamente remarcadas após cada período de cheia. Esta necessidade prática motivou o estudo e desenvolvimento daquilo que hoje se denomina "trigonometria"[9].

Segundo Roque (2012, p. 73), antes da unificação do Egito sob o regime dos faraós, por volta de 3.000 a.E.C., os egípcios já utilizavam o sistema decimal, embora não fosse posicional.

A representação numérica era feita por barras verticais para números de 1 a 9. Para as potências de dez em diante, eram atribuídos símbolos conforme mostrado na figura abaixo:

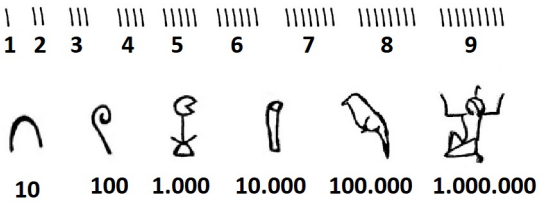


Figura 5 – Sistema de Numeração Egípcio.

Fonte: Roque (2012, p. 73)

[9] A palavra *trigonometria* é proveniente da justaposição dos seguintes radicais gregos: *tri*, que significa "três"; *gono*, que significa "ângulo" e *metria*, que significa "medida".

Um aspecto notável da Matemática egípcia era o seu caráter prático. Isso porque os egípcios se concentravam em técnicas e algoritmos para resolver problemas geralmente relacionados a situações do cotidiano. Isso fica evidente no *Papiro Rhind*, um dos mais famosos documentos matemáticos do Egito Antigo, que contém uma coleção de problemas e soluções práticas.

A aritmética egípcia também incluía um sistema para lidar com frações. Os egípcios usavam frações unitárias — ou seja, frações com numerador igual a um — e desenvolveram métodos para trabalhar com essas frações em cálculos relativamente complexos.

Papiro Rhind (ou de Ahmes)

Segundo Darling (2004, p. 272-273) é o mais extenso documento egípcio que trata de Matemática que se tem conhecimento e é uma cópia de outro papiro do século XIX a.E.C., que foi perdido. O escriba Ahmes[10] foi responsável por reescrevê-lo e hoje o Papiro Rhind é um dos mais antigos documentos ainda existentes de Matemática. O egiptólogo escocês Alexander Rhind (1833 - 1863) o adquiriu no Egito e o levou ao Reino Unido, onde está exposto no museu britânico de Londres. Nesse papiro, há cerca de 80 problemas de Matemática resolvidos que, em sua maioria, tratam de assuntos ordinários tais como preço do pão, alimentação do gado e armazenagem de grãos.

Figura 6 – Questão geométrica no Papiro Rhind (ou de Ahmes) (1.650 a.E.C).

Fonte: Garbi (2011, p. 13)

[10] Também conhecido por Amósis, escriba do Antigo Egito e escreveu o papiro de Rhind em cerca de 1.650 a.E.C., sendo considerado o mais antigo contribuidor da Matemática cujo nome é conhecido.

Papiro de Moscou (ou de Golonishev)

Segundo Garbi (2011, p. 15), trata-se de um papiro matemático egípcio, também conhecido por *Papiro de Golonishev* em alusão a seu primeiro proprietário fora do Egito, o egiptologista Vladimir Golenishchev[11], que o comprou em 1892 na cidade egípcia de Tebas. Atualmente exposto no Museu Pushkin, em Moscou, o Papiro de Moscou data da 13ª Dinastia Egípcia[12], cerca de 1850 a.E.C. Nele, constam cerca de 25 problemas matemáticos e respectivas soluções. Dos problemas tratados neste papiro, destacam-se os que envolvem cálculo de comprimento de leme e do mastro de navios e cálculo do volume de tronco de pirâmide. O problema 19, por exemplo, pede para que se determine a quantidade que, somando-se a sua metade, mais quatro, tem como resultado o número 10. Em notação atual, seria o equivalente a calcular o valor de x tal que $x+\frac{x}{2}+4=10$.

Outro exemplo interessante é o problema 14, cujo enunciado aproximado seria:

Um campo tem a forma de um trapézio. A largura no topo é de 6 khet e na base de 4 khet. A altura do campo é de 20 khet. Qual é a área do campo?

Para resolver a questão, aplicamos a fórmula da Área de um Trapézio (A_T):

$$A_T = \frac{\text{Base maior} + \text{Base menor}}{2} \times \text{Altura} = \frac{(6+4)}{2} \times 20 = 100 \text{ khet}^2.$$

Portanto, a área do campo em forma de trapézio é de 100 khet quadrados.

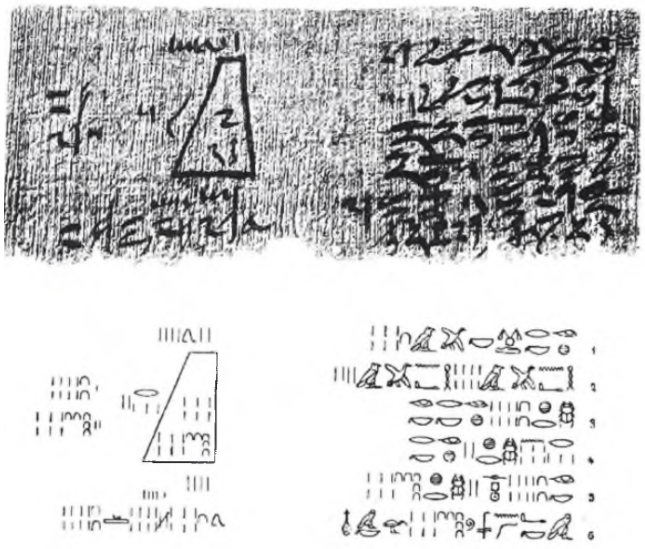


Figura 7 – Problema 14 do papiro Moscou.

Fonte: Eves (2004, p. 86)

[11] Vladimir Golenishchev (1856 – 1947) egiptólogo russo conhecido por suas contribuições ao estudo da civilização egípcia antiga e se tornou famoso por sua coleção de artefatos egípcios antigos, uma das maiores e mais importantes coleções privadas do mundo na época

[12] A 13ª Dinastia Egípcia é marcada pela invasão dos Hicsos no Egito, povo responsável pela introdução de cavalos naquele país.

Como se pode observar, trata-se de uma questão bastante simples, sendo necessário conhecimento básico de geometria do ensino fundamental para resolvê-la.

Uma técnica comumente empregada para resolução de problemas matemáticos era o que hoje se conhece por *"Falsa Posição"*[13]. Nesse método, as quantidades desconhecidas nos problemas, que hoje denominamos incógnitas, eram chamadas de "montão".

Eis um exemplo de problema a ser resolvido pelo referido método:

Exemplo 2.3.1. A idade de Hórus, contada duas vezes, somada à sua metade, à sua terça parte e à sua quarta parte resulta em 74. Qual a idade da Hórus?

Solução:

Seja x a idade de Hórus. Em notação atual, teríamos:

$$2x + \frac{x}{2} + \frac{x}{3} + \frac{x}{4} = 74. \tag{2.3.1}$$

Consideremos o número 12 como sendo o *"Falsa Posição"*, por ser divisível por 2, 3 e 4, que são os denominadores das frações envolvidas no enunciado do problema:

$$2 \times 12 + \frac{12}{2} + \frac{12}{3} + \frac{12}{4} = 24 + 6 + 4 + 3 = 37. \tag{2.3.2}$$

Segundo o enunciado, o resultado obtido diverge do informado. Nesse caso, teríamos então a seguinte correspondência, que pode ser resolvida por *Regra de Três Simples*[14]:

Tabela 1 – Método da "Falsa Posição"

Montão	Resultado
12	37
x	74

Realizando-se os cálculos, obtemos $37x = 74 \times 12$ então $x = 24$, de onde se conclui que Hórus teria 24 anos de idade.

[13] Tal método foi utilizado pelo Matemático Girolamo Cardano (1501-1576), de quem falaremos mais adiante, na tentativa de obter soluções para Equações Algébricas. Esse método deu origem ao que hoje se conhece por *Interpolação Linear*.

[14] Embora as relações entre proporções sejam conhecidas desde a Antiguidade, a aplicação sistemática para resolução de problemas matemáticos se deu a partir da introdução, pelos árabes, da regra de três na Europa durante a Idade Média, tendo sido difundida no séc. XIII por Leonardo de Pisa, também conhecido por *Fibonacci*, em seu livro *Liber Abaci*, de 1202.

2.4 Grécia Antiga

Segundo Garbi (2009, p. 7), a palavra Matemática é proveniente de um radical grego que significa "saber" e era compreendida como "aquilo que é ensinado".

Considerado um dos Sete Sábios da Grécia Antiga, Tales de Mileto[15], foi o pensador a romper com a mitologia para explicar fenômenos naturais. Por essa atitude, é frequentemente considerado o primeiro cientista da história.

O pouco que se sabe sobre sua biografia é conhecido principalmente através de relatos de historiadores posteriores, como Aristóteles[16] e Heródoto[17], pois não há registros originais de sua autoria que tenha chegado aos dias atuais.

Tales é frequentemente considerado um dos primeiros matemáticos da história do pensamento ocidental. Na geometria, é conhecido por suas diversas contribuições, dentre as quais se destaca o famoso *Teorema de Tales*. É atribuída a Tales, também, o cálculo da altura das pirâmides do Egito, onde se supõe que ele tenha sido educado.

Figura 8 – Grande Pirâmide de Gizé (Quéops), no Egito.

Fonte: o autor.

Na astronomia, é considerado o primeiro ser humano a ser capaz de prever um eclipse solar total, o qual teria ocorrido no ano de 585 a.E.C., a partir de conhecimentos astronômicos que ele teria obtido em uma viagem à Babilônia.

Além disso, foi um importante filósofo, precursor da teoria de que a água era a origem de

[15] Tales de Mileto (624 - 548 a.E.C) astrônomo, filósofo e matemático grego.
[16] Aristóteles (384 - 322 a.E.C.) filósofo e cientista grego, sendo considerado um dos mais influentes na história do pensamento ocidental.
[17] Heródoto (c. 484 - 425 a.E.C.) historiador e geógrafo grego, considerado o "Pai da História".

todas as coisas. Dentre seus principais discípulos, destacam-se Anaximandro[18] e Anaxímenes[19].

Tales era também um comerciante muito bem-sucedido, tendo boa parte de sua fortuna sido obtida após prever uma colheita extraordinária de azeitonas com razoável antecedência, o que lhe permitiu adquirir grandes quantidades de prensas, as quais posteriormente foram utilizadas na produção de azeite, rendendo-lhe uma pequena fortuna.

Dentre os matemáticos da Grécia Antiga, talvez Pitágoras[20] seja um dos mais conhecidos em virtude de seu teorema sobre triângulos retângulos — um dos resultados mais importantes da geometria básica. Igualmente célebres são suas contribuições à filosofia e à música.

A Pitágoras também se credita um papel significativo na fundação conceitual das *Sete Artes Liberais*, compostas por *Trivium* e *Quadrivium*[21] — as quais se tornariam a base da educação na Europa medieval. Enquanto no *Trivium* eram estudadas as disciplinas de gramática, retórica e lógica (ou dialética) — cuja natureza do conhecimentos era considerada elementar —, o *Quadrivium* incluía disciplinas consideradas avançadas, no caso, aritmética, geometria, música (teoria musical) e astronomia. Dessa acepção, surge a palavra "trivial" para se referir a algo demasiadamente simples.

Figura 9 – Afresco retratando a Escola de Atenas, de autoria de Rafael Sanzio (1509-1510)

Fonte: Janson e Janson (2004)

[18] Anaximandro (610 - 546 a.E.C.) filósofo, geógrafo e astrônomo grego pré-socrático, considerado um dos primeiros pensadores a propor uma visão racional e científica do mundo.

[19] Anaxímenes (585 - 528 a.E.C.) filósofo grego pré-socrático, conhecido por ser um dos três filósofos jônicos principais, ao lado de Tales e Anaximandro, sendo seu discípulo e sucessor.

[20] Pitágoras (c. 570 – 495 a.E.C.) filósofo e matemático grego antigo, considerado um dos mais importantes da Grécia Antiga.

[21] *Trivium* e *Quadrivium* significam, em latim, "o cruzamento e articulação de três (ou quatro) ramos ou caminhos", respectivamente.

Pitágoras é conhecido também por ser o fundador da Escola Pitagórica, sociedade na qual seus membros, denominados pitagóricos[22] se referiam a si mesmos por *mathematikoi*, em oposição àqueles que eram ouvintes, os quais eram chamados de *akousmatikoi*.

Cerca de dois séculos adiante, temos a figura de Euclides[23], conhecido principalmente por sua obra "os Elementos", um compêndio abrangente que serviu como base para o ensino de Matemática, especialmente a geometria, até o início do século XX. Embora detalhes específicos sobre sua vida sejam escassos, acredita-se que Euclides tenha atuado principalmente em Alexandria, no Egito, onde teve acesso a importantes obras a partir das quais se supõe que ele tenha sistematizado o conhecimento da época em uma estrutura lógica e rigorosa, estabelecendo axiomas e postulados a partir dos quais são deduzidos os teoremas.

Nessa obra de treze volumes, Euclides abordou não apenas conceitos de geometria, mas também tópicos de teoria dos números, sendo notável o "Teorema de Euclides", que trata da infinitude dos números primos.

Nesse sentido, Boyer e Merzbach (2019, p. 118) complementa:

> "Os Elementos de Euclides não apenas foi o mais antigo trabalho matemático a sobreviver até nós, mas foi também o maior livro didático de todos os tempos. (...) As primeiras versões impressas dos Elementos apareceram em Veneza em 1482, um dos primeiros livros de Matemáticas a serem feitos em tipos; tem sido estimado desde então pelo menos mil edições foram publicadas. Talvez nenhum outro livro, com a exceção da Bíblia, podem se gabar de tantas edições, e certamente nenhuma obra de Matemática teve influência comparável à dos Elementos de Euclides." (BOYER; MERZBACH, 2019)

Segundo Sant'anna (2003, p. 2), não são atribuídas a Euclides conquistas Matemáticas significativas, mas sim contribuições creditadas a outros matemáticos, tais como Pitágoras e Hipócrates de Chios[24], de modo que a importância do trabalho de Euclides reside na organização do conhecimento matemático da época, o qual foi apresentado em sua obra "Os Elementos".

Por volta do século III a.E.C., o mundo conheceu um de seus maiores pensadores de todos os tempos: o gênio Arquimedes[25]. Dentre suas contribuições à Matemática, destacam-se a criação do método exaustivo, considerado precursor da integração, assim como seus estudos em

[22] A Escola Pitagórica, fundada por Pitágoras, foi uma corrente da filosofia grega, com tendências místico-religiosas e científico-racionais e cuja influência estende-se até a atualidade.

[23] Euclides (c. 300 a.E.C. - ??) matemático grego antigo, considerado o "o pai da Geometria".

[24] Hipócrates de Chios (c. 470 a.E.C – 410 a.E.C.) matemático grego antigo, notável por suas contribuições à geometria. Conhecido por seu trabalho em quadraturas — ou seja, a tentativa de encontrar áreas equivalentes, especialmente a quadratura de lunulas (regiões em forma de crescente formadas pela interseção de dois círculos) — a ele também é creditada a primeira tentativa sistemática de resolver o problema clássico da duplicação do cubo.

[25] Arquimedes (c. 287 – 212 a.E.C.) matemático, físico, engenheiro, inventor e astrônomo grego antigo, considerado um dos maiores cientistas da antiguidade.

geometria plana e sólida, destacando-se o estudo das espirais, a quadratura da parábola e estudos sobre esfera e cilindro.

Arquimedes aplicou seus métodos matemáticos para resolver problemas práticos, que muitas vezes envolviam a formulação e solução de equações relacionadas às leis físicas. Por exemplo, no *Princípio de Arquimedes*, que determina a relação entre o peso de um fluido deslocado e a flutuabilidade de um corpo imerso — um problema que pode ser interpretado em termos de equações da física. É conhecido também por seus estudos sobre alavancas. Além de cientista, era também um habilidoso inventor, tendo criado o famoso *Parafuso de Arquimedes*, que consistia em uma inovação para a elevação de água, utilizado ainda hoje, além de instrumentos bélicos de defesa de sua cidade natal, Siracusa, contra invasores pelo mar, sendo o mais famoso destes um enorme espelho côncavo que teria a capacidade de incendiar navios inimigos.

Segundo Boyer e Merzbach (2019, p. 122), quando Arquimedes enviou o tratado sobre "o Método", escolheu Eratóstenes[26] como destinatário devido à sua familiaridade com muitas áreas de estudo, dada a sua posição de diretor da Biblioteca de Alexandria[27].

Eratóstenes tornou-se conhecido por ter sido um dos primeiros a calcular o raio da Terra. Para tanto, observou que na cidade egípcia de Alexandria (S), o Sol não criava sombra no fundo de um poço ao meio-dia durante o solstício de verão, indicando que os raios solares incidiam de forma perpendicular. No mesmo dia e hora na atual cidade de Assuã (A), antiga Siena, cerca de 800 km ao sul de Alexandria, um poste vertical (gnômon) criava uma sombra, de modo que Eratóstenes, ao medir o ângulo da sombra, obteve um valor próximo de 7,2 graus.

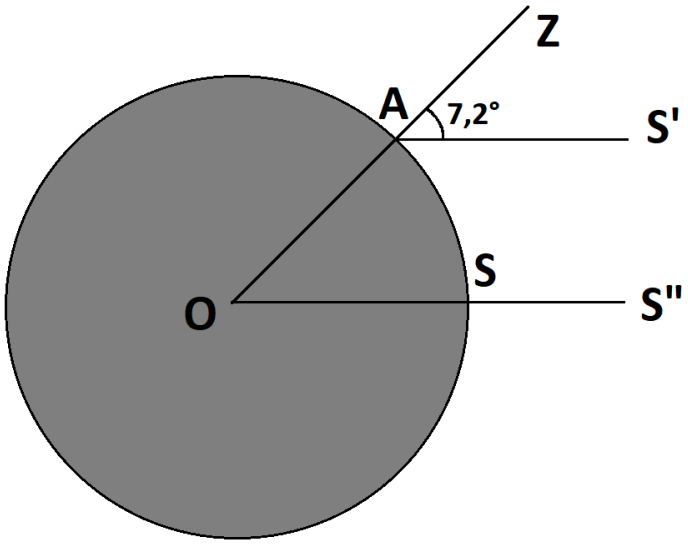


Figura 10 – Cálculo do raio da Terra, por Eratóstenes.

Fonte: Boyer e Merzbach (2019, p. 122)

[26] Eratóstenes (c. 276 – 194 a.E.C.) matemático, geógrafo, poeta, astrônomo e músico grego.

[27] A Biblioteca de Alexandria foi um complexo de ensino e pesquisa cuja origem remonta ao final do século IV a.E.C. e seu ápice ocorreu entre os séculos III e II a.E.C.

Com base nessas informações, aplicou o seguinte raciocínio.

$$\frac{7,2}{360} = \frac{800 \text{ km}}{\text{Circunferência da Terra}}$$

Portanto, a circunferência da Terra é:

$$\text{Circunferência da Terra} = \frac{360 \times 800 \text{ km}}{7,2}$$

Calculando, obtemos 40.000 km para a circunferência da Terra. Considerando a fórmula da circunferência $C = 2\pi r$, podemos encontrar o raio da Terra (r):

$$r = \frac{C}{2\pi} = \frac{40.000 \text{ km}}{2\pi} \approx 6.370 \text{ km}.$$

Assim, Eratóstenes chegou a uma estimativa incrivelmente precisa para o raio da Terra.

Outra notável contribuição de Eratóstenes à Matemática foi a criação do "crivo de Eratóstenes", que é um método simples para encontrar todos os números primos até um valor dado. Um resultado particularmente interessante decorre do fato de que somente precisa fazer o teste dos números até a raiz quadrada do maior número da sequência. Ou seja, se tomarmos uma sequência de cem números, devemos utilizar os múltiplos de 2 até $\sqrt{100} = 10$ [28].

Em Alexandria, por volta do ano 250, surge Diofanto[29], conhecido por seu trabalho pioneiro na introdução de uma forma inicial de álgebra simbólica. Em sua obra mais famosa, *Arithmetica*, desenvolveu um sistema de notação algébrica que representava tanto números desconhecidos quanto potências desses números. Embora esse sistema seja primitivo comparado aos padrões modernos, foi um passo significativo em direção à abstração algébrica, haja vista a dificuldade de realizar cálculos cada vez mais abstratos. Dessa forma, a partir de uma série de símbolos em substituição às expressões então escritas totalmente com palavras, foi possível representar as informações do problema por meio de abreviações. Por exemplo, o que hoje conhecemos por incógnita era representado pela letra grega ς, provavelmente por ser a última letra da palavra *arithmos*. Assim, o respectivo quadrado era escrito como Δ^{γ}; o cubo, K^{γ}; a quarta potência como $\Delta^{\gamma}\Delta$; a quinta como ΔK^{γ} e a sexta como $K^{\gamma}K$, por exemplo.

