



**PROGRAMA DE
PÓS-GRADUAÇÃO EM
MATEMÁTICA**

**Alguns Aspectos Históricos do Teorema de Abel-Ruffini e sua
Demonstração via Permutações e Laços**

CLAUDINEI PEDRILLO JUNIOR

INSTITUTO DE GEOCIÊNCIAS E CIÊNCIAS EXATAS

RIO CLARO
2024

UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO”
Instituto de Geociências e Ciências Exatas
Câmpus de Rio Claro

Alguns Aspectos Históricos do Teorema de Abel-Ruffini e sua Demonstração via Permutações e Laços

Claudinei Pedrillo Junior

Dissertação de Mestrado apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, mestrado profissional, do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista “Júlio de Mesquita Filho”, Câmpus de Rio Claro.

Orientadora
Profa. Dra. Carina Alves

Rio Claro - SP
2024

| | |
|-------|---|
| P371a | <p>Pedrillo Junior, Claudinei</p> <p>Alguns aspectos históricos do teorema de Abel-Ruffini e sua demonstração via permutações e laços / Claudinei Pedrillo Junior. -- Rio Claro, 2024</p> <p>67 p.</p> <p>Dissertação (mestrado profissional) - Universidade Estadual Paulista (UNESP), Instituto de Geociências e Ciências Exatas, Rio Claro</p> <p>Orientadora: Carina Alves</p> <p>1. Álgebra. 2. Teorema de Abel-Ruffini. 3. Equação Algébrica. 4. Raízes. I. Título.</p> |
|-------|---|

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Universidade Estadual Paulista (UNESP), Instituto de Geociências e Ciências Exatas, Rio Claro. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

Impacto potencial desta pesquisa

Esta pesquisa tem como objetivo principal fornecer um material didático para estudantes da área da matemática e áreas afins sobre a história e as soluções de equações algébricas. Além disso, mostrar que é possível, através de conhecimento dos números complexos e outras ferramentas elementares, fornecer uma ideia da demonstração do Teorema de Abel-Ruffini, que estabelece que a solução de uma equação algébrica de grau maior ou igual a cinco não pode ser escrita usando radicais. Esta proposta é dedicada aos estudantes e professores que não estão familiarizados com a Teoria de Galois, que é a teoria usada para provar este teorema. Ao apresentarmos um texto acessível e didático a estudantes e pesquisadores que não possuem uma formação avançada em matemática, difundimos o conhecimento de resultados importantes da matemática.

Potential impact of this research

The main objective of this research is to provide educational material for students in mathematics and related fields on the history and solutions of algebraic equations. Moreover, it aims to show that, through the knowledge of complex numbers and other elementary tools, one can convey an understanding of the proof of the Abel-Ruffini theorem. This theorem states that the solution of an algebraic equation of degree five or higher cannot be expressed using radicals. This proposal is dedicated to students and teachers who are not familiar with Galois Theory, which is the theory used to prove this theorem. By presenting an accessible and educational text to students and researchers without advanced mathematical training, we spread knowledge of important mathematical results.

UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO”
Instituto de Geociências e Ciências Exatas
Câmpus de Rio Claro

Claudinei Pedrillo Junior

ALGUNS ASPECTOS HISTÓRICOS DO TEOREMA DE ABEL-RUFFINI E SUA
DEMONSTRAÇÃO VIA PERMUTAÇÕES E LAÇOS

Dissertação de Mestrado apresentada ao Instituto de Geociências e Ciências Exatas do Câmpus de Rio Claro, da Universidade Estadual Paulista “Júlio de Mesquita Filho”, como parte dos requisitos para obtenção do título de Mestre em Matemática.

Comissão Examinadora

Profa. Dra. Carina Alves
Orientadora

Profa. Dra. Marta Cilene Gadotti
Departamento de Matemática - IGCE - UNESP/Rio Claro

Profa. Dra. Cintya Wink de Oliveira Benedito
FE- UNESP/São João da Boa Vista

Conceito: Aprovado

Rio Claro/SP, 30 de abril de 2024

Aos meus pais, por me trazerem ao mundo.

Agradecimentos

Em primeiro lugar, agradeço aquele que está acima de tudo, Deus.

À minha esposa Ana Amabile, luz da minha vida, pelo apoio, amor, cumplicidade, paciência e dedicação.