A esse tipo de notação, denomina-se "sincopada", sendo a principal diferença em relação à notação algébrica moderna a ausência de símbolos especiais para operações e relações, assim como de notação exponencial.

[28] Para demonstrar esse fato, seja n um número composto. Logo, podemos escrever $n = ab$. Supondo, por absurdo, que $a > \sqrt{n}$ e $b > \sqrt{n}$, então$n = ab > \sqrt{n}\sqrt{n} = n$, o que é uma contradição. Logo, $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$. Portanto, todo primo p que divide a satisfaz$p \leq a \leq \sqrt{n}$ (CQD).

[29] Diofanto (c. 200 - 284 E.C.) matemático grego antigo, frequentemente referido como o "pai da álgebra". Ele é mais conhecido por seu trabalho *Arithmetica*, uma série de 13 livros que tratam de soluções para equações algébricas e a teoria dos números, dos quais apenas seis se mantiveram preservados até os dias atuais.

Segundo Boyer e Merzbach (2019, p. 135), a inspiração que Fermat[30] teve ao formular o célebre último teorema foi em decorrência de uma tentativa de generalizar um problema que havia lido na *Arithmetica* de Diofanto, cujo enunciado original seria dividir um dado quadrado em dois quadrados. Além disso, as equações polinomiais que requerem soluções inteiras são conhecidas por "equações diofantinas", em sua homenagem.

2.5 China Antiga e Medieval

De acordo com Boyer e Merzbach (2019, p. 143), os registros cronológicos da História da Matemática na China são menos confiáveis do que os relativos ao Egito e Mesopotâmia.

Na China, os primeiros registros de Matemática começam com os primeiros registros na dinastia Shang (1600 - 1046 a.E.C.), quando foi escrito um livro chamado *I-king* (O Livro das Permutações), considerada uma obra mística, mas que possuía algum conteúdo matemático, por exemplo, o quadrado mágico mais antigo de que se tem notícia.

As civilizações que se desenvolveram às margens dos rios Iang-Tsé e Amarelo compilaram, ao longo de sua história, um rico acervo matemático, sendo o Zhoubi Suanjing (Chou-Pei Suan-King) o clássico mais antigo, provavelmente no século XII a.E.C.. Segundo Garbi (2011, p. 16), nessa obra se encontra um diagrama, sem explicações, que corresponde a uma demonstração do Teorema de Pitágoras. Aliás, a prova moderna que utiliza tal diagrama é atualmente conhecida como "prova chinesa".

Figura 11 – Diagrama relativo aos triângulos retângulos (séc. XII a.E.C.).

Fonte: Garbi (2011, p. 16)

[30] Pierre de Fermat (1607 – 1665) jurista e matemático francês, reconhecido como um dos grandes matemáticos da história, especialmente por suas contribuições fundamentais à teoria dos números, à análise e à probabilidade, sendo famoso por seu *Último Teorema*, que afirma que não existem números inteiros positivos a, b e c tais que $a^n + b^n = c^n$, quando $n \geq 2$. Embora tenha afirmado possuir uma prova de tal teorema, esta nunca foi encontrada, permanecendo sem solução até 1994, quando o matemático britânico Andrew Wiles apresentou uma prova definitiva.

Os chineses desenvolveram técnicas de cálculo utilizando "numerais em barras", que eram representações posicionais cujos cálculos eram feitos em uma tábua de calcular, instrumento este que não deve ser confundido com o ábaco, que viria a ser utilizado muitos séculos mais tarde. Essa técnica se baseava em um sistema decimal posicional, conceito que depois viria a ser utilizado por outras civilizações.

Outra obra bastante influente da Matemática antiga chinesa é o Jiuzhang suanchu (Chui-chang suan-shu), que apresentava 246 problemas dispostos em nove capítulos, abrangendo tópicos cotidianos tais como agrimensura, cálculo de impostos e soluções de equações.

Por volta do do século XIII, a Matemática chinesa atingiu seu mais elevado patamar, tendo Li Zhi[31] sido um dos principais matemáticos do período. Autor do livro Ceyyan Haijing (Ts'e-yuan hai-ching) — cuja tradução literal seria "Espelho marinho das medidas do círculo" —, Li Zhi compilou uma lista de 170 problemas que abrangiam círculos inscritos e circunscritos e suas relações com triângulos retângulos, sendo que alguns desses problemas levavam a equações de quarto grau, as quais eram resolvidas por meio de representações geométricas.

Embora nessa obra não tenha sido feita a descrição de um método de resolução para tais equações, que em alguns casos podia chegar a sexto grau, a técnica empregada era similar à utilizada por Zhu Shijie (Chu Shih-chieh)[32].

De acordo com Boyer e Merzbach (2019, p. 148), Qin Jiushao (Ch'in Chiu-shao)[33] escreveu a obra Shushu jiuzhang (Tratado matemático em nove partes) na qual descreve os passos para obter a raiz quadrada de 71.824. Em notação atual, seria o equivalente a resolver a equação $x^2 - 71.824 = 0$. Com 200 como primeira aproximação, ele diminuiu as raízes dessa equação de 200. Substituindo $x = -y$, obteve $y^2 + 400y - 31.824 = 0$. Para esta equação, encontrou 60 como aproximação e subtraiu 60 das raízes. Substituiu $y = -z$ e chegou à equação $z^2 + 520z - 4.224 = 0$, cuja raiz exata é 8. Daí, concluiu que a raiz de $x^2 - 71.824 = 0$. seria $x = 200 + 60 + 8 = 268$. Aplicando o mesmo método, resolveu equações de grau três e quatro.

O último e maior matemático do período foi Zhu Shijie, de quem pouco se sabe. Autor de dois importantes tratados, Suanxue qimeng (Suan-hsueh ch'i-meng)(Introdução aos estudos matemáticos) e Siyuan yujian (Ssu-yuan yu-chien)(Precioso espelho dos quatro elementos), de 1303. Nessa obra, Zhu Shijie representa os quatro elementos (terra, fogo, água e ar) como sendo quatro incógnitas na mesma equação.

Considerado o *ápice* do desenvolvimento da álgebra chinesa, nessa obra constam equações de grau quatorze, as quais o autor emprega um método denominado *fan fa* para resolver. Tal método parece ter surgido muito tempo antes, sendo geralmente associada ao nome de Horner[34]

[31] Li Zhi (1192 - 1279), conhecido como Li Ye, matemático chinês do período da dinastia Song.
[32] Zhu Shijie (c. 1249 - 1314) matemático chinês, considerado um dos maiores antiguidade chinesa.
[33] Qin Jiushao(1202 - 1261) governador e ministro chinês, com questionável reputação.
[34] William George Horner (1786 - 1837) matemático britânico, conhecido por desenvolver, em 1819, o *Método de Horner*, para a simplificação do processo de divisão e resolução de equações polinomiais.

— que viveu cerca de 500 anos depois —, e consiste em uma translação do tipo $y = x - h$.

É importante destacar que nessa obra, Zhu Shijie apresenta o que hoje se conhece por *triângulo de Pascal* — constando, inclusive, na capa. Entretanto, o autor não reinvidicava o crédito de tal triângulo, referindo-se a ele por "O diagrama do velho método dos sete quadrados multiplicativos".

Yang Hui[35] também apresentou um arranjo semelhante ao triângulo de Pascal em seus trabalhos, mas sem utilizar o símbolo redondo para *zero*. De fato, algumas obras chinesas de cerca de 1.100 faziam referências a sistemas de tabulação para coeficientes binomiais. É provável, portanto, que arranjos semelhantes ao triângulo de Pascal tenham surgido já nessa época.

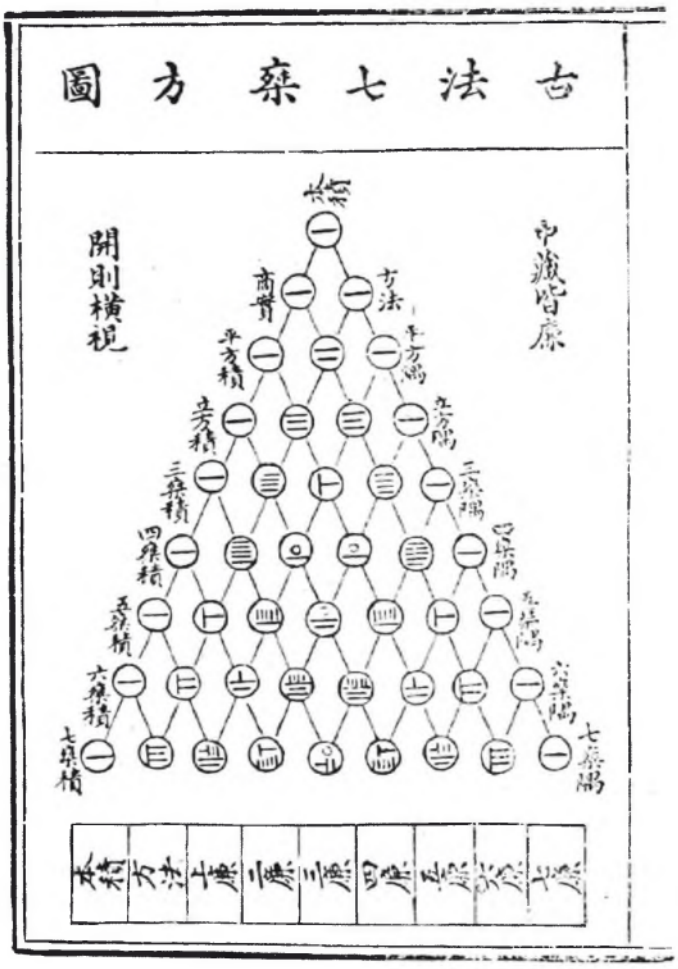


Figura 12 – O triângulo aritmético de Pascal, segundo Zhu Shijie, em 1303.

Fonte: Eves (2004, p. 250)

Um problema interessante que consta na obra de Yang Hui é o "problema do bambu quebrado", cujo enunciado é:

Há um bambu de 10 pés de altura cuja extremidade superior, ao ser quebrada, atinge o chão a 3 pés da haste. Achar a altura da quebra.

[35] Yang Hui (1261 - 1275) matemático chinês da dinastia Song.

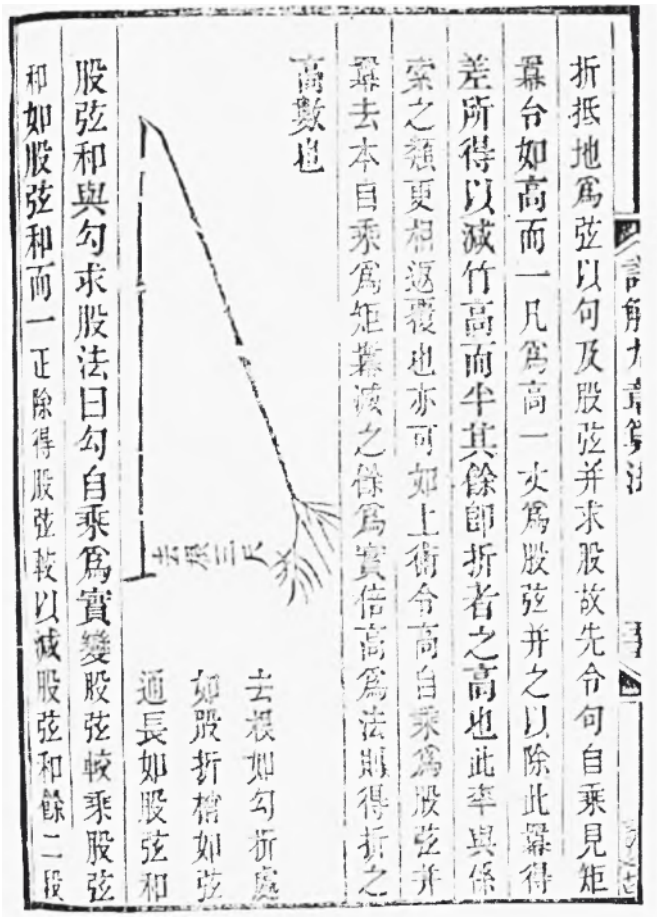


Figura 13 – O problema do bambu quebrado, de um trabalho de Yang Hui (1261).

Fonte: Eves (2004, p. 249)

A descoberta chinesa do teorema binomial para potências inteiras estava associada, originalmente, à extração de raízes, e não a potenciações. Tal fato era de conhecimento de Omar Khayan[36] mais ou menos na mesma época. Entretanto, a mais antiga obra da Matemática árabe que trata do assunto data do século XV, de autoria de al-Kashi[37].

A partir daí, a Matemática chinesa decaiu novamente, voltando a se dedicar somente às necessidades aritméticas comerciais, mantendo-se assim até o século dezesseis, quando a China aumentou novamente a sua interação com a Europa ocidental.

[36] Omar Khayan (1048—1131) poeta, matemático, filósofo e astrônomo persa. Conhecido por seu trabalho poético, o *Rubaiyat*, Khayan também se notabilizou por seus trabalhos na solução de equações cúbicas, tendo desenvolvido um método geométrico para resolver essas equações.

[37] Ghiyath al-Din Jamshid Mas'ud al-Kashi (c. 1380—1429) matemático e astrônomo persa, do período da dinastia Timúrida. Sua obra mais conhecida, *A Chave para a Aritmética* (Miftah al-Hisab), é um compêndio abrangente sobre a aritmética medieval e inclui tópicos como frações, raízes quadradas e cúbicas, e equações lineares e quadráticas. Em outra obra importante, *O Tratado dos Círculos Circulares*, al-Kashi calculou o valor de π com uma precisão de 16 casas decimais.

2.6 Índia Antiga e Medieval

Berço de alguns dos mais proeminentes matemáticos da história, a Índia teve na figura de Aryabhata[38] um papel semelhante ao que Euclides teve na Grécia Antiga, cerca de oito séculos antes. Diferentemente de Euclides, que apresentou uma síntese bem-ordenada de Matemática com elevado grau de abstração, Aryabhata escreveu uma obra descritiva, com 123 estrofes metrificadas. Nela, são apresentadas regras de cálculo para problemas de Astronomia e Matemática, sem qualquer metodologia dedutiva. Além disso, há imprecisões Matemáticas nas fórmulas apresentadas, tais como no cálculo do volume da pirâmide e da esfera (BOYER; MERZBACH, 2019, p. 153). Um resultado notável dessa obra é o cálculo aproximado de π, equivalente a $3,1416$.

Cerca de um século após Aryabhata, surge Brahmagupta[39], cuja obra mais conhecida *Brahmasphuta Siddhanta* (A abertura do Universo) apresenta um panorama da Matemática indiana da época — a despeito de incorrer em alguns erros conceituais e de cálculo. Nessa obra, Brahmagupta apresenta cálculos com zero e números negativos, além de seus métodos para resolver uma variedade de problemas algébricos, incluindo quadráticas e a equação linear diofantina conhecida como *Problema de Brahmagupta*.

Em meados do século XII, surge Bháskara II[40], o último matemático medieval importante da Índia, autor de *Vija-Ganita* e *Lilavati* — este último, que significa *a bela*, em homenagem à sua filha.

Em ambas as obras, Bháskara II apresenta diversos problemas matemáticos, versando sobre assuntos tais como equações lineares e quadráticas, progressões aritméticas e geométricas e ternas pitagóricas, além de resolver algumas equações do tipo $x^2 = 1 + py^2$ — conhecida como "equação de Pell" —, que havia sido proposta por Brahmagupta. Cabe destacar que Bháskara II apresentou soluções para os casos $p = 8, 11, 32, 61$ e 67. No caso $p = 61$, por exemplo, Bháskara II apresentou $x = 1.776.319.049$ e $22.615.390$ como solução — um feito notável para a época.

A relação entre a Matemática da Índia e a do Mundo Islâmico é uma fascinante história de trocas culturais e científicas, influenciando significativamente o desenvolvimento da Matemática. Essa interação iniciou por volta do século VIII, quando os árabes[41] entraram em contato com a Matemática indiana, motivados pelas trocas comerciais em torno da Roda da Seda, e continuou a

[38] Aryabhata (476 - 550) matemático e astrônomo indiano, considerado um dos maiores da Índia clássica. Sua obra magistral, *Aryabhatiya*, escrita em 499, é um dos primeiros registros de utilização do zero da forma como conhecemos hoje.

[39] Brahmagupta (598 - 670) matemático e astrônomo indiano .

[40] Bháskara II (1114 – c. 1185), matemático e astrônomo indiano. É considerado um dos primeiros a discutir conceitos como infinitesimal e derivação, que seriam mais tarde utilizados no que viria a ser conhecido como cálculo diferencial e integral.

[41] Haviam outros povos além dos árabes, tais como os persas e os turcos, cada qual com culturas e idiomas próprios. Por isso, alguns autores optam por se referir a "islâmicos", o que não contribui para um melhor entendimento, dada a diversidade de religiões da região.

florescer durante a Idade de Ouro Islâmica.

O primeiro contato significativo ocorreu com a conquista muçulmana da Índia. Os árabes, já influenciados pela Matemática grega, encontraram um considerável acervo de conhecimento na Índia, incluindo avançados sistemas numéricos e técnicas matemáticas. Eles rapidamente reconheceram a eficiência e a sofisticação do sistema numérico indiano e passaram a divulgá-lo.

Segundo Garbi (2011, p. 136), uma das maiores contribuições da Matemática indiana para o mundo foi o conceito do zero. Embora a noção de *nada* ou *vazio* já existisse em várias culturas, foi na Índia que o zero foi pela primeira vez sistematicamente utilizado como um número em cálculos matemáticos. Este avanço, registrado por volta do século V pelo matemático indiano Aryabhata, revolucionou a Matemática, permitindo o desenvolvimento de um sistema numérico posicional e facilitando cálculos complexos.

Os matemáticos árabes, fascinados pelo sistema numérico indiano, adotaram e adaptaram os numerais, resultando no que hoje conhecemos como numerais indo-arábicos. Al-Khwarizmi[42], um matemático persa do século IX, foi fundamental nesse processo. Seu trabalho, *Sobre o Cálculo com Numerais Hindus*, introduziu o sistema numérico indiano no mundo islâmico. Este sistema, por sua simplicidade e eficácia, eventualmente se espalhou para a Europa e se tornou o padrão em quase todo o mundo.

Além dos numerais, os matemáticos indianos também influenciaram os árabes em áreas como álgebra e trigonometria. O próprio termo *álgebra* tem origens árabes, mas a disciplina como um campo de estudo sistemático foi fortemente influenciada pelos trabalhos de matemáticos indianos, como Brahmagupta. Na trigonometria, as funções seno e cosseno, conceitos essenciais da Matemática moderna, foram desenvolvidas na Índia e posteriormente adotadas pelos árabes.

Através dos árabes, o conhecimento matemático indiano chegou à Europa. Traduções de textos árabes para o latim durante a Idade Média abriram caminho para o renascimento matemático na Europa. A introdução do sistema numérico indo-arábico, em particular, foi um catalisador para o desenvolvimento científico e econômico na Europa.

2.7 Mundo Islâmico

A história da Matemática no mundo islâmico é uma fascinante jornada de descobertas, inovações e intercâmbio cultural que se estendeu aproximadamente do século VIII ao século XV. Durante este período, o mundo islâmico floresceu como um centro de aprendizado e pesquisa, contribuindo significativamente para o desenvolvimento da Matemática.

No início, após a fundação do Islã no século VII, os muçulmanos começaram a estabelecer um vasto império que se estendia da Espanha ao subcontinente indiano. Este vasto império proporcionou aos eruditos muçulmanos acesso a uma riqueza de conhecimentos acumulados

[42] Al-Khwarizmi (c. 780 - c. 850) Matemática matemático, astrônomo e geógrafo persa.

de civilizações antigas, como a grega, a persa, a indiana e a egípcia. Bibliotecas e centros de aprendizado como a famosa *Casa da Sabedoria*, em Bagdá, serviram como locais de encontro para intelectuais de diversas origens culturais.

Um dos primeiros e mais influentes matemáticos do mundo islâmico foi Al-Khwarizmi, que viveu no século IX. Seu trabalho mais famoso, *Al-Kitab al-Mukhtasar fi Hisab al-Jabr wal-Muqabala*, introduziu a álgebra como uma disciplina Matemática independente, distinta da aritmética e da geometria. O termo *álgebra* deriva do título deste trabalho, e sua abordagem sistemática para a resolução de equações lineares e quadráticas estabeleceu as bases para a Matemática moderna.

Al-Khwarizmi também fez contribuições significativas para a trigonometria, incluindo tabelas de senos e cossenos e a formulação de regras trigonométricas. Sua obra sobre o sistema numérico indiano levou à adoção dos números arábicos no mundo ocidental. Além disso, ele compilou e melhorou dados astronômicos e geográficos, impactando profundamente o conhecimento científico e matemático em várias culturas. Seu nome deu origem a palavras como *algarismo* e *algoritmo*, perpetuando sua importância na Matemática e na ciência da computação (GARBI, 2009, p. 23).

O mundo islâmico também testemunhou avanços significativos na trigonometria. Al-Battani[43], um astrônomo e matemático do século IX, é conhecido por suas precisas tabelas trigonométricas. Ele introduziu as funções de seno e cosseno, refinando e expandindo o trabalho dos matemáticos gregos.

No campo da geometria, matemáticos islâmicos como Omar Khayyan contribuíram com métodos para a solução de equações cúbicas e a teoria das proporções. A geometria islâmica também se destacou na arte, como é evidente nos complexos padrões geométricos encontrados na arquitetura islâmica.

O trabalho dos matemáticos islâmicos não se limitou à teoria. Eles aplicaram suas descobertas de maneiras práticas, como na melhoria dos métodos de cálculo para impostos, divisão de heranças, comércio, engenharia e astronomia.

No século XII, à medida que a Europa começava a emergir da Idade das Trevas, as traduções das obras de matemáticos islâmicos para o latim desempenharam um papel crucial no renascimento do aprendizado na Europa. Através destas traduções, o conhecimento matemático acumulado no mundo islâmico passou a ser difundido mundo afora, influenciando matemáticos como Fibonacci, que introduziu o sistema numérico indo-arábico na Europa.

[43] Al-Battani (c. 858 - 929) foi um renomado astrônomo e matemático árabe, cujas contribuições tiveram um impacto profundo na ciência medieval, sendo conhecio por seus trabalhos em astronomia sobre a precessão dos equinócios.

2.8 Europa

Na antiguidade, a Matemática europeia atingiu um elevado nível de sofisticação a partir dos trabalhos gregos antigos, com figuras notáveis como Tales, Pitágoras, Euclides e Arquimedes — os quais pavimentaram o caminho do conhecimento em diversas áreas, com destaque para geometria, aritmética e álgebra.

Obras como *Os Elementos* de Euclides, sistematizaram grande parte do conhecimento matemático da época. No entanto, após a queda do Império Romano e ao longo da Idade Média, houve um declínio na produção matemática europeia.

No início do século XVI, entretanto, a Europa retorna ao centro das discussões, com o embate promovido pela busca de métodos resolutivos para as equações de terceiro e quarto graus, que envolveu matemáticos notáveis como Scipione del Ferro[44], Niccolò Tartaglia[45], Girolamo Cardano[46], Ludovico Ferrari[47], François Viète[48], René Descartes[49], Albert Girard[50] e Rafael Bombelli[51].

Scipione del Ferro, atuando na Universidade de Bolonha no início do século XVI, foi pioneiro ao resolver uma cúbica do tipo $x^3 + mx = n$. Sua descoberta, por volta de 1515, foi mantida em segredo até após sua morte, sendo um dos primeiros avanços significativos nessa área.

Após sua morte, seu genro e aluno, Annibale Della Nave, herdou seus papéis e divulgou a solução. A descoberta de del Ferro formou a base para avanços subsequentes por matemáticos como Niccolò Tartaglia e Girolamo Cardano, que eventualmente publicaram e expandiram o método de resolução das equações cúbicas.

De forma independente, Tartaglia apresentou sua descoberta independente para resolução de cúbicas do tipo $x^3 + mx^2 = n$. Em 1535, ele participou de um concurso matemático contra Antonio Maria Fior, um discípulo de del Ferro, que havia descoberto anteriormente um método para resolver um tipo específico de equação cúbica. Tartaglia venceu o concurso, revelando seu próprio método para resolver essas equações.

Após este evento, Tartaglia foi abordado por Girolamo Cardano, que lhe pediu que

[44] Scipione del Ferro (1465 - 1526) matemático italiano, conhecido por seus estudos sobre cúbicas.
[45] Niccolò Tartaglia (1499 - 1557) matemático italiano, conhecido por seus estudos sobre cúbicas.
[46] Girolamo Cardano (1501 - 1576) matemático, médico e astrólogo italiano.
[47] Ludovico Ferrari (1522 - 1565) matemático italiano, conhecido por seus estudos sobre quárticas.
[48] François Viète (1540 - 1603), também conhecido como Franciscus Vieta, matemático francês, é considerado "o pai da álgebra moderna".
[49] René Descartes (1596 - 1650) foi um filósofo, matemático e cientista francês, considerado um dos principais pensadores da História. Conhecido como o *pai da filosofia moderna,* Descartes é conhecido por ter desenvolvido a geometria analítica, a qual usou conceitos de álgebra para descrever a geometria.
[50] Albert Girard (1595 - 1632) matemático francês, conhecido por suas contribuições à álgebra, tendo sido pioneiro na introdução e desenvolvimento de ideias algébricas e no avanço da notação matemática.
[51] Rafael Bombelli (1526 - 1572) foi um matemático italiano notável por suas contribuições à álgebra, em particular no campo dos números complexos.

compartilhasse sua solução sob a promessa de que não a publicaria. Tartaglia cedeu, mas Cardano eventualmente quebrou sua promessa, incluindo a solução em seu livro *Ars Magna* em 1545, juntamente com a solução de equações de quarto grau de seu aluno, Ludovico Ferrari. Tartaglia ficou enfurecido com a quebra da promessa, o que levou a uma disputa amarga entre os dois.

Além de seu trabalho em equações, Tartaglia fez contribuições significativas para a trigonometria e foi um dos primeiros a aplicar a matemática ao estudo da trajetória de projéteis, um campo que mais tarde se tornaria a balística. Seu livro *Nova Scientia*, de 1537, que discute estas questões, é considerado um dos primeiros trabalhos sobre a mecânica do movimento.

Com a resolução de equações cúbicas, o desafio se voltou para as quárticas. Nesse sentido, Ludovico Ferrari, que havia sido aluno de Cardano, foi responsável por um marco significativo: a resolução da equação quártica. Seu método foi incorporado ao *Ars Magna*, de Cardano, elevando Ferrari a uma posição de destaque na história da álgebra.

François Viète, matemático francês, contribuiu substancialmente para a álgebra simbólica e deu importantes passos em direção a uma formulação mais geral de soluções para equações polinomiais. Sua abordagem representou um avanço na abstração algébrica.

René Descartes e Albert Girard também tiveram contribuições notáveis: Descartes é conhecido por seu trabalho na geometria analítica, que estabeleceu a base para a solução algébrica de problemas geométricos; Girard fez avanços na teoria das equações, formulando pela primeira vez a regra que o número de soluções reais de uma equação polinomial é no máximo igual ao seu grau — que no Brasil é conhecida por *Relações de Girard*, enquanto em outros países é creditada, indevidamente, a Viète.

Ocorre que, apesar de as fórmulas resolutivas para equações de terceiro e quarto graus terem sido descobertas, em alguns casos as soluções obtidas pareciam não fazer sentido. Um exemplo disso é dado pela cúbica

$$x^3 - 15x - 4 = 0.$$

Por simples verificação, observa-se que $x = 4$ é uma raiz para tal equação. Entretanto, ao se aplicar a Fórmula de Cardano, obtém-se:

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

o que aparentemente não faz sentido, haja vista que no conjunto dos números reais, não existe raiz quadrada de número negativo.

Bombelli, diante dessa situação, simplesmente realizou operações com tais números como se fossem reais. E chegou a conclusões que possibilitou a aceitação de tais números, denominados imaginários, dando origem ao estudo de tal conjunto, denominado *complexo*, cuja

teoria foi posteriormente desenvolvida por Euler[52].

O panorama da Matemática apresentado aqui não tem a pretensão de contemplar todos os principais matemáticos de cada período e respectivas obras, o que seria inviável do ponto de vista prático e fugiria ao objetivo deste trabalho, mas sim apresentar uma contextualização histórica que possibilite ao leitor ter uma breve descrição biográfica. Nesse sentido, informações mais detalhadas podem ser obtidas nas seguintes referências: Roque (2012), Boyer e Merzbach (2019) e Eves (2004).

[52] Leonhard Euler (1707 - 1783) matemático e físico suíço, considerado um dos mais prolíficos e influentes matemáticos da história. Euler fez contribuições fundamentais em diversas áreas, como geometria, cálculo, trigonometria, álgebra, teoria dos números e física.

CAPÍTULO

3

EQUAÇÕES ALGÉBRICAS

3.1 A História das Equações

Segundo Crease (2011, p. 7), "a primeira equação que a maioria de nós aprende é o sinônimo de simplicidade: $1+1=2$".

Na referida obra, o autor comenta que a palavra latina *aequare* significa "tornar plano" ou "tornar nivelado". Muitas palavras em português vêm dessa raiz, dentre as quais podemos citar: adequar, equidade, igualdade, equilíbrio, igualitário, equivalência e equívoco.

Nesse sentido, a palavra "equação" significava, em princípio, "separar em grupos iguais". Um exemplo seria a palavra "equador" — que é uma linha imaginária, inventada por geógrafos, que separa a Terra em duas partes iguais."

> "Os primeiros seres humanos viviam sem equações e não precisavam delas. Não havia equações no Jardim do Éden, nem na Árvore do Conhecimento. Não havia equações no paraíso sumério de *Dilmun*, nem tampouco no Ovo Cósmico que alguns chineses acreditam ter sido usado por *P'an Ku* para dar origem ao mundo, ou em qualquer dos outros lugares descritos nos mitos de criação. Os seres humanos nem tinham o *conceito* de equação. Este conceito é uma invenção humana, resultado de nossos esforços para dar sentido ao mundo. E mais: os homens não acordaram certo dia e de repente decidiram que iriam inventar as equações. A necessidade foi surgindo ao longo do tempo, e o conceito de equação, no sentido técnico-científico, só apareceu muito mais tarde na história." (CREASE, 2011, p. 8)

Segundo Cohen (2005), os números e a contagem se tornaram importantes para os homens uma vez que tais conceitos eram utilizados por comerciantes, por exemplo, em inventários, finanças e orçamentos. Autoridades religiosas utilizavam números para contar os anos, as estações e ocasiões especiais — tais como nascimentos, mortes e casamentos. Os governos, por

sua vez, utilizavam números em censos, pesquisas e cobranças de impostos. Essa necessidade de registrar números motivou a criação de símbolos para representar quantidades.

No século III a.E.C. , o matemático grego Diofanto[1] utilizou símbolos para representar quantidades *desconhecidas* e providenciou algumas regras para lidar com essas quantidades, incluindo a subtração e adição.

Ele mostrou não somente como utilizar símbolos para representar um número desconhecido de modo que este número pudesse ser descoberto a partir de outras quantidades conhecidas, que é chamado de equação determinada, mas também como os símbolos podiam descrever algo com um conjunto infinito de soluções, chamado de equação indeterminada ou diofantina.

Até Galileu[2] e Newton[3] expressaram seus importantes resultados em palavras, e não com as equações que hoje são familiares a qualquer estudante de ciências. Isso porque até o século XVIII os cientistas naturais não haviam tornado rotineira a prática de expressar suas conclusões na forma de equações como as conhecemos hoje.

A seguir, iremos caracterizar as equações polinomiais de grau até quarto, assim como apresentar as respectivas fórmulas resolutivas, tendo por referências Lima *et al.* (1997) e Stewart (2022).

3.2 A Equação de 1º Grau

Definição 3.2.1. Uma *equação do primeiro grau* é do tipo

$$a\,x+b=0\,, \tag{3.2.1}$$

em que a e b são reais e $a \neq 0$.

Para encontrar a raiz da equação do primeiro grau, basta encontrar um modo de se "isolar" a variável x, o que pode ser feito por meio das seguintes operações algébricas.

$$(a\,x+b)-b=0-b \iff a\,x+[b+(-b)]=-b \iff a\,x+0=-b \iff a\,x=-b \therefore x=-\frac{b}{a}.$$

Portanto, a solução de uma equação do primeiro grau é dada por $x=-\dfrac{b}{a}$.

[1] Diofanto de Alexandria viveu no século III a.E.C. e foi um matemático grego e é considerado por muitos como "o pai da álgebra". Desempenhou nessa área papel semelhante ao que Euclides (360–295 a.E.C.) teve na Geometria e Ptolomeu (85–165 E.C.) teve na Astronomia.

[2] Galileu Galilei (1564–1642), foi um astrônomo, físico e engenheiro italiano, considerado o "pai da astronomia observacional", "pai da física moderna", "pai do método científico" e "pai da ciência moderna"

[3] *Sir* Isaac Newton (1642–1727) foi um matemático, físico, astrônomo e teólogo inglês, reconhecido como um dos cientistas mais influentes de todos os tempos.

3.3 A Equação de 2º Grau

Definição 3.3.1. Uma equação do *segundo grau* é do tipo

$$a\,x^2 + b\,x + c = 0\,, \tag{3.3.1}$$

em que a, b e c são reais e $a \neq 0$.

Para determinar as raízes de 3.3.1, podemos considerar o trinômio:

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

Como $a \neq 0$ então $x^2 + \dfrac{b}{a}\,x + \dfrac{c}{a} = 0$. Daí, observando-se que as duas primeiras parcelas da soma de dentro dos parênteses são as mesmas do desenvolvimento de $\left(x + \dfrac{b}{2a}\right)^2$, podemos somar e subtrair o termo $\left(\dfrac{b}{2a}\right)^2 = \dfrac{b^2}{4a^2}$ no primeiro membro e escrever:

$$\left[x^2 + 2\left(\frac{b}{2a}\right)x + \left(\frac{b}{2a}\right)^2\right] + \frac{c}{a} - \frac{b^2}{4a^2} = 0$$

ou seja,

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

Ao numerador do lado direito da equação, dá-se o nome de "discriminante" — denotando-o por Δ — de uma equação de segundo grau. Assim, fazendo-se $\Delta = b^2 - 4ac$ e extraindo-se as raízes quadradas de ambos os lados, temos:

$$x + \frac{b}{2a} = \pm\sqrt{\frac{\Delta}{4a^2}}$$

Portanto, as raízes da equação 3.3.1 são dadas por:

$$x = \frac{-b \pm \sqrt{\Delta}}{2a}. \tag{3.3.2}$$

Há três possibilidades para o discriminante:

- Se $\Delta < 0$, então a equação não possui raízes reais (ou seja, possui raízes complexas conjugadas[4]);

[4]

- Se $\Delta = 0$, então a equação possui uma única raiz real; e
- Se $\Delta > 0$, então a equação possui duas raízes reais e distintas;

3.4 A Equação de 3º Grau

Definição 3.4.1. Uma equação do *terceiro grau* é do tipo

$$a\,x^3 + b\,x^2 + c\,x + d = 0\,, \tag{3.4.1}$$

em que a, b, c e d são reais e $a \neq 0$.

Para determinar uma raiz de 3.4.1, faremos a substituição $x = y + h$, com y e h reais. Assim, podemos reescrever a equação da seguinte forma:

$$a\,(y+h)^3 + b(y+h)^2 + c\,(y+h) + d = 0$$

Desenvolvendo a expressão e agrupando os termos segundo as potências de y, temos:

$$ay^3 + (3ah+b)y^2 + (3ah^2 + 2bh + c)y + (ah^3 + bh^2 + ch + d) = 0$$

Uma maneira de se resolver equações é reduzir o problema a um outro cuja solução seja conhecida. Nesse sentido, ao fazer a substituição $h = -\dfrac{b}{3a}$, eliminamos o termo em y^2, reduzindo o problema a uma equação do tipo $y^3 + py + q = 0$, sendo p e q reais.

Dessa forma, teremos:

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

Simplificando e dividindo ambos os lados da equação por $a \neq 0$, temos:

$$y^3 + \left(\frac{c}{a} - \frac{b^2}{3a^2}\right)y + \left(\frac{2b^3}{27a^3} - \frac{bc}{3a^2} + \frac{d}{a}\right) = 0\,,$$

que é uma equação do tipo $y^3 + py + q = 0$, em que $p = \dfrac{c}{a} - \dfrac{b^2}{3a^2}$ e $q = \dfrac{2b^3}{27a^3} - \dfrac{bc}{3a^2} + \dfrac{d}{a}$.

Uma forma de resolver a equação $y^3 + py + q = 0$ é fazer a substituição $y = z - \dfrac{p}{3z}$.

Assim, teremos:

$$\left(z-\frac{p}{3z}\right)^3+p\left(z-\frac{p}{3z}\right)+q=0$$

Expandindo o termo ao cubo,

$$\left[z^3-3z^2\left(\frac{p}{3z}\right)+3z\left(\frac{p}{3z}\right)^2-\left(\frac{p}{3z}\right)^3\right]+pz-\frac{p^2}{3z}+q=0$$

Simplificando,

$$z^3-zp+\frac{p^2}{3z}-\frac{p^3}{27z^3}+pz-\frac{p^2}{3z}+q=0$$

Daí,

$$z^3-\frac{p^3}{27z^3}+q=0 \tag{3.4.2}$$

Multiplicando-se ambos os lados da equação por z^3, temos:

$$z^6+qz^3-\frac{p^3}{27}=0\,,$$

que, após a substituição $z^3=t$, torna-se uma equação quadrática na variável t dada por:

$$t^2+qt-\frac{p^3}{27}=0 \tag{3.4.3}$$

que pode ser resolvida por meio da aplicação da fórmula resolutiva para equações do segundo grau apresentada em 3.3.2.

Desse modo, as raízes da equação 3.4.3 são dadas por:

$$t=-\frac{q}{2}\pm\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}$$

Ao radicando do lado direito da equação, dá-se o nome de "discriminante" — denotando-o por Δ — de uma equação de terceiro grau. Assim, fazendo-se $\Delta=\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3$, temos três possibilidades para o discriminante:

- Se $\Delta>0$, então a equação possui três raízes reais distintas;
- Se $\Delta=0$, então a equação possui raízes reais múltiplas; e
- Se $\Delta<0$, então a equação possui uma raiz real e duas complexas conjugadas;

Como $t = z^3$,

$$z_1 = \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} \quad \text{e} \quad z_2 = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

Dessa forma, como $y^3 + py + q = 0$

$$y = \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} \tag{3.4.4}$$

é uma solução da equação reduzida $y^3 + py + q = 0$.

Exemplo 3.4.1. Reduzir a equação cúbica:

$$-2x^3 + x^2 + \frac{1}{3}x - 6 = 0.$$

Solução:

Para resolvê-la, devemos transformá-la em uma equação reduzida do tipo $y^3 + py + q = 0$.

Assim, dividindo-se todos os termos por -2, que é o coeficiente de x^3, para tornar o coeficiente líder igual a 1, temos:

$$x^3 - \frac{1}{2}x^2 - \frac{1}{6}x + 3 = 0.$$

O passo seguinte é eliminar o termo quadrático. Daí, fazemos $x = y + \frac{1}{6}$:

$$\left(y + \frac{1}{6}\right)^3 - \frac{1}{2}\left(y + \frac{1}{6}\right)^2 - \frac{1}{6}\left(y + \frac{1}{6}\right) + 3 = 0,$$

obtendo a forma reduzida da equação cúbica $y^3 + py + q = 0$, para os quais obtemos os valores $p = -\frac{1}{4}$ e $q = \frac{27}{80}$.

Alternativamente, poderíamos ter obtido a forma reduzida da equação utilizando o fato de que

$$p = \frac{c}{a} - \frac{b^2}{3a^2} = \frac{1/3}{-2} - \frac{1^2}{3(-2)^2} = -\frac{1}{6} - \frac{1}{12} = -\frac{1}{4}.$$

e

$$q = \frac{2b^3}{27a^3} - \frac{bc}{3a^2} + \frac{d}{a} = \frac{2(1^3)}{27(-2)^3} - \frac{1 \cdot 1/3}{3(-2)^2} + \frac{-6}{-2} = \frac{2}{-216} - \frac{1/3}{12} + 3 = -\frac{1}{108} - \frac{1}{36} + 3 = \frac{80}{27}.$$

Agora a equação pode ser resolvida aplicando-se a fórmula apresentada em 3.4.4.