À minha filha Luiza, que é a alegria e a razão do meu viver.

Gostaria de agradecer também ao Departamento de Matemática UNESP, Campus Rio Claro, a todos os meus professores que tanto contribuíram para minha formação, aprendizagens e evolução e aos meus colegas de curso pelas trocas, amizade e experiências.

Agradeço a minha orientadora Carina, por ter me aceitado como seu orientando, pelos seus ensinamentos, paciência e pela maneira que me conduziu e me incentivou para realização dessa dissertação.

Também preciso salientar e agradecer aos membros da banca examinadora, por aceitarem o convite e pelos apontamentos, sempre muito pertinentes e precisos para que eu pudesse concluir essa etapa final desse trabalho.

Agradeço a vida e obra de Abel, que sempre com poucos recursos, conseguiu consolidar conhecimentos que até hoje são objetos de pesquisa e trabalho de muitos matemáticos.

“Ele escolheu um panfleto como maneira mais rápida de imprimi-lo e, para economizar nos custos de impressão, reduziu a prova para caber em meia folha de fólho (seis páginas).”

Ayoub sobre Abel.

Resumo

Este trabalho apresenta alguns aspectos históricos do Teorema de Abel-Ruffini e, em particular, métodos matemáticos para resolução de equações de grau 2, 3 e 4. Mostramos as dificuldades de encontrar um método por meio de radicais para resolver equações de grau ≥ 5 . Além disso, destacamos alguns matemáticos que contribuíram para chegar ao referido teorema e apresentamos uma demonstração do Teorema de Abel-Ruffini via permutações e laços.

Palavras-chave: Álgebra. Teorema de Abel-Ruffini. Equação Algébrica. Raízes.

Abstract

This work presents some historical aspects of the Abel-Ruffini Theorem and, in particular, mathematical methods for solving equations of degree 2, 3, and 4. We demonstrate the difficulties of finding a method through radicals to solve equations of degree ≥ 5 . Furthermore, we highlight some mathematicians who contributed the development of the aforementioned theorem and present a proof of the Abel-Ruffini Theorem via permutations and loops.

Keywords: Algebra. Abel-Ruffini Theorem. Algebraic Equation. Roots.

Lista de Figuras

| | | |
|-----|--|----|
| 2.1 | Niels Henrik Abel. | 17 |
| 2.2 | Paolo Ruffini. | 21 |
| 2.3 | Ideia de completar o quadrado. | 24 |
| 2.4 | Completando o quadrado. | 24 |
| 2.5 | Parábola $X^2 = 2Y$ | 26 |
| 2.6 | Círculo $X^2 + Y^2 = 4$ | 26 |
| 2.7 | Interseção ente a parábola e o círculo. | 26 |
| 3.1 | Divisão do cubo e seis sólidos. | 31 |
| 4.1 | As duas curvas à esquerda denotam a transposição (12) e curva à direita, o ciclo (123), ambos permutando soluções (s_1, s_2, s_3) de uma equação algébrica de grau $n \geq 3$ | 39 |
| 4.2 | Quando z percorre um laço γ que não circunda a origem, suas raízes ζ_i também percorrem laços (à direita). No entanto, para o laço γ que circunda uma vez, as raízes então seguem os caminhos vermelhos, não fechados. | 41 |
| 4.3 | Combinando coeficientes (c_0, \dots, c_{n-1}) com $+, -, \times, \div$ define-se uma F -função. Combinando F -funções e suas raízes \sqrt{F} com $+, -, \times, \div$ define-se uma G -função, e assim sucessivamente. | 42 |
| 4.4 | A transposição (12) aplicada nas soluções (s_1, s_2) induz um laço nos coeficientes (c_0, c_1) | 44 |
| 4.5 | Elaborado pelo autor | 44 |
| 4.6 | Um laço percorrido por (c_0, c_1) induz um laço sobre as F -funções $F_1(c_0, c_1)$ e $F_2(c_0, c_1)$ | 45 |
| 4.7 | Efeito do comutador $[(12), (23)]$ num coeficiente c , numa F -função e numa \sqrt{F} -função. Ao fim do processo, F e \sqrt{F} percorreram laços. Note que o laço percorrido por \sqrt{F} é composto por 4 caminhos abertos. | 46 |