3.5 A Equação de 4º Grau

Definição 3.5.1. Uma equação do *quarto grau* é do tipo

$$a\,x^4 + b\,x^3 + c\,x^2 + d\,x + e = 0\,, \tag{3.5.1}$$

em que a, b, c, d e e são reais e $a \neq 0$.

Para determinar uma raiz de 3.5.1, faremos a substituição $x = y + h$, com y e h reais. Assim, podemos reescrever a equação da seguinte forma:

$$a\,(y+h)^4 + b(y+h)^3 + c(y+h)^2 + d(y+h) + e = 0$$

Desenvolvendo a expressão e agrupando os termos segundo as potências de y, temos:

$$ay^4 + (4ah+b)y^3 + (6ah^2+3bh+c)y^2 + (4ah^3+3bh^2+2ch+d)y + (ah^4+bh^3+ch^2+dh+e) = 0$$

Uma maneira de se resolver equações é reduzir o problema a um outro cuja solução seja conhecida. Nesse sentido, ao fazer a substituição $h = -\dfrac{b}{4a}$, eliminamos o termo em y^3, reduzindo o problema a uma equação do tipo $y^4 + py^2 + qy + r = 0$, sendo p, q e r reais.

Dessa forma, teremos:

$$\begin{aligned} ay^4 + \left[4a\left(-\frac{b}{4a}\right)+b)\right]y^3 + \left[6a\left(-\frac{b}{4a}\right)^2 + 3b\left(-\frac{b}{4a}\right) + c\right]y^2 + \\ + \left[4a\left(-\frac{b}{4a}\right)^3 + 3b\left(-\frac{b}{4a}\right)^2 + 2c\left(-\frac{b}{4a}\right) + d\right]y + \\ + \left[a\left(-\frac{b}{4a}\right)^4 + b\left(-\frac{b}{4a}\right)^3 + c\left(-\frac{b}{4a}\right)^2 + d\left(-\frac{b}{4a}\right) + e\right] = 0 \end{aligned}$$

Simplificando e dividindo ambos os lados da equação por $a \neq 0$, temos:

$$y^4 + \left(-\frac{3b^2}{8a^2} + \frac{c}{a}\right)y^2 + \left(-\frac{b^3}{8a^3} - \frac{bc}{2a^2} + \frac{d}{a}\right)y + \left(-\frac{3b^4}{256a^4} + \frac{b^2c}{16a^3} - \frac{db}{4a^2} + \frac{e}{a}\right) = 0\,,$$

que é uma equação do tipo $y^4 + py^2 + qy + r = 0$, em que $p = -\dfrac{3b^2}{8a^2} + \dfrac{c}{a}$, $q = -\dfrac{b^3}{8a^3} - \dfrac{bc}{2a^2} + \dfrac{d}{a}$ e $r = -\dfrac{3b^4}{256a^4} + \dfrac{b^2c}{16a^3} - \dfrac{db}{4a^2} + \dfrac{e}{a}$.

Uma forma de resolver a equação $y^4 + py^2 + qy + r = 0$ é escrevê-la de modo que:

$$y^4 + py^2 + qy + r = (y^2 + ty + u)(y^2 - ty + v) \ ,$$

com t, u e v reais.

Assim, teremos:

$$y^4 + py^2 + qy + r = y^4 + (u + v - t^2)y^2 + (v - u)ty + uv$$

Logo, como os coeficientes devem ser iguais, escrevemos:

$$\begin{cases} u + v - t^2 = p \\ (v - u)t = q \\ u\,v = r \end{cases}$$

Da terceira equação do sistema acima, temos que $v = \dfrac{r}{u}$. Daí,

$$\begin{cases} u + \dfrac{r}{u} - t^2 = p \\ \left(\dfrac{r}{u} - u\right) t = q \end{cases}$$

Ou seja,

$$\begin{cases} u^2 - u(t^2 + p) + r = 0 \\ u^2 + u\left(\dfrac{q}{t}\right) t - r = 0 \end{cases}$$

Em ambos os casos, tem-se uma equação do segundo grau na variável u. Logo, aplicando-se a fórmula dada em 3.3.2, tem-se:

$$u = \frac{(t^2 + p) \pm \sqrt{(t^2 + p)^2 - 4r}}{2}$$

e

$$u = \frac{-\dfrac{q}{2} \pm \sqrt{\left(\dfrac{q}{t}\right)^2 + 4r}}{2}$$

Assim,

$$t^2 + p + \frac{q}{t} = \pm \left(\sqrt{\left(\frac{q}{t}\right)^2 + 4r} - \sqrt{(t^2 + p)^2 - 4r} \right)$$

Elevando-se ambos os membros ao quadrado, temos:

$$t^4+2pt^2+2qt+\left(\frac{q^2}{t^2}+p^2+\frac{2pq}{t}\right)=$$

$$=\left[\left(\frac{q}{t}\right)^2+4r\right]-2\left[\sqrt{\left(\frac{q}{t}\right)^2+4r}\,\sqrt{(t^2+p)^2-4r}\right]+\left[(t^2+p)^2-4r\right]$$

Após simplificações, escrevemos:

$$qt+\frac{pq}{t}=\sqrt{\left[\left(\frac{q}{t}\right)^2+4r\right]\left[(t^2+p)^2-4r\right]}$$

Elevando-se novamente ambos os membros ao quadrado e simplificando, obtemos:

$$t^6+2pt^4+(p^2-4r)t^2-q^2=0\,,$$

que por meio da substituição $t^2=k$ se torna uma equação cúbica, que pode ser resolvida segundo a seção anterior.

3.6 Equações de 5º Grau em diante

Para descobrir se uma equação genérica de grau maior ou igual a cinco é solúvel algebricamente — ou seja, por meio de um número finito de operações de soma, subtração, multiplicação, divisão, potenciação inteira e radiciação aplicadas a seus coeficientes —, Garbi (2009, p. 175) menciona que, na maioria dos casos, faz-se necessário aplicar conceitos de *Teoria de Grupos*, que são considerados avançados para o público geral. Entretanto, há uma infinidade de casos particulares em que é possível resolver uma equação polinomial, independentemente do grau.

O teorema a seguir trata de um desses casos.

Teorema 3.6.1. (das Raízes Racionais) Se um número racional N/D, com N e D primos entre si, é raiz da equação polinomial de coeficientes inteiros $a_o\,x^n+a_1\,x^{n-1}+\cdots+a_{n-1}\,x+a_n=0$, então a_o é divisível por D e a_n é divisível por N.

Demonstração. Dado que N/D é uma fração irredutível e raiz da referida equação, então

$$a_o\left(\frac{N}{D}\right)^n+a_1\left(\frac{N}{D}\right)^{n-1}+\cdots+a_{n-1}\left(\frac{N}{D}\right)+a_n=0$$

Multiplicando-se ambos os lados da equação por D^n, tem-se:

$$a_o\, N^n + a_1\, D\, N^{n-1} + \cdots + a_{n-1}\, D^{n-1}\, N + a_n\, D^n = 0$$

Pondo-se N em evidência e subtraindo-se $a_n D^n$ de ambos os lados da equação, tem-se:

$$N\left(a_o\, N^{n-1} + a_1\, D\, N^{n-2} + \cdots + a_{n-1}\, D^{n-1}\right) = -a_n\, D^n$$

Como o lado esquerdo da igualdade é divisível por N, então o lado direito também o será. Uma vez que D^n não pode ser divisível por N — pois por hipótese N e D são primos entre si —, então a_n deve ser divisível por N.

Por outro lado, pode-se reescrever a mesma igualdade da seguinte maneira:

$$D\left(a_1\, N^{n-1} + a_2\, D\, N^{n-2} + \cdots + a_{n-1}\, D^{n-2}\, N + a_n\, D^{n-1}\right) = -a_o\, N^n$$

Outrossim, como N e D são primos entre si, então a_o é divisível por D e, desse modo, o teorema está demonstrado.

□

Algumas consequências importantes deste teorema são:

Corolário 3.6.1. Toda equação polinomial de coeficientes inteiros cujos coeficientes do termo de maior grau seja igual a um, se possuir raízes racionais, serão todas inteiras.

Demonstração. Para provar que toda equação polinomial de coeficientes inteiros, cujo coeficiente do termo de maior grau é igual a um e que possui raízes racionais, terá todas as raízes como números inteiros, podemos usar o Teorema das Raízes Racionais.

Suponha que tenhamos uma equação polinomial de grau n com coeficientes inteiros e que possua raízes racionais. Podemos escrever a equação como $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, em que a_n é o coeficiente do termo de maior grau e $a_n, a_{n-1}, \ldots, a_0$ são inteiros.

Se r é uma raiz racional da equação $p(x) = 0$, então $p(r) = 0$ e $r = \dfrac{p}{q}$, onde p e q são inteiros primos entre si.

Pelo Teorema das Raízes Racionais, se r é raiz racional da equação, então q divide a_n — que é o coeficiente do termo de maior grau —, e p divide o termo independente a_0. Por conseguine, r deve ser um número inteiro. Logo, como r é uma raiz arbitrária, então todas as raízes racionais são números inteiros.

Portanto, se uma equação polinomial de coeficientes inteiros — cujo coeficiente do termo de maior grau é igual a um — possui raízes racionais, então resta demonstrado que todas as raízes são números inteiros. □

Corolário 3.6.2. Uma equação polinomial de coeficientes inteiros cujo coeficiente de maior grau seja diferente de um — depois de estarem todos os coeficientes divididos por seu *máximo divisor comum* — não pode ter somente raízes inteiras.

Demonstração. Seja o polinômio p dado por $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, em que a_n é o coeficiente de maior grau, e a_i são coeficientes inteiros para $0 \leq i \leq n$.

Se dividirmos todos os coeficientes pelo máximo divisor comum (MDC) de todos os coeficientes, obtemos a seguinte equação polinomial:

$$Q(x) = \frac{a_n}{d}\, x^n + \frac{a_{n-1}}{d}\, x^{n-1} + \ldots + \frac{a_1}{d}\, x + \frac{a_0}{d},$$

em que d é o máximo divisor comum de $a_n,\ a_{n-1}, \ldots,\ a_0$.

Agora, vamos supor que o polinômio P tenha uma raiz inteira r. Isso significa que $P(r) = 0$. Substituindo-se na equação, tem-se $a_n\, r^n + a_{n-1}\, r^{n-1} + \ldots + a_1\, r + a_0 = 0$.

Dividindo-se ambos os lados da equação pelo máximo divisor comum $d \neq 0$ elevado à potência do grau do polinômio, tem-se:

$$\frac{a_n}{d} r^n + \frac{a_{n-1}}{d} r^{n-1} + \ldots + \frac{a_1}{d} r + \frac{a_0}{d} = 0$$

Dessa forma, todos os termos da equação acima são frações com denominador d, o que significa que são inteiros. Ou seja, r é uma raiz de $Q(x)$.

No entanto, isso contradiz a condição inicial de que todos os coeficientes de $Q(x)$ são inteiros e a_n/d é diferente de 1.

Portanto, chegamos à conclusão de que $P(x)$ não pode ter somente raízes inteiras quando seus coeficientes são divididos pelo máximo divisor comum.

□

Corolário 3.6.3. Toda raiz inteira de uma equação polinomial de coeficientes inteiros é divisor do termo independente.

Demonstração. Seja o polinômio P com coeficientes inteiros tal que $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_o$. Seja r uma raiz inteira dessa equação, ou seja, $P(r) = 0$. Logo, podemos escrever $a_n\, r^n + a_{n-1}\, r^{n-1} + \ldots + a_1\, r + a_o = 0$.

Isolando-se o termo a_o na equação, temos $a_o = -a_n\, r^n - a_{n-1}\, r^{n-1} - \ldots - a_1\, r$.

Dado que cada termo do lado direito da equação é um múltiplo de r — pois r é uma raiz da equação —, podemos fatorar r do lado direito e reescrever a igualdade do seguinte modo:

$$a_o = r\,(-a_n\, r^{n-1} - a_{n-1}\, r^{n-2} - \ldots - a_1)$$

Como a_o é igual a r multiplicado por um termo inteiro, então toda raiz inteira r de uma equação polinomial de coeficientes inteiros é um divisor do termo independente a_o.

□

A seguir, apresentaremos um tipo de equação polinomial particularmente interessante, denominado *equações recíprocas*.

Definição 3.6.1. Uma equação recíproca é uma equação em que os coeficientes do polinômio são substituídos por seus inversos multiplicativos. A forma geral de uma equação recíproca de grau n é:

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

A equação recíproca correspondente terá a seguinte forma:

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

Para que uma equação seja equivalente à sua recíproca, é necessário e suficiente que

$$\frac{a_o}{a_n} = \frac{a_1}{a_{n-1}} = \frac{a_2}{a_{n-2}} = \cdots = \frac{a_i}{a_{n-i}} = \cdots = \frac{a_{n-2}}{a_2} = \frac{a_{n-1}}{a_1} = \frac{a_n}{a_o} = k$$

Desse modo, se $\frac{a_o}{a_n} = \frac{a_n}{a_o} = k$, então $a_o^2 = a_n^2$. Logo, $a_o = \pm\, a_n$ e $\frac{a_o}{a_n} = \pm\, 1 = k$.

Para fins didáticos, será feita a distinção entre os casos $k = 1$ e $k = -1$, que serão denominados de *primeira* e *segunda* espécie, respectivamente.

Assim, com base na definição 3.6.1, obtemos os seguintes corolários:

Corolário 3.6.4. Toda recíproca de primeira espécie e grau ímpar admite -1 como raiz, que pode eventualmente ser uma raiz múltipla.

Demonstração. De fato, pois uma equação recíproca de primeira espécie e grau ímpar pode ser escrita como

$$a_o\, x^{2p+1} + a_1\, x^{2p} + a_2\, x^{2p-1} + \cdots + a_2\, x^2 + a_1\, x + a_o = 0$$

Tomando-se $x = -1$, resta demonstrado que o polinômio se anula. □

Corolário 3.6.5. Toda recíproca de segunda espécie e grau par admite $+1$ e -1 como raízes, que podem eventualmente serem raízes múltiplas.

Demonstração. De fato, pois uma equação recíproca de segunda espécie e grau par pode ser escrita como

$$a_o\, x^{2p} + a_1\, x^{2p-1} + a_2\, x^{2p-2} + \cdots - a_2\, x^2 - a_1\, x - a_o = 0$$

Tomando-se $x = 1$ ou $x = -1$, resta demonstrado que o polinômio se anula. □

Corolário 3.6.6. Toda recíproca de segunda espécie e grau ímpar admite $+1$ como raiz, que pode eventualmente ser uma raiz múltipla.

Demonstração. De fato, pois uma equação recíproca de segunda espécie e grau ímpar pode ser escrita como

$$a_o\, x^{2p+1} + a_1\, x^{2p} + a_2\, x^{2p-1} + \cdots - a_2\, x^2 - a_1\, x - a_o = 0$$

Tomando-se $x = 1$, resta demonstrado que o polinômio se anula. □

Diferentemente dos três casos apresentados acima, é importante destacar que não se pode afirmar — em relação às equações recíprocas de primeira espécie e grau par — que $+1$ ou -1 sejam as raízes. De fato, há casos em que isso acontece, mas não se pode generalizá-los.

Segundo Garbi (2009, p. 178), um exemplo de equação de primeira espécie e grau par pode ser dado pela equação $4x^4 - 5x^3 + 7x^2 - 5x + 4 = 0$. Dividindo-se ambos os membros da igualdade por x^2, tem-se $4x^2 - 5x + 7 - \frac{5}{x} + \frac{4}{x^2} = 0$. Assim, podemos reescrever a equação da seguinte maneira:

$$4\left(x^2 + \frac{1}{x^2}\right) - 5\left(x + \frac{1}{x}\right) + 7 = 0.$$

Tomando-se $x + \frac{1}{x} = y$, temos que $x^2 + \frac{1}{x^2} = y^2 - 2$. Assim, $4(y^2 - 2) - 5y + 7 = 0$. Ou seja, $4y^2 - 5y - 1 = 0$. Aplicando-se a fórmula resolutiva para equações do segundo grau, concluímos que $y = \frac{5 \pm \sqrt{41}}{8}$.

Desse modo, $x + \frac{1}{x} = \frac{5 \pm \sqrt{41}}{8}$. Logo, $x^2 - \left(\frac{5 \pm \sqrt{41}}{8}\right) x + 1 = 0$, equação quadrática com discriminante positivo, ou seja, sua resolução fornece as quatro raízes para a equação original.

De forma análoga, equações recíprocas de primeira espécie e grau par podem ser resolvidas algebricamente, bastando lembrar que:

$$x^3 + \frac{1}{x^3} = \left(x + \frac{1}{x}\right)^3 - 3\left(x + \frac{1}{x}\right)$$

e

$$x^4 + \frac{1}{x^4} = \left(x + \frac{1}{x}\right)^4 - 4\left(x + \frac{1}{x}\right)^2 + 2$$

Isso mostra que, embora Abel e Galois tenham demonstrado que equações polinomiais de grau maior ou igual a cinco não possuem uma solução geral, há casos particulares em que é possível resolver uma equação polinomial de forma algébrica.

CAPÍTULO

4

NOÇÕES GERAIS

4.1 Grupos

O desenvolvimento formal do conceito de grupo começou no início do século XIX.

Enquanto várias estruturas que agora reconhecemos como grupos foram usadas implicitamente por matemáticos como Lagrange[1] e Gauss[2], foi Évariste Galois quem, na década de 1830, primeiro começou a usar grupos de uma maneira que reconhecemos hoje, particularmente em seu estudo das raízes das equações polinomiais, levando ao desenvolvimento da Teoria de Galois.

O trabalho de Galois foi fundamental para estabelecer a conexão entre a teoria dos grupos e a teoria das equações algébricas, mostrando como as propriedades dos grupos podem determinar a solubilidade de equações polinomiais em radicais.

Ao longo do século XIX e início do século XX, a teoria dos grupos foi formalizada e

[1] Joseph-Louis Lagrange (1736-–1813) foi um matemático e astrônomo ítalo-francês, reconhecido como uma das figuras mais importantes da matemática do século XVIII, com contribuições em diversos campos, incluindo a análise matemática, teoria dos números, teoria das equações e mecânica celeste.

[2] Carl Friedrich Gauss (1777-–1855) foi um matemático, astrônomo e físico alemão, frequentemente chamado de *Príncipe dos Matemáticos* devido às suas notáveis contribuições para muitas áreas da matemática e da ciência. Prodígio matemático desde a infância, algumas de suas descobertas mais significativas foram feitas ainda e sua juventude. Gauss fez contribuições fundamentais em teoria dos números, incluindo sua obra *Disquisitiones Arithmeticae*. Também é conhecido por seus trabalhos em análise, geometria diferencial, geodésia, magnetismo, astronomia e óptica. Entre suas descobertas mais famosas, está o *Teorema Fundamental da Álgebra*, que afirma que todo polinômio não constante tem pelo menos uma raiz complexa. Na matemática, o *Método de Gauss* para solucionar sistemas lineares e a *Distribuição Normal* (ou *Curva de Gauss*) na estatística são apenas dois exemplos de sua influência. Na astronomia, Gauss contribuiu para a teoria do movimento planetário e foi o primeiro a calcular a órbita do asteroide Ceres. Sua influência estende-se por muitas áreas da matemática e da ciência, sendo lembrado como um dos maiores matemáticos de todos os tempos.

expandida por matemáticos como Augustin-Louis Cauchy[3], Arthur Cayley[4] e Felix Klein[5].

Neste seção, apresentaremos o conceito de Grupos e algumas de suas propriedades seguindo Martin (2010, p. 3).

Um grupo consiste num conjunto não vazio G munido de uma operação binária $\mu : G \times G \to G$, denotada simplesmente

$$(a,b) \in G \times G \mapsto a \cdot b \in G,$$

que satisfaz os seguintes axiomas:

G1. $(ab)c = a(bc)$ **(lei associativa)**;

G2. $\exists\, e \in G$ tal que $e \cdot a = a, \forall a \in G$ **(elemento neutro)**;

G3. $\forall a \in G$, $\exists\, b \in G$ tal que $b \cdot a = e$ **(elemento inverso)**.

A fim de simplificar a notação, escreveremos ab em vez de $a \cdot b$ que, por sua vez, já é a simplificação de $\mu(a,b)$.

Alguns grupos possuem uma propriedade adicional: a operação binária comutativa. Isso significa que $ab = ba$, para quaisquer $a,b \in G$. Nesse caso, é comum o emprego da notação aditiva

$$(a,b) \in G \times G \mapsto a + b \in G$$

para a operação binária.

Na notação aditiva, a identidade e é geralmente denotada por 0 e chamada de *elemento neutro*. Denotamos por $-a$ o inverso aditivo de a é chamado de *oposto* de a.

Exemplo 4.1.1. Alguns exemplos de grupos:

[3] Augustin-Louis Cauchy (1789—1857) foi um matemático francês cujas contribuições tiveram um impacto profundo em várias áreas da matemática e da física teórica. Conhecido pelo importante *Teorema do Resíduo* em análise complexa, tem seu nome vinculado a diversos conceitos, tais como *sequências de Cauchy*, *critérios de Cauchy*, e a *integral de Cauchy*. Suas obras abordam mais de 800 artigos e livros, tornando-o um dos matemáticos mais produtivos e influentes do século XIX.

[4] Arthur Cayley (1821—1895) foi um matemático britânico, conhecido por seus trabalhos fundamentais em álgebra, geometria, teoria dos números, e teoria dos grupos. Pioneiro na criação da álgebra matricial, notabilizou-se também por suas contribuições à teoria dos grupos abstratos.

[5] Felix Klein (1849—1925) foi um matemático alemão notável por suas contribuições em teoria dos grupos e geometria diferencial. Notabilizou-se pela formulação do *Programa de Erlangen*, em 1872, que propôs uma nova maneira de organizar e classificar a geometria com base nos conceitos de grupos de simetria, influenciando o desenvolvimento tanto da geometria quanto da álgebra. Teve importantes contribuições também em áreas como a teoria das funções, equações diferenciais e física matemática.

1. Os números inteiros $\mathbb{Z}$ com a operação de soma; ou ainda $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ — também com a operação de soma.

2. O anel $\mathbb{Z}_n$ das classes residuais módulo n, com a operação de soma.

3. O conjunto A^* dos elementos invertíveis de um anel $(A, +, \cdot)$, com a operação de produto do anel. Em particular $\mathbb{Q}^*$, $\mathbb{R}^*$ ou $\mathbb{C}^*$ com a operação de multiplicação.

4. (O grupo linear). O conjunto $GL_n(K)$ das matrizes quadradas de ordem n invertíveis, com entradas em um corpo K (por exemplo, K = $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ ou $\mathbb{Z}_p$ com p um número primo), com o produto usual de matrizes. O elemento neutro é a matriz identidade. Esse é o grupo dos elementos invertíveis do anel $(M_n(K), +, \cdot)$ formado por todas as matrizes quadradas de ordem n com operação usual de soma e multiplicação de matrizes.

5. O conjunto S_1 dos números complexos z com módulo $\mid z \mid = 1$, com a operação de produto.

6. O conjunto $GL(V)$ formado pelas transformações lineares invertíveis de um espaço vetorial V em si mesmo, com a operação de composição de funções. O elemento neutro é a função identidade.

Lema 4.1.1. (Associatividade Generalizada)

Seja $g_1, \cdots g_n$ uma lista ordenada com $n \geq 3$ elementos de um grupo G. Então podemos inserir parênteses no produto $g_1 g_2 \cdots g_n$, do modo que quisermos, sem alterar o resultado.

Demonstração. Vamos provar por indução em n. Para $n = 3$, o lema se reduz ao axioma G1 da definição de grupo. Seja $n > 3$ e suponhamos que o resultado seja válido para qualquer lista com menos do que n elementos. Suponhamos que o produto tenha sido feito de modo a resultar num produto final de dois fatores:

$$(g_1\, g_2 \cdots g_r)(g_{r+1}\, g_{r+2} \cdots\, g_n),$$

onde os parênteses intermediários foram retirados em virtude da hipótese de indução. Seja

$$(g_1\, g_2 \cdots g_s)(g_{s+1}\, g_{s+2} \cdots\, g_n),$$

um outro resultado final de dois fatores, advindo de outra distribuição de parênteses. Podemos supor que $r \leq s$. Se $r = s$ não há nada a provar. Se $r < s$ podemos escrever:

$$\begin{aligned}(g_1 \cdots g_s)(g_{s+1} \cdots g_n) &= ((g_1 \cdots g_r)(g_{r+1} \cdots g_s))(g_{s+1} \cdots g_n) \\ &= (g_1 \cdots g_r)(g_{r+1} \cdots g_s)(g_{s+1} \cdots g_n) \\ &= (g_1 \cdots g_r)(g_{r+1} \cdots g_n),\end{aligned}$$

o que conclui a demonstração do lema. □

Um outro lema importante é o apresentado a seguir:

Lema 4.1.2. Sejam a, b, c elementos quaisquer de um grupo G, cuja identidade é e. Valem as propriedades:

(a) Se $ab = ac$ então $b = c$.

(b) Se $aa = a$ então $a = e$.

(c) Se $ba = e$ então $ab = e$.

(d) $ae = ea = a$

(e) O elemento $e \in G$ é o único que verifica G2.

(f) Dado $a \in G$ existe um único $b \in G$ que verifica G3.

Demonstração. Seja $q \in G$ tal que $qa = e$. Então $q(ab) = q(ac)$ e, portanto, $(qa)b = (qa)c$, ou seja, $eb = ec$, o que implica $b = c$. Isso prova (a) e (b).

Para provar (c), seja $z = ab$. Então,

$$zz = (ab)(ab) = a(ba)b = aeb = ab = z,$$

e, assim, pelo item (b), $z = e$. Para o item (e), suponhamos que exista outro elemento $e' \in G$ verificando

$$e'a = a, \quad \forall a \in G.$$

Então, em particular,$e'e' = e'$ e, por (b), $e = e'$. Para o item (d), tomamos $q \in G$ verificando $qa = e$. Então,

$$ae = a(qa) = (aq)a = ea = a,$$

pelo item (c). Finalmente, se $ba = ca = e$, então

$$b = be = b(ca) = b(ac) = ec = c,$$

o que prova (f).

□

Ao lidarmos com os elementos de um grupo G é conveniente definirmos as *potências* de um elemento $a \in G$ do seguinte modo:

1. $a^o = e$,
2. Se $n \in \mathbb{Z}$, $n \geq 1$, então $a^n = a^{n-1}a$,
3. Se $n \in \mathbb{Z}$, $n \geq 1$, então $a^{-n} = (a^{-1})^n$.

Com base nessa definição, apresentamos o seguinte lema:

Lema 4.1.3. Se $m, n \in \mathbb{Z}$ e $a \in G$ então:

1. $a^m a^n = a^{m+n}$
2. $(a^m)^n = a^{mn}$

Demonstração. Considere um grupo G com um elemento $a \in G$ e inteiros $m, n \in \mathbb{Z}$. Demonstraremos que $a^m a^n = a^{m+n}$ e $(a^m)^n = a^{mn}$ usando o princípio da indução finita.

1. $a^m a^n = a^{m+n}$

   Para $n = 1$, tempos que $a^m a^1 = a^m a = a^{m+1}$, o que mostra que a igualdade é verdadeira. No passo indutivo, seja $a^m a^n = a^{m+n}$ para um n fixo. Então, para $n+1$, temos $a^m a^{n+1} = a^m(a^n a) = a^{m+n}a = a^{(m+n)+1} = a^{m+(n+1)}$.

2. $(a^m)^n = a^{mn}$ Para $n = 1$, a igualdade é verdadeira já que $(a^m)^1 = a^{m \cdot 1} = a^m$. No passo indutivo, seja $(a^m)^n = a^{mn}$ para um n dado. Então, para $n+1$, temos $(a^m)^{n+1} = (a^m)^n a^m = a^{mn}a^m = a^{mn+m} = a^{m(n+1)}$,.

Portanto, $a^m a^n = a^{m+n}$ e $(a^m)^n = a^{mn}$ para quaisquer $a \in G$ e inteiros $m, n \in \mathbb{Z}$.

□

Um grupo que particularmente nos interessa é o **grupo das permutações de um conjunto** X: tomamos $G = \mathscr{S}(X)$ o conjunto de todas as funções bijetoras $\phi : X \to X$, munido da operação de composição de funções. Então $\mathscr{S}(X)$ é um grupo, o qual se denomina *grupo de permutações* de X.

Se X for um conjunto finito com n elementos, denotamos $\mathscr{S}(X)$ simplesmente por $\mathscr{S}_n$, o qual será denominado de o *grupo simétrico em n elementos*.

Se $X = \{1, 2, 3, ..., n\}$ então um elemento f de $\mathscr{S}_n$ é uma função bijetora $f : X \to X$ que pode ser descrita designando-se os valores que assume em cada inteiro de X:

$$f(1) = a_1, f(2) = a_2, f(3) = a_3, ..., f(n) = a_n.$$

Alternativamente, podemos descrever essa permutação f por uma tabela:

$$\begin{pmatrix} 1 & 2 & \dots & j & \dots & n \\ a_1 & a_2 & \dots & a_j & \dots & a_n \end{pmatrix}.$$

Nessa representação está indicada a permutação que se pretende realizar, de modo que o elemento que está na posição ou ordem indicada por a_1 vai para a primeira posição, o que está na posição ou ordem indicada por a_2 vai para a segunda posição, e assim sucessivamente.

Assim, todas as permutações em $\mathscr{S}_3$ podem ser exibidas por essa forma:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Percebe-se assim que o último elemento $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ é obtido da permutação fundamental (123), de modo que seu terceiro elemento (3) ocupe a primeira posição, o primeiro elemento (1) ocupe a segunda a posição e o segundo elemento (2) ocupe a terceira posição.

Subgrupos

Um subgrupo é um subconjunto de um grupo que forma um grupo com a operação herdada do grupo maior.

Neste seção, apresentaremos o conceito de Subgrupos e algumas de suas propriedades seguindo Martin (2010, p. 8).

Um subconjunto H de um grupo G é dito *um subgrupo* de G se verificar:

S.1 H é não vazio.

S.2 $\forall a, b \in H$, temos $ab \in H$.

S.3 $\forall a \in H$, temos $a^{-1} \in H$.

Usando a notação $H \leq G$ para indicar que H é subgrupo de G, temos que os subgrupos óbvios $\{e\} \leq G$ e $G \leq G$ de um grupo G são chamados de *subgrupos triviais*.

Lema 4.1.4. Se H e K são subgrupos e um grupo G, então $H \cap K$ é um subgrupo de G. Mais geralmente, se $\{H_\alpha\}_{\alpha \in A}$ é uma família qualquer de subgrupos de G, então a intersecção $\cap H_\alpha$ é um subgrupo de G.

Definição 4.1.1. (de subgrupo gerado)

Se S é um subconjunto não vazio de um grupo G, definimos o **subgrupo gerado por** S, denotado $\langle S\rangle$, por:

$$\langle S\rangle = \bigcap\{H : H \leq G \text{ e } S \subseteq H\}.$$

Assim, $\langle S\rangle$ é o *menor* subgrupo de G que contém o subconjunto S.

O lema 4.1.4 garante que $\langle S\rangle$ é um subgrupo de G e seus elementos podem ser escritos explicitamente.

Lema 4.1.5. Se S é um subconjunto não vazio de um grupo G, então

$$\langle S\rangle = \{a_1a_2\cdots a_n : a_j \in S \text{ ou } a_j^{-1} \in S \quad n \geq 1\}$$

Demonstração. Na igualdade do enunciado, o subconjunto do lado direito é um subgrupo que contém S, e, portanto, contém $\langle S\rangle$. A inclusão oposta é clara. □

Proposição 4.1.1. Seja a um elemento de um grupo G. Então,

1. $\langle a\rangle = \{\cdots, a^{-2}, a^{-1}, e, a, a^2, cdots\}$.
2. Se $a^m = e$, para certo $m \geq 1$ e $\{e, a, a^2, \cdots, a^{m-1}\}$ forem disjuntos, então

$$\langle a\rangle = \{e, a, a^2, \cdots, a^{m-1}\}.$$

Nesse caso, $a^n = a^p$ se, e somente se, $n \equiv p\ mod\ m$, de onde $a^t = e$ se, e somente se, $m \mid t$.

Demonstração.

1. Basta tomar $S = \{a\}$ no lema 4.1.5.
2. Dado que $a^{m-1}a = a^m = e$, temos que $a^{-1} = a^{m-1}$, pela unicidade do inverso. Assim, basta mostrar que todas as potências positivas a^k estão em $\{e, a, a^2, \cdots, a^{m-1}\}$. Se $k \geq m$, a divisão euclidiana fornece $k = qm + r$, com $q, r \in \mathbb{N}$ e $0 \leq r < m$, de onde $a^k = a^{qm}a^r = (a^m)^q a^r = a^r$. Portanto, $\langle a\rangle = \{e, a, a^2, \cdots, a^{m-1}\}$. Se $a^n = a^p$ (podemos supor que n>p) então $a^{n-p} = e$ e, por hipótese, $n - p \geq m$. A divisão euclidiana fornece $n - p = qm + r$, com $0 \leq r < m$, obtemos $a^r = e$, de onde $r = 0$, ou seja, $n \equiv p\ mod\ m$.

□

Definição 4.1.2. (de subgrupo cíclico, de grupo cíclico, grupo finito e de ordem)

Um subgrupo G da forma $\langle a \rangle$ é chamado **um subgrupo cíclico** de G. Se $G = \langle g \rangle$ dizem que G é um **grupo cíclico**. Um grupo G é dito um **grupo finito** se G, como conjunto, for um conjunto finito. Nesse caso, o número de seus elementos é denotado por $\mid G \mid$ e denominado **a ordem** de G. Dizemos que $a \in G$ é um **elemento de ordem finita** se $\langle a \rangle$ for um grupo finito. Nesse caso, o número $\mid \langle a \rangle \mid$ é chamado de **a ordem de** a, e denotado por $\mid a \mid$.

Proposição 4.1.2. Um grupo não trivial G que só possui como subgrupos os subgrupos triviais, é um grupo finito cíclico cuja ordem é um número primo.

Demonstração. Se $g \in G$, com $g \neq e$, então, por hipótese, $G = \langle g \rangle$, o que prova que G é cíclico. Se G não fosse finito, então $H = \langle g^2 \rangle$ seria um subgrupo não trivial de G; portanto, G é finito. Se $\mid G \mid = k = l\,m$, com $l > 1$ e $m > 1$, pondo $h = g^l$, então $h \neq e$ e $h^m = e$ com $2 \leq \mid h \mid \leq m$ pela proposição 4.1.1. Como isso é impossível, k é primo. □

Coclasses (ou Classes Laterais)

Definição 4.1.3. (de coclasse à direita e à esquerda)

Se H é um subgrupo de um grupo G e $x \in G$, o subconjunto de G

$$Hx = \{hx : h \in H\}$$

é chamado de uma **coclasse (à direita) de** H **em** G. Analogamente, podemos definir uma **coclasse à esquerda** de H em G.

Quando o conjunto das coclasses (à direita ou à esquerda) de H em G for finito, dizemos que H é um subgrupo de *índice finito* em G, e o número de coclasses é chamado o **índice** de H em G, e denotado por $\mid G : H \mid$.

Lema 4.1.6. Seja H um subgrupo de um grupo G e suponha que $g_1.g_2 \in G$. Então, as seguintes proposições são equivalentes:

1. $g_1 H = g_2 H$
2. $H g_1^{-1} = H g_2^{-1}$
3. $g_1 H \subset g_2 H$
4. $g_2 \in g_1 H$
5. $g_1^{-1} g_2 \in H$

Demonstração.

- $(1) \to (2)$

  Se $g_1H = g_2H$, então para cada $gh \in g_1H$, existe um $g_2h' \in g_2H$ e vice-versa. Multiplicando à direita por g_1^{-1} e g_2^{-1} respectivamente, obtemos $H = g_1^{-1}g_2H$ e $H = g_2^{-1}g_1H$. Portanto, $Hg_1^{-1} = Hg_2^{-1}$.

- $(2) \to (3)$

  Se $Hg_1^{-1} = Hg_2^{-1}$, então g_1^{-1} e g_2^{-1} estão na mesma coclasse à esquerda de H. Logo, $g_1H \subset g_2H$.

- $(3) \to (4)$

  Se $g_1H \subset g_2H$, então $g_1 \in g_2H$. Portanto, $g_2 \in g_1H$.

- $(4) \to (5)$

  Se $g_2 \in g_1H$, então existe um $h \in H$ tal que $g_2 = g_1h$. Multiplicando por g_1^{-1}, temos $g_1^{-1}g_2 = h \in H$.

- $(5) \to (1)$

  Se $g_1^{-1}g_2 \in H$, então para cada $h' \in H$, $g_2h' = g_1(g_1^{-1}g_2h') \in g_1H$. Portanto, $g_1H = g_2H$.

□

Teorema 4.1.7. Seja H um subgrupo de um grupo G. Então:

(a) Todo elemento de G está contido numa coclasse de H em G.

(b) Duas coclasses distintas não possuem elementos em comum.

(c) Duas coclasses quaisquer possuem a mesma cardinalidade.

(d) Dois elementos $x, y \in G$ estão na mesma coclasse de H se, e somente se, $xy^{-1} \in H$.

(e) O grupo G é particionado numa união disjunta de coclasses de H.

Demonstração.

(a) Para qualquer $g \in G$, definimos a coclasse esquerda gH. Como H é um subgrupo, ele contém o elemento identidade e, e $ge = g$ está em gH.

(b) Suponha que gH e $g'H$ tenham um elemento em comum. Então $gh = g'h'$ para algum $h, h' \in H$, o que implica $g = g'h'h^{-1}$. Como $h'h^{-1} \in H$, g e g' estão na mesma coclasse.

(c) Definimos uma bijeção entre gH e $g'H$ por $f(gh) = g'h$, que é injetiva e sobrejetiva, o que mostra que as coclasses têm a mesma cardinalidade.

(d) Se x e y estão na mesma coclasse então $xy^{-1} \in H$. Além disso, $x = gh$ e $y = gh'$ para algum $g \in G$, $h, h' \in H$ e $xy^{-1} = ghh^{-1} \in H$. Idem para a recíproca.

(e) Cada elemento de G está em uma coclasse de H, coclasses distintas são disjuntas, e todos os elementos de G estão em alguma coclasse, formando uma partição de G.

□

Se H é um subgrupo de um grupo G, é usual denotarmos o conjunto das coclasses de H em G por G/H. Em consequência deste teorema, temos:

Teorema 4.1.8. (Lagrange) Se G é um grupo finito e H é um subgrupo de G então

$$| G | = | H | | G : H |$$

Demonstração. Pelo item (e) do teorema 4.1.7, G é particionado em $| G : H |$ coclasses distintas e, pelo item (c), todas as coclasses possuem a mesma cardinalidade, a saber, $| H |$. □

Corolário 4.1.1. Se H é um subgrupo de um grupo finito G então a ordem de H divide a ordem de G.

Demonstração. Considere G um grupo finito e H um subgrupo de G. Vamos demonstrar que a ordem de H (denotada como $|H|$) divide a ordem de G (denotada como $|G|$).

Pela definição de subgrupo, H contém pelo menos o elemento identidade de G, então $|H| \geq 1$. Além disso, $|H| \leq |G|$ pois H é um subconjunto de G.

O grupo G pode ser particionado em coclasses de H. Uma coclasse de H em G é um conjunto da forma $gH = \{gh : h \in H\}$ para algum $g \in G$. Pela propriedade de coclasses, todas as coclasses de H em G têm a mesma cardinalidade, igual à ordem de H.

Sejam $g_1H, g_2H, \ldots, g_nH$ as coclasses distintas de H em G, em que $n \in \mathbb{Z}$ é o número total de coclasses. Então, G é a união disjunta dessas coclasses:

$$G = g_1H \cup g_2H \cup \ldots \cup g_nH.$$

A ordem de G é a soma das cardinalidades dessas coclasses. Como cada coclasse tem $|H|$ elementos, a ordem de G é $n \times |H|$.

Portanto, $|G| = n \times |H|$, o que implica que $|H|$ divide $|G|$. Assim, a ordem de H divide a ordem de G. □

Corolário 4.1.2. Um grupo finito de ordem prima p é cíclico e só possui os subgrupos triviais.

Demonstração. Seja G um grupo finito de ordem p, sendo p um número primo. Verifiquemos:

- **Que G é cíclico:**
  Seja g um elemento de G diferente da identidade e. Consideramos o subgrupo gerado por g, denotado por $\langle g \rangle$. Por definição, $\langle g \rangle$ contém todos os elementos da forma g^n para $n \in \mathbb{Z}$.

  Como G é finito, $\langle g \rangle$ também é finito. Então, deve existir um menor inteiro positivo n tal que $g^n = e$. Pela ordem de G ser p e p ser primo, a ordem de g deve ser p, caso contrário, haveria um divisor de p menor que p e maior que 1, o que contradiz a hipótese de que p é primo. Portanto, $\langle g \rangle = G$ e G é cíclico.