Lista de Tabelas

| | | |
|-----|--|----|
| 4.1 | Resumo dos métodos utilizados para demonstrar os dois primeiros resultados de impossibilidade. | 47 |
| 4.2 | Extensão da Tabela 4.1 para H -funções e grau $n \geq 4$ | 48 |

Sumário

| | | |
|----------|--|-----------|
| 1 | Introdução | 15 |
| 2 | Aspectos históricos | 17 |
| 2.1 | Abel “O mais humano dos Matemáticos” | 17 |
| 2.2 | As dificuldades enfrentadas por Abel | 19 |
| 2.3 | Ruffini - o precursor | 21 |
| 2.4 | Ideias geométricas da antiguidade para a solução de equações quadráticas e cúbicas | 23 |
| 3 | Resolução por radicais | 27 |
| 3.1 | Equação de grau 2 | 28 |
| 3.2 | Equação de grau 3 | 29 |
| 3.3 | Equação de grau 4 | 33 |
| 3.4 | Equações de grau $n \geq 5$ | 36 |
| 4 | Uma demonstração do Teorema de Abel-Ruffini usando permutações e laços | 38 |
| 4.1 | Permutações, Laços, Raízes e F , G , H -funções | 38 |
| 4.2 | A equação quadrática, cúbica e quártica | 42 |
| 4.2.1 | A equação quadrática | 43 |
| 4.2.2 | A equação cúbica | 45 |
| 4.2.3 | A equação quártica | 47 |
| 4.3 | A equação quártica | 48 |
| 5 | Considerações Finais | 51 |
| | Referências | 52 |
| A | Polinômios | 54 |
| A.1 | Definições e propriedades básicas | 54 |
| A.2 | Divisão euclidiana | 60 |
| A.3 | Raízes de polinômios | 62 |
| A.4 | O Teorema Fundamental da Álgebra | 65 |

| | | |
|-----|--|----|
| A.5 | Relações entre coeficientes e raízes | 68 |
|-----|--|----|

1 Introdução

As equações algébricas desempenham um papel fundamental em várias áreas da matemática e da ciência. Elas são utilizadas para modelar e resolver problemas em física, engenharia, economia e muitas outras disciplinas. Equações polinomiais, um tipo especial de equações algébricas, são particularmente importantes. Elas aparecem em diversos contextos, desde a descrição de curvas e superfícies até a análise de sistemas dinâmicos e a otimização de processos. O desenvolvimento de métodos para resolver equações algébricas, como a descoberta das fórmulas de resolução para equações cúbicas e quárticas, foi um marco histórico na matemática, abrindo caminho para avanços significativos.

O Teorema de Abel-Ruffini é um resultado central na teoria das equações algébricas. Provado por Niels Henrik Abel e baseado nos trabalhos de Paolo Ruffini, o teorema afirma que não existe uma fórmula geral para resolver equações polinomiais de grau cinco ou superior usando apenas operações aritméticas e radicais (extração de raízes). Embora o teorema limite as soluções por métodos tradicionais, ele também orienta os matemáticos a usar abordagens numéricas e computacionais para resolver equações de graus elevados, que têm aplicações práticas em várias áreas da ciência e engenharia.

Este trabalho tem como objetivo apresentar uma demonstração autocontida e acessível do Teorema de Abel-Ruffini, via permutações e laços. Utilizaremos as permutações do tipo transposições e ciclos para permutar as soluções das equações. Os laços são ferramentas usadas para verificar a insolubilidade de equações algébricas. O texto está organizado como segue.

No Capítulo 2, nomeado “Aspectos históricos”, conheceremos um pouco da trajetória e da vida de dois matemáticos brilhantes: Paolo Ruffini e Niels Henrik Abel, os quais foram incompreendidos e, mesmo passando por muitos reveses, contribuíram para a evolução e o sucesso da matemática que aplicamos em nossos dias. A princípio, falaremos de Paolo Ruffini, que nasceu em 1765 em Valentano – Estados Papais, atual Itália – e morreu em 1822, em Modena – Ducado de Modena, atual Itália. Além disso, ele era chamado de precursor porque usou a Teoria dos Grupos em seu trabalho e inventou o assunto. Em 1799, publicou um livro sobre a Teoria das Equações, intitulado Teoria das Equações, no qual afirmava que as quárticas não são solúveis por radicais. Nesse livro, ele mostrou que a solução algébrica da equação geral de grau maior que quatro é impossível. Os grandes matemáticos Scipione Del Ferro, Tartaglia e Cardano resolveram as cúbicas, e Ferrari as quárticas, porém as quárticas ficaram sem solução por radicais por mais de 250 anos. Paolo Ruffini publicou trabalhos em muitas