- **Que possui apenas subgrupos triviais:**
  Se H é um subgrupo de G, então a ordem de H divide a ordem de G (pelo teorema de Lagrange). Mas os únicos divisores de p são 1 e p, pois p é primo. Portanto, H deve ter ordem 1 (sendo $\{e\}$) ou ordem p (sendo G). Assim, os únicos subgrupos de G são os subgrupos triviais.

□

Corolário 4.1.3. Num grupo finito G a ordem de qualquer elemento $a \in G$ divide $\mid G \mid$.

Demonstração. Considere G um grupo finito e a um elemento de G. Vamos demonstrar que a ordem de a divide a ordem de G, denotada por $|G|$. Seja $o(a)$ a ordem de a, definida como o menor número inteiro positivo tal que $a^{o(a)} = e$, sendo e o elemento neutro de G. Seja o subgrupo de G gerado por a, denotado por $\langle a \rangle$. Este subgrupo consiste em todos os elementos da forma a^n, para n inteiro. De acordo com o teorema de Lagrange, a ordem de um subgrupo de G divide a ordem de G. Daí, a ordem de $\langle a \rangle$, que é igual a $o(a)$, divide $|G|$. Logo, $o(a)$ divide $|G|$. □

Corolário 4.1.4. Se G é um grupo finito de ordem m então para qualquer $g \in G$ temos que $g^m = e$.

Demonstração. Consideremos um grupo finito G de ordem m. Demonstraremos que para qualquer elemento $g \in G$, vale que $g^m = e$, onde e é o elemento neutro de G. Seja g um elemento arbitrário de G. Pela teoria dos grupos, sabemos que a ordem de um elemento g, denotada por $o(g)$, é o menor número inteiro positivo tal que $g^{o(g)} = e$. Pelo teorema de Lagrange, a ordem de qualquer elemento de G divide a ordem do grupo, logo $o(g)$ divide m. Isso implica que existe um número inteiro k tal que $m = k \cdot o(g)$. Considerando a propriedade das potências em grupos, temos $g^m = g^{k \cdot o(g)} = (g^{o(g)})^k$. Mas sabemos que $g^{o(g)} = e$, e portanto, $(g^{o(g)})^k = e^k = e$. Assim, para qualquer elemento g em G, $g^m = e$. □

Grupo Quociente

O conceito de grupo quociente emergiu no final do século XIX e início do século XX, à medida que a teoria dos grupos se desenvolvia. Galois havia introduzido ideias relacionadas

ao conceito em seus estudos de equações polinomiais, mas foram os trabalhos de matemáticos como Felix Klein e Sophus Lie[6] que solidificaram o conceito, especialmente no contexto dos grupos de Lie e da geometria algébrica.

Definição 4.1.4. (de Grupo Normal) Um subgrupo H de um grupo G é denominado normal em G se uma — e, portanto, todas — das condições abaixo, que são equivalentes, forem satisfeitas para todo $x \in G$.

1. $Hx = xH$.
2. $xHx^{-1} = H$.
3. $xHx^{-1} \subset H$.

Escreveremos $H \lhd G$ para dizer que H é um subgrupo normal de G.

Proposição 4.1.3. Todo subgrupo de um grupo abeliano[7] é um subgrupo normal.

Demonstração. Considere um grupo abeliano G e um subgrupo H de G. Para mostrar que H é normal, precisamos provar que para todo $g \in G$ e $h \in H$, os elementos ghg^{-1} e $g^{-1}hg$ também pertencem a H. Como G é abeliano, todos os elementos comutam, ou seja, para quaisquer $x, y \in G$, temos $xy = yx$. Portanto, para $g \in G$ e $h \in H$, temos:

$$ghg^{-1} = g^{-1}gh = hgg^{-1} = he = h,$$

em que e é o elemento neutro de G. Da mesma forma, podemos mostrar que $g^{-1}hg = h$. Como $h \in H$ e H é um subgrupo de G, então ghg^{-1} e $g^{-1}hg$ também pertencem a H. Portanto, concluímos que $H \lhd G$ quando G é abeliano, pois a conjugação de qualquer elemento de H, por qualquer elemento de G, resulta em um elemento que ainda está em H. □

Teorema 4.1.9. Se H é um subgrupo normal de um grupo G, então o conjunto das coclasses G/H tem estrutura de grupo relativamente ao produto natural

$$(Hx)(Hy) = Hxy.$$

O elemento neutro é a coclasse H e o inverso da coclasse Hx é a coclasse Hx^{-1}.

[6] Sophus Lie (1842-–1899) foi um matemático norueguês que se destacou por suas contribuições à teoria dos grupos e à geometria diferencial. É conhecido por seu trabalho pioneiro na teoria dos grupos de Lie, que são uma classe de grupos contínuos fundamentais na análise matemática e na física teórica.

[7] Se $x, y \in G$ são dois elementos tais que $xy = yx$, dizemos que eles *comutam*. Um grupo em que dois quaisquer elementos comutam é chamado de *grupo comutativo* ou *grupo abeliano*.

Demonstração. Demonstraremos que, se H é um subgrupo normal de um grupo G, então o conjunto das coclasses G/H tem estrutura de grupo com o produto natural definido por $(Hx)(Hy) = Hxy$. O elemento neutro é a coclasse H e o inverso da coclasse Hx é a coclasse Hx^{-1}. Seja G um grupo e H um subgrupo normal de G. Consideramos o conjunto de coclasses G/H formado pelas coclasses esquerdas de H em G. Primeiramente, mostramos que a operação definida é bem definida em G/H. Para $x,y,x',y' \in G$ tais que $Hx = Hx'$ e $Hy = Hy'$, temos que $x' \in Hx$ e $y' \in Hy$, o que implica $x' = hx$ e $y' = hy$ para alguns $h_1, h_2 \in H$. Como H é normal em G, segue que $x'h_2 \in Hx$ e, portanto, $Hx'Hx = Hxh_2$. Da mesma forma, $Hy'Hy = Hyy'$. Assim, $(Hx')(Hy') = Hx'y' = Hxy = (Hx)(Hy)$. A operação é associativa, pois para quaisquer $x,y,z \in G$, temos $((Hx)(Hy))(Hz) = (Hxy)(Hz) = H(xy)z = Hx(yz) = (Hx)(Hyz) = (Hx)((Hy)(Hz))$. O elemento neutro é a coclasse H pois para qualquer $x \in G$, $(Hx)H = Hx = H(Hx)$. Para cada coclasse Hx, a coclasse Hx^{-1} é o inverso, pois $(Hx)(Hx^{-1}) = Hxx^{-1} = H = Hx^{-1}x = (Hx^{-1})(Hx)$. Portanto, G/H com a operação definida é um grupo, onde cada elemento é uma coclasse de H em G.

□

Exemplo 4.1.2. Apresentamos três exemplos clássicos de grupos quocientes:

1. O Grupo Quociente $\mathbb{Z}/n\mathbb{Z}$:

   O grupo dos inteiros $\mathbb{Z}$ sob a operação de adição é um exemplo de grupo abeliano. Consideremos $n\mathbb{Z}$, o subgrupo de $\mathbb{Z}$ formado pelos múltiplos de um inteiro fixo n. O grupo quociente $\mathbb{Z}/n\mathbb{Z}$ é formado pelas coclasses de $n\mathbb{Z}$ em $\mathbb{Z}$ e representa os restos da divisão por n, sendo um exemplo fundamental de um grupo finito.

2. O Grupo Quociente $\mathbb{R}/\mathbb{Z}$:

   O grupo $\mathbb{R}$ dos números reais sob a operação de adição também é um grupo abeliano. O subgrupo $\mathbb{Z}$ de $\mathbb{R}$ consiste nos inteiros. O grupo quociente $\mathbb{R}/\mathbb{Z}$ é formado pelas coclasses de $\mathbb{Z}$ em $\mathbb{R}$ e pode ser visualizado como o círculo unitário, onde cada ponto no círculo representa uma coclasse.

3. O Grupo Quociente G/N com N Subgrupo Normal:

   Em um grupo G com um subgrupo normal N, o grupo quociente G/N é formado pelas coclasses de N em G. Este grupo quociente desempenha um papel crucial em muitos ramos da matemática, incluindo a teoria de grupos, a álgebra e a topologia.

Quando $H \lhd G$, o conjunto das coclasses, *com essa estrutura de grupo*, é chamado de **o grupo quociente** de G por H. No caso desse quociente ser um grupo finito, a sua ordem é o índice $|\ G\ :\ H\ |$ de H em G. Se o próprio G for finito, o teorema de Lagrange nos garante que

$$|\ G/H| = \frac{|\ G\ |}{|\ H\ |}.$$

Homomorfismo

O termo *homomorfismo* foi introduzido pelo matemático alemão Arthur Cayley, no século XIX, e se refere a um conceito fundamental na teoria dos grupos e na álgebra abstrata.

A ideia de homomorfismo surgiu naturalmente da necessidade de entender como as estruturas de grupo podem ser relacionadas e comparadas. Um homomorfismo de grupos é uma função entre dois grupos que preserva a operação de grupo.

Definição 4.1.5. Sejam $(G.\,\cdot\,)$ e $(G',\,*\,)$ dois grupos. Uma função $f : G \to G'$ satisfazendo

$$f(a \cdot b) = f(a) * f(b),$$

para todos os $a, b \in G$, é dita um homomorfismo de grupos. Um homomorfismo de grupos que, como função, é injetor, será chamado de *monomorfismo* de grupos. Se ele for sobrejetor, será chamado de um *epimorfismo* de grupos. Se o homomorfismo for uma bijeção, dizemos que f é um *isomorfismo* entre G e G'. Alternativamente, podemos dizer que G e G' são grupos isomorfos e utilizar a seguinte notação: $G \cong G'$.

Teorema 4.1.10. Sejam os grupos G e H. Se $f : G \to H$ é um isomorfismo de grupos, então a função inversa $f^{-1} : H \to G$ também é um isomorfismo.

Demonstração. Se $f : G \to H$ é um isomorfismo de grupos, então f é um homomorfismo bijetivo. Queremos mostrar que a função inversa $f^{-1} : H \to G$ é também um homomorfismo. Para ser um homomorfismo, f^{-1} deve preservar a operação de grupo. Sejam h_1, h_2 elementos arbitrários de H. Como f é bijetiva, existem elementos únicos $g_1, g_2 \in G$ tais que $f(g_1) = h_1$ e $f(g_2) = h_2$. Agora, considere $f^{-1}(h_1h_2)$. Como f é um homomorfismo, temos $f(g_1g_2) = f(g_1)f(g_2) = h_1h_2$. Já que f é bijetiva, $f^{-1}(h_1h_2) = g_1g_2$. Portanto, $f^{-1}(h_1h_2) = f^{-1}(h_1)f^{-1}(h_2)$, demonstrando que f^{-1} é um homomorfismo. Já que f^{-1} é uma função inversa de uma bijeção, f^{-1} é também bijetiva. Assim, f^{-1} é um isomorfismo, pois é um homomorfismo bijetivo. Portanto, se f é um isomorfismo, então f^{-1} também é um isomorfismo. □

Definição 4.1.6. Se $f : G \to G'$ é um homomorfismo de grupos, o subconjunto

$$ker(f) = \{g \in G : f(g) = e'\}$$

é chamado de *núcleo* de f. (Acima, e' é a identidade de G)

Teorema 4.1.11. Seja $f : G \to G'$ um homomorfismo de grupos. Então:

(a) $f(e) = e'$ e $f(x^{-1}) = f(x)^{-1}$.

(b) Se $H \leq G$ então $f(H) = \{f(h) : h \in H\} \leq G'$.

(c) Se $K \leq G'$, então $f^{-1}(K) := \{x \in G : f(x) \in K\} \leq G$.

(d) Em particular, se $K = \{e'\}$ então $ker(f) \leq G$.

(e) $f(x) = f(y) \iff xy^{-1} \in ker(f)$.

(f) Em particular, f é injetora se, e somente se, $ker(f) = \{e\}$.

(g) Se $K \lhd G'$, então $f^{-1}(K) \lhd G$.

Demonstração.

(a) Para o elemento neutro e em G, temos $f(e) = f(ee) = f(e)f(e)$, o que implica que $f(e)$ é um elemento neutro em G', ou seja, $f(e) = e'$. Para $f(x^{-1}) = f(x)^{-1}$, note que $e' = f(e) = f(xx^{-1}) = f(x)f(x^{-1})$, logo $f(x^{-1})$ é o inverso de $f(x)$ em G'.

(b) Se $H \leq G$, então $f(H) = \{f(h) : h \in H\}$ é um subconjunto de G'. A operação de grupo em G' é fechada em $f(H)$, e o elemento neutro e os inversos estão presentes, portanto $f(H) \leq G'$.

(c) Para $K \leq G'$, definimos $f^{-1}(K) := \{x \in G : f(x) \in K\}$. Mostramos que $f^{-1}(K)$ é um subgrupo de G. A operação de grupo em G é fechada em $f^{-1}(K)$, o elemento neutro está presente, e os inversos também, então $f^{-1}(K) \leq G$.

(d) Em particular, para $K = \{e'\}$, temos que $ker(f) = f^{-1}(\{e'\}) \leq G$, já que $ker(f)$ é o conjunto de elementos em G que são mapeados para o elemento neutro em G'.

(e) Para $f(x) = f(y) \iff xy^{-1} \in ker(f)$, observe que $f(x) = f(y)$ implica $e' = f(x)f(y)^{-1} = f(xy^{-1})$, então $xy^{-1} \in ker(f)$. Idem para a recíproca.

(f) Em particular, f é injetora se, e somente se, $ker(f) = \{e\}$. Se $ker(f) = \{e\}$, então $f(x) = f(y)$ implica $xy^{-1} = e$, ou seja, $x = y$. Se f é injetora, então $f(x) = e'$ implica $x = e$, portanto $ker(f) = \{e\}$.

(g) Se $K \lhd G'$, então para qualquer $x \in f^{-1}(K)$ e $g \in G$, temos $f(gxg^{-1}) = f(g)f(x)f(g)^{-1} \in K$, já que K é normal em G', o que implica $gxg^{-1} \in f^{-1}(K)$, portanto $f^{-1}(K) \lhd G$.

□

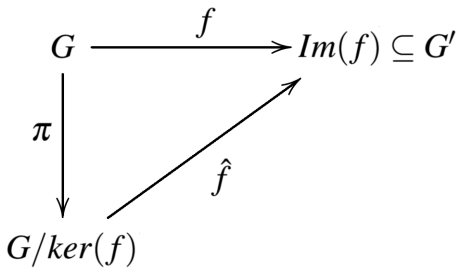
No item (b) acima, quando $H = G$, o subgrupo f(G) é chamado de *imagem* do homomorfismo f, e é denotado por $Im(f)$. Os itens (d), (e) e (f) garantem que $ker(f)$ é um subgrupo que mede quão longe f está de ser injetora.

Teorema 4.1.12. (Teorema do Isomorfismo I)

Seja $f : G \to G'$ um homomorfismo de grupos. Então:

(a) ker(f) é um subgrupo normal de G.

(b) Existe um único isomorfismo $\hat{f} : G/ker(f) \to Im(f)$ que faz comutar o diagrama[8]:



Demonstração.

(a) O núcleo de f, definido por $\ker(f) = \{g \in G : f(g) = e'\}$, onde e' é o elemento neutro em G', é um subgrupo de G pois contém o elemento neutro de G, é fechado sob a operação de grupo, e contém os inversos de seus elementos. Além disso, para qualquer $g \in G$ e $x \in \ker(f)$, $f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)e'f(g)^{-1} = f(g)f(g)^{-1} = e'$, o que mostra que $gxg^{-1} \in \ker(f)$ e, portanto, $\ker(f)$ é normal em G.

(b) Definimos $\hat{f}\ (g\ \ker(f)) = f(g)$. Esta função está bem definida: se $g\ \ker(f) = g'\ \ker(f)$, então $g^{-1}g' \in \ker(f)$, implicando $f(g) = f(g')$. A função $\hat{f}$ é um homomorfismo, pois $\hat{f}((g\ \ker(f))(h\ \ker(f))) = \hat{f}(g\ h\ \ker(f)) = f(gh) = f(g)f(h) = \hat{f}(g\ \ker(f))\hat{f}(h\ \ker(f))$. $\hat{f}$ é sobrejetiva por definição, e é injetiva: se $\hat{f}(g\ \ker(f)) = e'$, então $f(g) = e'$, implicando $g \in \ker(f)$. Resta mostrar a unicidade de $\hat{f}$. Suponha que exista um isomorfismo $\psi : G/\ker(f) \to \mathrm{Im}(f)$ tal que $\psi \circ \pi = f$. Para todo $g\ker(f) \in G/\ker(f)$, temos $\psi(g\ \ker(f)) = (\psi \circ \pi)(g) = f(g) = \hat{f}(g\ \ker(f))$. Portanto, $\psi = \hat{f}$, estabelecendo a unicidade de $\hat{f}$.

□

Lema 4.1.13. Sejam H e K subgrupos de um grupo G. Então:

(a) $HK = \{hk : h \in H, k \in K\} \leq G$ se, e somente se, $HK = KH$.

(b) Se $H \lhd G$ ou $K \lhd G$ então $HK \leq G$.

(c) Se $H \lhd G$ e $K \lhd G$ então $HK \lhd G$.

(d) Se $S = H \cup K$ e $H \lhd G, K \lhd G$ então $\langle S \rangle \lhd G$.

Demonstração.

[8] Dizer que esse diagrama *comuta* é dizer que $\hat{f} \circ \pi = f$.

(a) ($\Rightarrow$) Para HK ser um subgrupo de G, ele deve ser fechado sob a operação de grupo e conter inversos. Se $HK = KH$, então para quaisquer $h \in H$ e $k \in K$, $hk \in HK$ implica $kh \in KH = HK$, mostrando que HK é fechado. Os inversos também estão em HK pois $(hk)^{-1} = k^{-1}h^{-1}$ e $k^{-1}h^{-1} \in KH = HK$.
($\Leftarrow$) Reciprocamente, para mostrar que, se $HK = KH$ então $HK \leq G$, devemos provar que HK é fechado sob a operação do grupo e contém o inverso de cada um de seus elementos. Para mostrar que HK é fechado sob a operação do grupo, consideremos quaisquer $h_1k_1, h_2k_2 \in HK$ para $h_1, h_2 \in H$ e $k_1, k_2 \in K$. Temos $h_1k_1h_2k_2 = h_1(k_1h_2)k_2$. Como $HK = KH$, existe $h_3 \in H$ e $k_3 \in K$ tal que $k_1h_2 = h_3k_3$, assim $h_1k_1h_2k_2 = h_1h_3k_3k_2$. Como H e K são subgrupos, $h_1h_3 \in H$ e $k_3k_2 \in K$, portanto $h_1k_1h_2k_2 \in HK$. Para mostrar que cada elemento de HK tem um inverso em HK, considere um elemento $hk \in HK$ para $h \in H$ e $k \in K$. O inverso de hk em G é $(hk)^{-1} = k^{-1}h^{-1}$. Como $HK = KH$, existe $h' \in H$ e $k' \in K$ tal que $k^{-1}h^{-1} = h'k'$. Portanto, $k^{-1}h^{-1} \in HK$, mostrando que o inverso de cada elemento de HK também está em HK. Portanto, HK é um subgrupo de G quando $HK = KH$.

(b) Se $H \lhd G$, então para todo $g \in G$ e $h \in H$, $ghg^{-1} \in H$. Similarmente, se $K \lhd G$, então para todo $g \in G$ e $k \in K$, $gkg^{-1} \in K$. Em ambos os casos, HK é fechado sob a operação de grupo e contém inversos, portanto $HK \leq G$.

(c) Se $H \lhd G$ e $K \lhd G$, então para todo $g \in G$, $g(HK)g^{-1} = (gHg^{-1})(gKg^{-1}) \subset HK$, mostrando que $HK \lhd G$.

(d) Se $S = H \cup K$ e $H \lhd G, K \lhd G$, então $\langle S \rangle$ é normal em G. Isso ocorre porque $\langle S \rangle$ contém todos os produtos de elementos de H e K e seus inversos, e como H e K são normais, $\langle S \rangle$ é fechado sob conjugação por elementos de G, logo $\langle S \rangle \lhd G$.

□

Teorema 4.1.14. (do Isomorfismo II) Sejam H e K subgrupos de um grupo G com $H \lhd G$. Então,

(a) $H \cap K \lhd K$.

(b) $K/H \cap K \cong KH/H$.

Demonstração.

(a) Para $k \in K$ e $x \in H \cap K$, devemos mostrar que $kxk^{-1} \in H \cap K$. Como $x \in H$ e $H \lhd G$, temos $kxk^{-1} \in H$. Além disso, como $x \in K$ e K é um subgrupo de G, $kxk^{-1} \in K$. Portanto, $kxk^{-1} \in H \cap K$, o que prova que $H \cap K \lhd K$.

(b) Seja a função $\varphi : K \to KH/H$ definida por $\varphi(k) = kH$. Primeiro, mostramos que φ está bem definida. Para $k, k' \in K$, se $k(H \cap K) = k'(H \cap K)$, então $k^{-1}k' \in H \cap K \subset H$,

logo $kH = k'H$ em KH/H. A função φ é um homomorfismo, pois $\varphi(k_1k_2) = (k_1k_2)H = k_1Hk_2H = \varphi(k_1)\varphi(k_2)$. A função φ é sobrejetiva, pois cada elemento de KH/H tem a forma $khH = kH$ para algum $k \in K$. Para mostrar que φ é injetiva, consideramos $\varphi(k) = eH$. Isso implica $k \in H$, portanto $k \in H \cap K$. Logo, $\text{Ker}(\varphi) = H \cap K$, e pelo Primeiro Teorema do Isomorfismo, $K/(H \cap K) \cong KH/H$.

□

Se $f : G \to G'$ é um homomorfismo de grupos e K é um subgrupo normal de G contido no núcleo de f, então f induz um homomorfismo $f : G/\tilde{K} \to G'$, dado por $\tilde{f}(gK) = f(g)$. É claro que neste caso $\tilde{f}$ só será injetora caso $K = ker(f)$.

Teorema 4.1.15. (do Isomorfismo III)

Sejam H e K subgrupos normais de um grupo G com $K \subseteq H \subseteq G$. Então,

$$(G/K)/(H/K) \cong G/H.$$

Demonstração. Sejam os grupos quocientes G/K e H/K. Definimos a função $\varphi : G/K \to G/H$ por $\varphi(gK) = gH$. Primeiro, mostramos que φ está bem definida. Se $gK = g'K$ em G/K, então $g^{-1}g' \in K \subseteq H$, logo $gH = g'H$ em G/H. A função φ é um homomorfismo, pois para quaisquer $gK, hK \in G/K$, temos $\varphi((gK)(hK)) = \varphi(ghK) = ghH = gHhH = \varphi(gK)\varphi(hK)$. A função φ é sobrejetiva, pois para cada $gH \in G/H$, existe $gK \in G/K$ tal que $\varphi(gK) = gH$. Para mostrar que φ é injetiva, consideramos $\varphi(gK) = e_{G/H}$. Isso implica que $gH = H$, ou seja, $g \in H$. Assim, $gK \in H/K$, que é o núcleo de φ. Portanto, $\text{Ker}(\varphi) = H/K$. Pelo Primeiro Teorema do Isomorfismo, a existência de tal homomorfismo bijetivo φ com $\text{Ker}(\varphi) = H/K$ implica que $(G/K)/(H/K) \cong G/H$. Portanto, $(G/K)/(H/K) \cong G/H$ para subgrupos normais H e K de G com $K \subseteq H \subseteq G$.

□

O teorema a seguir permite descrever os subgrupos de um grupo quociente G/H em função dos subgrupos de G.

Teorema 4.1.16. (da Correspondência)

Seja G um grupo e $N \lhd G$ um subgrupo normal de G. Existe uma correspondência biunívoca entre os subgrupos de G/N e os subgrupos de G que contêm N.

Demonstração. Seja $\pi : G \to G/N$ a projeção natural de G sobre G/N. Para cada subgrupo H' de G/N, o conjunto $\pi^{-1}(H')$ é um subgrupo de G que contém N. De fato, como π é um homomorfismo, $\pi^{-1}(H')$ é fechado sob a operação de grupo e contém inversos. Além disso, $N \subseteq \pi^{-1}(H')$ pois $e_{G/N} \in H'$ e $\pi^{-1}(e_{G/N}) = N$. Por outro lado, para cada subgrupo H de G

que contém N, $\pi(H)$ é um subgrupo de G/N. A projeção π preserva a operação de grupo, logo $\pi(H)$ é fechado sob a operação do grupo quociente. Além disso, essas correspondências são inversas uma da outra. Para um subgrupo H' de G/N, $\pi(\pi^{-1}(H')) = H'$. E para um subgrupo H de G que contém N, $\pi^{-1}(\pi(H)) = H$. Portanto, existe uma correspondência biunívoca entre os subgrupos de G/N e os subgrupos de G que contêm N, conforme afirmado pelo Teorema da Correspondência.

□

4.2 Anéis e Corpos

Um anel é uma estrutura algébrica que generaliza alguns conceitos de aritmética, tendo o conceito surgido no final do século XIX. A noção de anel, como conhecemos hoje, foi formalizada principalmente por David Hilbert[9] e Richard Dedekind[10], que introduziu o termo *ring* — que significa *anel*, em alemão — em 1894 ao estudar as propriedades dos números inteiros. Contudo, o conceito já estava implícito no trabalho de outros matemáticos, como Ferdinand Georg Frobenius[11] e Leopold Kronecker[12], ao estudarem as matrizes e os números algébricos.

Neste seção, apresentaremos o conceito de Anéis e algumas de suas propriedades seguindo Griffiths e Hilton (1975) e Milies (1972).

Consideremos um conjunto não vazio R, munido de duas operações binárias denominadas *aditiva* e *multiplicativa* — denotadas por $(+)$ e $(\,.\,)$, respectivamente.

Essas operações são funções $R \times R \to R$ que, para todo a, b e c em R, satisfazem as seguintes condições:

A1. $a+(b+c) = (a+b)+c$ **(lei associativa da adição)**;

A2. $a+b = b+a$ **(lei comutativa da adição)**;

[9] David Hilbert (1862-–1943) foi um matemático alemão, considerado um dos mais influentes do final do século XIX e início do século XX. Notabilizou-se por sua lista de 23 problemas de matemática não resolvidos, apresentada no *Congresso Internacional de Matemáticos*, em Paris, em 1900. Esses "Problemas de Hilbert" nortearam a pesquisa matemática por muitas décadas, sendo fundamental para o desenvolvimento da matemática no século XX.

[10] Richard Dedekind (1831—1916) foi um matemático alemão, conhecido por suas contribuições em teoria dos números, álgebra e análise. Notabilizou-se pelos "*cortes de Dedekind*", subconjuntos do corpo ordenado de $\mathbb{Q}$ usados para construir um corpo ordenado completo arquimediano.

[11] Ferdinand Georg Frobenius (1849—1917) foi um matemático alemão conhecido por suas contribuições em teoria dos grupos, teoria dos números e álgebra linear.

[12] Leopold Kronecker (1823–1891) foi um matemático alemão, conhecido por suas contribuições em teoria dos números, álgebra e lógica matemática. Em particular, por desenvolver a teoria das extensões de corpos e por ter sido um dos primeiros a usar métodos algébricos para resolver equações polinomiais.

A3. Existe em R um elemento **zero** (denotado por 0), tal que, para todo $a \in R$, $a+0=a$; **(elemento neutro da adição)**;

A4. Para cada a em R existe um elemento (denotado por $-a$), tal que $a+(-a)=0$; **(elemento oposto)**;

M1. $a(bc)=(ab)c$ **(lei associativa da multiplicação)**;

M2. $a(b+c)=ab+ac$, $(a+b)c=ac+bc$ **(leis distributivas)**;

M3. $ab=ba$ **(lei comutativa da multiplicação)**;

M4. Existe em R um elemento unidade (denotado por 1) tal que para todo $a \in R$, $a \cdot 1 = 1 \cdot a = a$, além disso, $1 \neq 0$. **(existência da unidade)**;

Com frequência, utiliza-se a tripla $(R, +, \cdot)$ para denotar um conjunto R com operações binárias $(+)$ e $(\cdot)$. Qualquer tripla satisfazendo A1 a M2 é denominada *Anel*. Se satisfizer também M3, será um *anel comutativo*. Se satisfizer A1 a M2 e M4, chama-se *anel com elemento unidade*. Se satisfizer a todos os axiomas de A1 a M4, será denominado *anel comutativo com elemento unidade*. Um anel é chamado *anel de integridade* (ou *domínio de integridade*) se for comutativo, com unidade e valer:

D.1 Dados $a, b \in R$, se $a \cdot b = 0$ então $a = o$ ou $b = 0$.

Os axiomas A1 a M4 para um anel comutativo com unidade não nos permitem necessariamente efetuar divisões. Assim, nem sempre é possível resolver equações do tipo $ax = b$ num anel R, mesmo que $a \neq 0$. Por exemplo $3x = 1$ não tem solução em $\mathbb{Z}$. Em alguns sistemas aritméticos, entretanto, uma equação desse tipo sempre tem solução. A esses sistemas denominamos *corpos*.

Um conjunto $(F, +, \cdot)$ chama-se *corpo* se for um anel comutativo com elemento unidade e, para cada elemento não nulo x em F, existir em F um elemento, denotado por x^{-1}, tal que $x \cdot x^{-1} = 1$.

Proposição 4.2.1. Seja R um anel. Então, para quaisquer $a, b \in R$:

i) o zero 0 é univocamente determinado pela propriedade que $a+0=a$, isto é, a única solução em R da equação $a+x=a$ é $x=0$.

ii) o elemento $-a$ é univocamente determinado pela propriedade que $a+(-a)=0$, isto é, a única solução em R da equação $a+x=0$ é $x=-a$.

iii) $-(-a)=a; -0=0; -(a+b)=(-a)+(-b)$;

iv) $a0=0a=0$

v) $a(-b) = (-a)b = -(ab)$

vi) $(-a)(-b) = ab$

Demonstração.

i) Seja $x \in R$ tal que $a+x = a$. Por A2, $x+a = a$. Por A4, $(x+a)+(-a) = a+(-a)$. Por A1 e A4, $x+[a+(-a)] = 0$. Por A4 novamente, $x+0 = 0$. Por A3, conclui-se que $x = 0$.

ii) Seja $x \in R$ tal que $a+x = 0$. Por A2, $x+a = 0$. Por A4, $(x+a)+(-a) = 0+(-a)$. Por A1 e A4, $x+[a+(-a)] = -a$. Por A4, $x+0 = -a$. Por A3, conclui-se que $x = -a$.

iii) Por A4, $a+(-a) = 0$. Ou seja, $-a+[-(-a)] = 0$. Somando-se a à esquerda de cada lado da igualdade, temos: $a+[-a+[-(-a)]] = a+0$. Por A1 e A3, $[a+(-a)]+[-(-a)] = a$. Por A4, $0+[-(-a)] = a$. Por A3, conclui-se que $-(-a) = a$. Se $a = 0$, segue imediatamente que $-0 = 0$. Por fim, de $-(-a) = a$, temos: $-[-((-a)+(-b))] = (-a)+(-b)$. Segue imediatamente que $-(a+b) = (-a)+(-b)$.

iv) Seja $x \in R$ tal que $a+x = a$. Vamos mostrar que $x = 0$. De fato, pois por A4, $a+(-a) = 0$. Usando a hipótese, $(a+x)+(-a) = 0$. Por A2, $(x+a)+(-a) = 0$. Por A1, $x+[a+(-a)] = 0$. Por A4, $x+0 = 0$. Por A3, concluímos que $x = 0$. Para quaisquer $a, b \in R$. Por A3, $ab = a(0+b)$. Por M2, $ab = a0+ab$. Por A3, conclui-se que $a0 = 0$. Do mesmo modo, pode-se verificar que $0a = 0$ sem que seja necessário usar M3.

v) Por M2, A4 e (iv), $a(-b)+ab = a[(-b)+b] = a \cdot 0 = 0$. Como $ab+a(-b) = 0$, então $a(-b) = -(ab)$. Do mesmo modo, $(-a)b+ab = (-a+a)b = 0 \cdot b = 0$. Ou seja, $(-a)b = -(ab)$. E já que $a(-b)$ e $(-a)b$ são iguais a $-(ab)$, conclui-se que: $a(-b) = (-a)b = -(ab)$.

vi) Por (iv), $0 = (-a)0$. Por A4, $0 = (-a)[b+(-b)]$. Por M2, $(-a)b+(-a)(-b)$. Por (v), $0 = -ab+(-a)(-b)$. Por (iii), conclui-se que $(-a)(-b) = -(-ab) = ab$.

□

Definição 4.2.1. Um elemento a de um anel com unidade A diz-se invertível se existe um elemento, denotado por $a^{-1} \in A$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Diz-se que um anel comutativo com unidade é um *corpo* se todo elemento não nulo é inversível.

É fácil verificar que todo corpo é um anel de integridade.

A definição acima implica que se K é um corpo, o conjunto $K*$ dos elementos diferentes de zero é um grupo abeliano, exceto a comutativa do produto, diz-se um *anel com divisão.*

Definição 4.2.2. Seja A um anel e B um subconjunto de A. Diz-se que B é um *subanel* de A se verificar:

i) B é fechado em relação às operações de A (isto é, para todo $a, b \in B$, $a + b \in B$ e $a \cdot b \in B$)

ii) B é um anel em relação às operações induzidas por restrição das operações de A.

De forma semelhante, define-se a noção de *subcorpo*.

CAPÍTULO

5

SOLUBILIDADE POR RADICAIS

5.1 Solubilidade por Radicais

Segundo Stillwell (1994, p. 22), a Teoria de Galois é considerada o ápice da álgebra universitária. Nesse sentido, muito da álgebra moderna que se estuda na academia tem por finalidade demonstrar a insolubilidade por radicais de uma equação polinomial genérica de grau maior ou igual a cinco.

A despeito de conceitos como extensões normais, polinômios irredutíveis, corpos de decomposição serem indispensáveis no contexto acadêmico de um curso de álgebra, não faremos uso de tais conceitos para demonstrar o resultado almejado. Outrossim, também não utilizaremos o Teorema Fundamental da Teoria de Galois.

O objetivo desta seção será apresentar uma abordagem alternativa à referida questão, tendo por objetivo demonstrar a insolubilidade por radicais de uma equação polinomial genérica de grau maior ou igual a cinco. Para tanto, utilizaremos apenas conceitos relacionados a Grupos, Anéis e Corpos.

O ponto central dessa abordagem é considerar que se ϕ é um homomorfismo de um grupo G em um grupo G' então $G' \cong G\ ker\ \phi$ e, reciprocamente, se $G\ /\ H \cong G'$ então H é o núcleo de um homomorfismo de G em G'.

Para tanto, a demonstração será estruturada nas seguintes três ideias:

1. Corpos que contenham n indeterminadas podem ser “simetrizáveis”
2. O grupo Galois de uma extensão radical é solúvel.
3. O grupo simétrico S_n não é solúvel.

Iniciaremos essa discussão com a seguinte definição:

Definição 5.1.1. Uma equação polinomial de grau n é do tipo

$$x^n + a_{n-1}\, x^{n-1} + \cdots + a_1\, x + a_o = 0\,, \tag{5.1.1}$$

em que a_k são reais, com $k = 0, 1, 2, \cdots, n-1$

Sem perda de generalidade, para fins didáticos consideramos acima a equação cujo coeficiente líder — que é o coeficiente do termo de maior grau — é igual a um. Além de simplificar os cálculos, tal suposição se justifica porque, para um dado $a_n \neq 0$, a equação polinomial $a_n x^n + a_{n-1}\, x^{n-1} + \cdots + a_1\, x + a_o = 0$ pode ser dividida por a_n, resultando em uma equação do mesmo tipo daquela apresentada em 5.1.1.

Dado que qualquer equação polinomial de grau menor ou igual a quatro pode ser resolvida algebricamente — ou seja, por meio de um número finito de operações de soma, subtração, multiplicação, divisão, potenciação inteira e radiciação aplicadas a seus coeficientes —, é natural pensar que deve haver um método geral para resolver equações polinomiais de qualquer grau.

Nesse sentido, apresentaremos a seguir dois dos mais importantes teoremas da álgebra.

Teorema 5.1.1. Todo polinômio $P(x)$ de grau $n \geq 1$

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

pode ser fatorado como o produto de uma constante por polinômios de primeiro grau:

$$P(x) = a_n\, (x - r_1)(x - r_2) \cdots (x - r_n),$$

em que $r_1, r_2, \cdots r_n$ são todas as raízes de $P(x)$.

Demonstração. □

Teorema 5.1.2.

Demonstração. □

O conjunto de elementos obtidos de $a_o, \cdots a_{n-1}$ por $+$, $-$, $\times$, $\div$ é denominado o corpo $\mathbb{Q}(a_o, \cdots, a_{n-1})$.

Se denotarmos as soluções de 5.1.1 por $x_1, \cdots, x_n$, então, pelo teorema da decomposição[1] odemos escrever:

$$(x - x_1) \cdots (x - x_n) = x^n + a_{n-1}\, x^{n-1} + \cdots + a_1\, x + a_o\,,$$

[1] p

então $a_o, \cdots, a_{n-1}$ são funções polinomiais de $x_1, \cdots, x_n$ denominadas *funções simétricas elementares*:

$$a_o = (-1)^n \, x_1 \, x_2 \cdots x_n \cdots, a_{n-1} = -(x_1 \, + \, x_2 \, + \, \cdots \, + \, x_n)$$

O objetivo de se obter a solução por radicais é estender $\mathbb{Q}(a_o, \cdots, a_{n-1})$ por meio de adjunção de radicais até que o corpo contendo as raízes $x_1, \cdots, x_n$ seja obtido.

Para ilustrar, apresentaremos o exemplo dado por Stillwell (1994, p. 23):

Exemplo 5.1.1. As raízes x_1 e x_2 de uma equação quadrática estão na extensão de $\mathbb{Q}(a_o, a_1) = \mathbb{Q}(x_1, x_2, x_1 + x_2)$ pelo radical:

$$\sqrt{a_1^2 - 4a_o} = \sqrt{(x_1 + x_2)^2 - 4x_1x_2} = \sqrt{(x_1 - x_2)^2} = \pm(x_1 - x_2)$$

Nesse caso, consideramos $\mathbb{Q}(x_1, x_2)$ como sendo a própria extensão radical

$$\mathbb{Q}\left(a_o, a_1, \sqrt{a_1^2 - 4a_o}\right),$$

embora existam casos em que uma extensão radical de $\mathbb{Q}(a_o, \cdots, a_{n-1})$ contendo $x_1, \cdots, x_n$ é maior do que $\mathbb{Q}(x_1, \cdots, x_n)$.

Um exemplo seria o caso das equações cúbicas, cuja solução fornece uma extensão radical de $\mathbb{Q}(a_o, a_1, a_2)$ que inclui raízes cúbicas imaginárias da unidade, assim como x_1, x_2, x_3.

De modo geral, a adjunção de um elemento α a um corpo F representa o fechamento de $F \cup \{\alpha\}$ sob as operações $+$, $-$, $\times$ e $\div$ (por um elemento não nulo); ou seja, tomando a interseção de todos os corpos contendo $F \cup \{\alpha\}$. A essa adjunção dá-se o nome de *radical* se alguma potência inteira positiva α^m de α igual a um elemento $f \in F$, situação em que α pode ser representado pela expressão radical $\sqrt[m]{f}$.

Assim, denotamos por $F(\alpha_1, \cdots, \alpha_k)$ o resultado $F(\alpha_1)(\alpha_2) \cdots (\alpha_k)$ das sucessivas adjunções. Se cada adjunção for um radical, diremos que $F(\alpha_1, \cdots, \alpha_k)$ é uma extensão radical de F.

Desse modo, uma extensão radical E de $\mathbb{Q}(a_o, \cdots, a_{n-1})$ contendo $x_1, \cdots, x_n$ é também uma extensão radical de $\mathbb{Q}(x_1, \cdots, x_n)$, desde que $a_o, \cdots a_{n-1} \in \mathbb{Q}(x_1, \cdots, x_n)$. Logo, precisaremos também estudar as extensões radicais de $\mathbb{Q}(x_1, \cdots, x_n)$, pois uma de suas principais propriedades é que é *simétrica* em relação a $x_1, \cdots, x_n$, no sentido de que qualquer permutação σ de $x_1, \cdots, x_n$ estende a bijeção σ de $\mathbb{Q}(x_1, \cdots, x_n)$ definida por:

$$\sigma \, f(x_1, \cdots, x_n) = f(\sigma x_1, \cdots, \sigma x_n) \, ,$$

para cada função racional f de $x_1, \cdots, x_n$.