áreas além da Matemática, entretanto, Abel levou os créditos sobre a impossibilidade de resolver as quárticas por radicais. Isso se deu devido a Abel ter provado, em 1824, a impossibilidade de resolver a equação geral do quinto grau em radicais, embasando seus estudos na obra de Ruffini. Por conseguinte, abordaremos a vida de Niels Henrik Abel, que nasceu em 1802, na pequena cidade de Finnøy, na Noruega, e era excepcionalmente talentoso, tendo em vista que ele se interessou, ainda com 17 anos, pelas equações algébricas e pensou haver encontrado uma forma geral de resolver as do quinto grau. Contudo, pouco tempo depois, ele percebeu uma falha em sua solução e, somente após conhecer a obra de Ruffini, em 1815, por meio da obra de um terceiro matemático, Augustin Louis Cauchy, é que pôde completar seu trabalho. A ideia de examinar permutações de raízes para estudar a (in)solubilidade de equações algébricas teve sua origem em 1771 com os trabalhos pioneiros de J. L. Lagrange. As ideias de Lagrange amadureceram e foram estendidas à equação quártica por Paolo Ruffini, no começo dos anos 1800. Apesar de, tecnicamente, Ruffini não ter provado o teorema que hoje carrega seu nome, seus resultados eram fortes o suficiente para levantar sérias dúvidas a respeito da possibilidade de se encontrar uma solução para a equação quártica geral. Finalmente, em 1824, N. H. Abel escreveu a primeira demonstração completa do teorema. A abordagem histórica apresentada foi retirada das referências [1], [2], [3] e [4].

No Capítulo 3, discorreremos sobre a importância das equações algébricas e conheceremos um pouco da história de figuras responsáveis pela descoberta das soluções algébricas das equações cúbicas e quárticas, como Niccolo Fontana (1499-1577), Rafael Bombelli (1526-1572), que conseguiu chegar aos novos números, em 1530, e que demorou mais de dois séculos para saber como extrair raízes de números complexos, através de Euler. Além disso, veremos algumas das contribuições do matemático Girolamo Cardano (1501-1576), que esteve envolvido na solução algébrica da equação cúbica, a qual foi o maior avanço matemático desde o tempo dos gregos. Assim, chegaremos até Niels Henrik Abel (1802-1829), autor do artigo publicado em 1829 sobre as equações gerais de graus maiores ou iguais a cinco, e descobridor do teorema, posteriormente intitulado Teorema de Abel-Ruffini, no qual afirma que não existe fórmula para as soluções da equação geral de grau maior ou igual a 5 usando apenas as operações elementares e radicais. A demonstração desse resultado depende do conhecimento de uma vertente da Matemática chamada Teoria de Galois. Em particular, as ideias de Galois, Abel e Ruffini se baseiam em um único e fundamental ponto: a simetria de uma equação algébrica sob a permutação de suas soluções. Para o desenvolvimento deste capítulo, utilizamos as referências [5], [6] e [7].

No Capítulo 4, baseando-se somente nessa simetria fundamental, esboçaremos, uma prova do Teorema de Abel-Ruffini, usando apenas conhecimentos elementares de números complexos, laços e permutações. Essa demonstração é recente, datada de 2022, [8]. Por isso, neste trabalho, apresentaremos argumentos novos. A demonstração do Teorema de Abel-Ruffini pode ser feita através da Teoria de Galois, todavia, seu entendimento pode se tornar bastante difícil.