Assim, trata-se de um automorfismo de $\mathbb{Q}(x_1, \cdots, x_n)$ uma vez que essa bijeção satisfaz:

$$\sigma(f+g) = \sigma f + \sigma g$$

$$\sigma(fg) = \sigma\, f \cdot \sigma\, g$$

Nesse sentido, uma extensão radical E de $\mathbb{Q}(x_1, \cdots, x_n)$ não é necessariamente simétrica. Por exemplo, $\mathbb{Q}(x_1, \cdots, x_n), \sqrt{x_1}$ contém uma raiz quadrada de x_1, mas não de x_2, uma vez que não existe automorfismo entre x_1 e x_2. Entretanto, podemos restabelecer a simetria pela adjunção $\sqrt{x_2}, \cdots, \sqrt{x_n}$. A generalização dessa ideia nos sugere um modo de "simetrizar" qualquer extensão radical E de $\mathbb{Q}(x_1, \cdots, x_n)$.

Teorema 5.1.3. Para toda extensão radical E de $\mathbb{Q}(x_1, \cdots, x_n)$ existe uma extensão radical $\bar{E} \supseteq E$ com automorfismos σ estendendo todas as permutações de $x_1, \cdots, x_n$

Demonstração. Para todo elemento da adjunção, representado pela expressão radical $e(x_1, \cdots, x_n)$, e cada permutação σ de $(x_1, \cdots, x_n)$, façamos a adjunção do elemento $e(\sigma x_1, \cdots, \sigma x_n.)$ Dado que existe uma quantidade finita de permutações σ, o corpo resultante $\bar{E} \supseteq E$ também será uma extensão radical de $\mathbb{Q}(x_1, \cdots, x_n)$.

Dessa forma, obtém-se uma bijeção — também denominada σ — de $\bar{E}$ associando cada $f(x_1, \cdots, x_n) \in \bar{E}$ — que é uma função racional de $x_1, \cdots, x_n$ e radicais adjuntos — a $f(\sigma x_1, \cdots, \sigma x_n)$. Essa bijeção será um automorfismo de $\bar{E}$, estendendo a permutação σ.

□

A motivação para obter um automorfismo σ estendendo toda permutação de $x_1, \cdots, x_n$ é que $a_o, \cdots, a_{n-1}$ são fixados por tais permutações, assim como os elementos do corpo $\mathbb{Q}(a_o, \cdots, a_{n-1})$. Se $E \supseteq F$ são corpos quaisquer, os automorfismos σ de E fixando todos os elementos de F dão origem ao que se chama de *grupo de Galois de E sobre F*, denotado por $Gal(E/F)$. Com base nesse conceito, obtemos o seguinte resultado:

Corolário 5.1.1. Se E é uma extensão radical de $\mathbb{Q}(a_o, \cdots, a_{n-1})$ contendo $x_1, \cdots, x_n$, então existe uma extensão radical $\bar{E} \supseteq E$ de modo que $Gal(\bar{E}/\mathbb{Q}(a_o, \cdots, a_{n-1}))$ inclua automorfismos σ estendendo todas as permutações de $x_1, \cdots, x_n$.

Demonstração. Segue diretamente do teorema 5.1.3 e do fato de que uma extensão radical de que $\mathbb{Q}(a_o, \cdots, a_{n-1})$ contendo $x_1, \cdots, x_n$ é também uma extensão radical de $\mathbb{Q}(x_1, \cdots, x_n)$. □

5.2 A Estrutura das Extensões Radicais

Até o momento, sabemos que a solubilidade por radicais de uma equação geral de grau n implica na existência de uma extensão radical $\mathbb{Q}(x_1,\cdots,x_n)$ contendo $x_1,\cdots,x_n$ e, por conseguinte, a existência de uma extensão radical $\bar{E}$ com a simetria descrita no corolário 5.1.1.

Isso nos indica uma possibilidade para provar a não existência de tal solução a partir do estudo de $Gal(\bar{E}/\mathbb{Q}(a_o,\cdots,a_{n-1}))$, por meio da verificação da ausência de tal simetria quando $n \geq 5$.

Assim, nosso objetivo será mostrar que o grupo Galois $Gal(F(\alpha_1,\cdots,\alpha_k)/F))$ de qualquer extensão radical possui uma estrutura especial, a qual denominaremos "solubilidade", herdada da estrutura de $F(\alpha_1,\cdots,\alpha_k)$. A partir daí, verificaremos que essa estrutura é, de fato, incompatível com a simetria descrita no corolário 5.1.1.

A fim de simplificar tal verificação, iremos considerar, sem perda de generalidade, algumas hipóteses sobre a adjunção de radicais α_i. A primeira hipótese é considerar que cada adjunção radical α_i é uma p-ésima raiz de algum primo. Por exemplo, ao invés de fazer a adjunção $\sqrt[6]{\alpha}$, primeiro faremos $\sqrt{\alpha}=\beta$ e então $\sqrt[3]{\beta}$. Segundo, se α_i é uma p-ésima raiz então podemos considerar que $F(\alpha_1,\cdots,\alpha_i)$ não contém p-ésimas raízes da unidade que não estejam em $F(\alpha_1,\cdots,\alpha_{i-1})$, exceto nos casos em que α_i seja a própria p-ésima raiz da unidade. Se este não for o caso, basta fazer a adjunção da p-ésima raiz da unidade $\zeta \neq 1$ a $F(\alpha_1,\cdots,\alpha_{i-1})$ antes de fazer a adjunção de α_i — caso em que $F(\alpha_1,\cdots,\alpha_{i-1},\zeta)$ conterá todas as p-ésimas raízes da unidade $(1\zeta,\zeta^2,\cdots,\zeta^{p-1})$.

Com base nessas hipóteses, o corpo final $F(\alpha_1,\cdots,\alpha_k)$ se manterá inalterado, e assim permanecerá caso as raízes ζ adjuntadas forem incluídas na lista $\alpha_1,\cdots,\alpha_k$.

Assim, qualquer extensão radical $F(\alpha_1,\cdots,\alpha_k)$ será a união de uma torre ascendente de corpos

$$F = F_o \subseteq F_1 \subseteq \cdots \subseteq F_k = F(\alpha_1,\cdots,\alpha_k)\ ,$$

em que cada $F_i = F_{i-1}(\alpha_i)$, α_i é a p_i-ésima raiz de um elemento em F_{i-1}, p_i primo, e F_i não contém nenhuma p_i-ésima de um elemento em F_{i-1}, exceto se α_i for a própria p_i-ésima raiz da unidade.

Fazendo-se a correspondência com essa torre de corpos, teremos a seguinte torre de grupos:

$$Gal(F_k/F_o) = G \supseteq G_1 \supseteq \cdots \supseteq G_k = Gal(F_k/F_k) = \{1\}\ ,$$

em que $G_i = Gal(F_k/F_i) = Gal(F_k/F_{i-1}(\alpha_i))$ e 1 denotam o automorfismo identidade.

Da definição de $Gal(E/B)$, para qualquer corpo $E \supseteq B$, o grupo de automorfismos de E fixa cada elemento de B. Com o aumento de B para E, $Gal(E/B)$ deve diminuir até $\{1\}$. É

importante destacar que o passo G_{i-1} para seu subgrupo G_i — que reflete a adjunção da p_i-ésima raiz α_i para F — é "pequeno" o bastante para ser descrito em termos de Teoria de Grupos: G_i é um subgrupo normal de G_{i-1} e G_{i-1}/G_i é abeliano, conforme mostraremos a seguir.

Para simplificar a notação, utilizaremos:

$$E = F_k,\ B = F_{i-1},\ \alpha = \alpha_i,\ p = p_i\ ,$$

logo, o enunciado do teorema será:

Teorema 5.2.1. Se $E \supseteq B(\alpha) \supseteq B$ são corpos com $\alpha^p \in B$ para algum primo p, e se $B(\alpha)$ contém p-ésima raiz da unidade que não esteja em B, a menos que o próprio α seja a p-ésima raiz da unidade, então $Gal(E/B(\alpha))$ é um subgrupo normal de $Gal(E/B)$ e $Gal(E/B)/Gal(E/B(\alpha))$ é abeliano.

Demonstração. Pelo Teorema do Homomorfismo para Grupos, é suficiente encontrar um homomorfismo de $Gal(E/B)$, com núcleo $Gal(E/B(\alpha))$ em um grupo abeliano — ou seja, em um subgrupo de um grupo abeliano, que obviamente também é abeliano —. O mapa com núcleo $Gal(E/B(\alpha))$ é uma *restrição* para $B(\alpha), |_{B(\alpha)}$, dado que, pela definição,

$$\sigma \in Gal(E/B(\alpha)) \iff \sigma\,|_{B(\alpha)} \text{ é o mapa identidade.}$$

A propriedade do homomorfismo

$$\sigma'\,\sigma\,|_{B(\alpha)} = \sigma'\,|_{B(\alpha)}\,\sigma\,|_{B(\alpha)}\ , \text{ para todo } \sigma', \sigma \in Gal(E/B),$$

está automaticamente munido $\sigma\,|_{B(\alpha)}\,(b) \in B(\alpha)$ para todo $b \in B(\alpha)$, ou seja, desde que $B(\alpha)$ seja fechado em cada $\sigma \in Gal(E/B)$.

Desde que σ fixa B, $\sigma\,|_{B(\alpha)}$ fica completamente determinado pelo valor $\sigma(\alpha)$. Se α é uma p-ésima raiz da unidade ζ, então

$$(\sigma(\alpha))^p = \sigma(\alpha)^p = \sigma(\zeta^p) = \sigma(1) = 1,$$

portanto, $\sigma(\alpha) = \zeta^i = \alpha^i \in B(\alpha)$, desde que cada p-ésima raiz da unidade seja algum ζ^i. Se α não for uma raiz da unidade, então

$$(\sigma(\alpha))^p = \sigma(\alpha^p) = \alpha^p,\ \text{ desde que } \alpha^p \in B,$$

portanto, $\sigma(\alpha) = \zeta^j\alpha$ para alguma p-ésima raiz da unidade ζ, que por hipótese está em B. Então, $\sigma(\alpha) \in B(\alpha)$. Portanto, $B(\alpha)$ é fechado.

Isso implica também que $|_{B(\alpha)}$ leva $Gal(E/B)$ em $Gal(B(\alpha)/B)$, restando apenas verificar que $Gal(B(\alpha)/B)$ é abeliano. Se α é uma raiz da unidade, então, vimos que cada $\sigma\,|_{B(\alpha)} \in Gal(B(\alpha)/B)$ é da forma σ_i, com $\sigma_i(\alpha) = \alpha^i$, portanto,

$$\sigma_i\,\sigma_j(\alpha) = \sigma_i(\alpha^j) = \alpha^{ij} = \sigma_j\sigma_i(\alpha).$$

Do mesmo modo, se α não é uma raiz da unidade então cada $\sigma\,|_{B(\alpha)} \in Gal(B(\alpha)/B)$ será da forma σ_i, com $\sigma_i(\alpha) = \zeta^i\alpha$, portanto,

$$\sigma_i\,\sigma_j(\alpha) = \sigma_i(\zeta^j\alpha) = \zeta^{i+j}\alpha = \sigma_j\sigma_i(\alpha),$$

desde que $\zeta \in B$ e, assim, ζ está fixado. Em qualquer dos casos, está demonstrado que $Gal(B(\alpha)/B)$ é abeliano.

□

A implicação do fato de que $Gal(F(\alpha_1,\cdots,\alpha_k)/F)$ possua subgrupos

$$Gal(F(\alpha_1,\cdots,\alpha_k)/F) = G_o \supseteq G_1 \supseteq \cdots \supseteq G_k = \{1\},$$

com cada G_i normal em G_{i-1}/G_i abeliano é chamada "solubilidade" de $Gal(F(\alpha_1,\cdots,\alpha_k)/F)$.

5.3 A Inexistência de Soluções por Radicais quando $n \geq 5$

Conforme mencionado, afirmar que não existe solução por radical quando $n \geq 5$ equivale a demonstrar que uma extensão radical de $\mathbb{Q}(a_o,\cdots,a_{n-1})$ não contém $x_1,\cdots,x_n$, ou equivalentemente, $\mathbb{Q}(x_1,\cdots,x_n)$. Desse modo, a questão se reduz a provar que a simetria da hipotética extensão $\bar{E}$ contendo $x_1,\cdots,x_n$ — dada pelo corolário 5.1.1 — é incompatível com a solubilidade de $Gal(\bar{E}/\mathbb{Q}(a_o,\cdots,a_{n-1}))$ — dada pelo teorema 5.2.1.

Segundo Stillwell (1994, p. 26), com essa abordagem é possível identificar quais seriam as implicações caso existisse um hipotético automorfismo de $\bar{E}$ em $x_1,\cdots,x_n$, e sua relação com o grupo simétrico S_n de todas as permutações de $x_1,\cdots,x_n$.

Teorema 5.3.1. Uma extensão radical de $\mathbb{Q}(a_o,\cdots,a_{n-1})$ não contém $\mathbb{Q}(x_1,\cdots,x_n)$ quando $n \geq 5$.

Demonstração. Suponhamos, por contradição, que E seja uma extensão radical de $\mathbb{Q}(a_o,\cdots,a_{n-1})$ que contenha $\mathbb{Q}(x_1,\cdots,x_n)$. Então E será também uma extensão radical de $\mathbb{Q}(x_1,\cdots,x_n)$.

Segundo o corolário 5.1.1, existirá uma extensão $\bar{E} \supseteq E$ de modo que:

$$G_o = Gal(\bar{E}/\mathbb{Q}(a_o,\cdots,a_{n-1}))\,,$$

inclua automorfismos σ estendendo todas as permutações de $x_1, \cdots, x_n$.

Pelo teorema 5.2.1, G_o possuirá uma decomposição do tipo:

$$G_o \supseteq G_1 \supseteq \cdots \supseteq G_k = \{1\} ,$$

em que cada G_{i-1} é um subgrupo normal de G_i e G_{i-1}/G_i é abeliano, o que implica na inexistência de automorfismos σ.

De fato, dado que G_{i-1}/G_i é abeliano, G_i será o núcleo de um homomorfismo de G_{i-1} em um grupo abeliano. Logo,

$$\sigma, \tau \in G_{i-1} \Rightarrow \sigma^{-1}\ \tau^{-1}\ \sigma\ \tau\ \in G_i$$

Com base nisso, provaremos por indução sobre i que, se $n \geq 5$, cada G_i contém automorfismos α estendendo todas as ternas do tipo (x_a, x_b, x_c). Isso é verdade para G_o por hipótese. Por outro lado, quando $n \geq 5$ a propriedade se mantém válida de G_{i-1} a G_i, pois:

$$(x_a, x_b, x_c) = (x_d, x_a, x_c)^{-1}\ (x_c, x_e, x_b)^{-1}\ (x_d, x_a, x_c)\ (x_c, x_e, x_b) ,$$

com a, b, c, d e e diferentes entre si. Portanto, se houver pelo menos cinco indeterminadas x_j, haverá um σ em cada G_i que estenderá ternas arbitrárias do tipo (x_a, x_b, x_c), o que significa, em particular, que $G_k \neq \{1\}$.

Essa contradição mostra que $\mathbb{Q}(x_1, \cdots, x_n)$ não está contida em qualquer extensão radical de $\mathbb{Q}(a_o, \cdots, a_{n-1})$ quando $n \geq 5$.

□

CAPÍTULO

6

CONCLUSÃO

Nesse trabalho, buscou-se o equilíbrio entre uma apresentação intuitiva de conceitos matemáticos gerais e o rigor matemático necessário para o desenvolvimento de temas mais avançados.

A partir de uma abordagem histórica, foi apresentado um panorama da Matemática desde os primórdios da humanidade até o Século XIX, culminando com a apresentação de conceitos inerentes à Teoria de Galois.

Nessa jornada, foi possível vivenciar épocas e culturas diferentes, conhecer um pouco mais sobre o desenvolvimento do pensamento matemático em diferentes partes do mundo e aprender novas maneiras de se pensar a Matemática.

Do ponto de vista Matemático, os assuntos abordados foram apresentados em diferentes níveis de complexidade, iniciando-se por equações de primeiro e segundo grau, avançando para terceiro e quarto grau, para finalmente abordar os casos cujo grau é maior ou igual a cinco.

A partir daí, foram apresentadas as ferramentas matemáticas necessárias para a compreensão da demonstração referente à insolubilidade de equações polinomiais com grau maior ou igual a cinco.

Desse modo, esperamos contribuir para que o assunto sejam mais bem entendido, assim como incentivar aqueles que se interessam pela área a se aprofundarem mais nessa fascinante e belíssima teoria.

REFERÊNCIAS

ANTHONY, D. W. **The horse, the wheel, and language: how Bronze-Age riders from the Eurasian steppes shaped the modern world**. [S.l.]: Princeton University Press, 2010. Citado na página 25.

BANGURA, A. K. **African mathematics: From bones to computers**. [S.l.]: University Press of America, 2011. Citado na página 25.

BOYER, C. B.; MERZBACH, U. C. **História da matemática**. [S.l.]: Editora Blucher, 2019. Citado nas páginas 26, 28, 35, 36, 38, 39, 42 e 47.

BRASIL. **Parâmetros curriculares nacionais: matemática**. Brasília: MEC, SEF, 1997. Citado na página 20.

COHEN, I. B. **The triumph of numbers: How counting shaped modern life**. [S.l.]: WW Norton & Company, 2005. Citado na página 49.

COURANT, R.; ROBBINS, H. O que é matemática. **Uma abordagem elementar de métodos e conceitos. Rio de Janeiro: Ciência Moderna**, 2000. Citado na página 24.

CREASE, R. P. **As grandes equações: A história das fórmulas matemáticas mais importantes e os cientistas que as criaram**. [S.l.]: Editora Schwarcz-Companhia das Letras, 2011. Citado na página 49.

DARLING, D. **The Universal Book of Mathematics from Abracadabra to Zeno's Paradoxes**. [S.l.]: John Wiley & Sons, Inc., 2004. Citado nas páginas 24 e 30.

EVES, H. Introdução à história da matemática, tradução: Hygino h. **Domingues, Campinas-SP: Editora da UNICAMP**, 2004. Citado nas páginas 26, 31, 40, 41 e 47.

GARBI, G. G. **O romance das equações algébricas**. [S.l.]: Editora Livraria da Física, 2009. Citado nas páginas 25, 33, 44, 57 e 61.

____. **A Rainha das Ciências**. São Paulo: Ed. Livraria da Física, 2011. Citado nas páginas 27, 29, 30, 31, 38 e 43.

GRANTHAM, G. Compte rendu d'ouvrage-histoire des agricultures du monde. du néolithique à la crise contemporaine. **Cahiers d'Economie et de Sociologie Rurales (CESR)**, v. 48, n. 905-2016-70129, p. 129–131, 1998. Citado na página 25.

GRIFFITHS, H. B.; HILTON, P. **Matematica classica: uma interpretação contemporanea**. [S.l.]: E. Blucher/Ed. da Universidade de Sao Paulo, 1975. Citado na página 81.

HIGHFIELD, R. Zeros to heroes: What's the point of electricity? **New Scientist**, Elsevier, v. 207, n. 2777, p. 34, 2010. Citado na página 19.

JANSON, H. W.; JANSON, A. F. **History of art: the Western tradition**. [S.l.]: Prentice Hall Professional, 2004. Citado na página 34.

LIMA, E. L.; CARVALHO, P. C. P.; WAGNER, E.; MORGADO, A. C. **A matemática do ensino médio**. [S.l.]: SBM Rio de Janeiro, 1997. v. 1. Citado na página 50.

MARTIN, P. A. Grupos, corpos e teoria de galois. 2010. Citado nas páginas 64 e 68.

MILIES, F. C. P. Anéis e módulos. 1972. Citado na página 81.

ROQUE, T. **História da matemática**. Rio de Janeiro: Ed. Zahar, 2012. Citado nas páginas 26, 27, 28, 29 e 47.

RUDGLEY, R. **The lost civilizations of the stone age**. [S.l.]: Simon and Schuster, 2000. Citado na página 25.

SANT'ANNA, A. S. **O que é um axioma**. [S.l.]: Manole, 2003. Citado na página 35.

STEWART, I. **Galois theory**. [S.l.]: CRC press, 2022. Citado na página 50.

STILLWELL, J. Galois theory for beginners. **The American Mathematical Monthly**, Taylor & Francis, v. 101, n. 1, p. 22–27, 1994. Citado nas páginas 85, 87 e 91.

STRUIK, D. J. **A concise history of mathematics**. [S.l.]: Courier Corporation, 2012. Citado na página 23.

VYGOTSKY, L. S. A formação social da mente. 5ª tiragem. **São Paulo: Martins**, 2002. Citado na página 20.


ICMC
USP
SÃO CARLOS