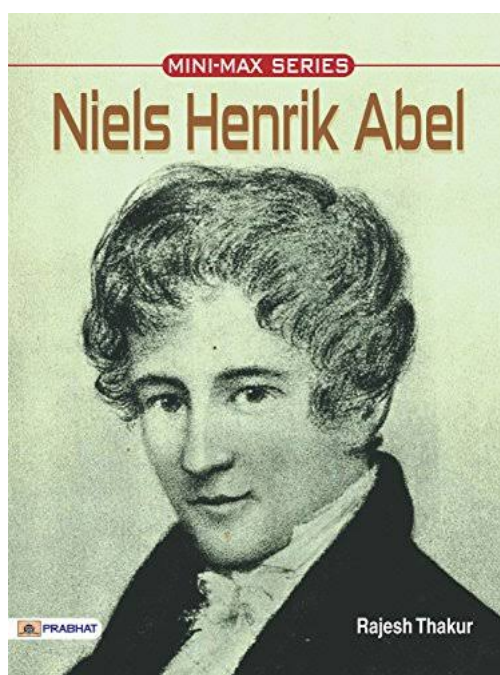
No apêndice deste trabalho apresentamos alguns resultados sobre polinômios, que contribuem para um melhor entendimento do Capítulo 3 e Capítulo 4.

2 Aspectos históricos

Neste capítulo é apresentado um apanhado histórico da vida do matemático Niels Henrik Abel, desde o seu nascimento até sua morte. Para o desenvolvimento deste capítulo foram utilizadas as referências [1], [2], [3] e [4].

2.1 Abel “O mais humano dos Matemáticos”

Figura 2.1: Niels Henrik Abel.



Fonte: Retirado de [9].

Niels Henrik Abel nasceu em 5 de agosto de 1802 na pequena cidade de Finnøy, na Noruega, filho e neto de pastores protestantes, teve quatro irmãos e uma irmã. Seu pai, Abel, foi um dos fundadores da universidade de Oslo, onde aos 13 anos Abel foi estudar. Abel era excepcionalmente talentoso e resolvia com facilidade problemas que seus colegas julgavam difíceis, e dos 17 aos 19 anos ele se interessou pelas equações algébricas e pensou haver

encontrado uma forma geral de resolver as do quinto grau, mas um pouco depois ele mesmo percebeu uma falha na sua solução.

Próximo ao Natal de 1823, aos 21 anos, ele provou que, exceto em casos particulares, que é impossível resolver uma equação de grau 5 utilizando-se apenas um número finito de operações algébricas como soma, multiplicação, subtração, divisão e extração de raízes. Sua contribuição matemática é tanta que vários objetos matemáticos levam seu nome, como por exemplo os chamados grupos abelianos, e um dos grandes prêmios matemáticos, chamado de prêmio Abel.

Depois dessa breve introdução sobre sua vida e obra vamos conhecer melhor o contexto histórico em que ele nasceu e viveu.

No final do século XVIII, a Noruega fazia parte da Dinamarca, os dinamarqueses tentaram ficar neutros na guerra contra Napoleão, mas nada adiantou. A Suécia dominou a Noruega e passou a controlar internamente o país através de um governo. E nessa situação difícil, Abel crescia em Gjerstad, no sudoeste da Noruega. O pai de Abel, Sören Georg Abel, tinha formação teológica e em filologia. Niels Abel, o segundo de sete filhos foi ensinado por seu pai no vicariato até os 13 anos de idade. No entanto, esses foram os 13 anos de crise econômica para a Noruega descritos acima e os pais de Abel não teriam conseguido alimentar muito bem sua família.

Ele foi estudar na chamada Escola da Catedral em Christiania (que hoje se chama Oslo) e provou ser um aluno bastante comum com algum talento para matemática e física. Até que um professor de matemática, Bernt Holmboë, ingressou na escola em 1817, mudando para sempre a vida desse grande gênio. Com o auxílio desse professor ele começou a estudar textos universitários e um ano após a chegada de Holmboe, Abel estava lendo obras de Euler, Newton, Lalande e D’Alembert. Nesse momento de descobrimento, em 1820 morre seu pai e se as coisas eram ruins agora pioraram consideravelmente, pois o pouco sustento da família acabara.

Não havia dinheiro para permitir que Abel completasse sua educação escolar, nem dinheiro para permitir que ele estudasse na universidade e, além disso, Abel tinha a responsabilidade de sustentar sua mãe e família. Holmboë conseguiu ajudar Abel a obter uma bolsa de estudos para permanecer na escola e ele conseguiu ingressar na Universidade de Christiania em 1821, dez anos após a fundação da universidade. Holmboë levantou dinheiro de seus colegas para permitir que Abel estudasse na universidade. No seu último ano na escola Abel começou a trabalhar na solução de equações quárticas por radicais.

Ele pensava ter resolvido a quártica em 1821 e apresentou um artigo ao matemático dinamarquês Ferdinand Degen, para publicação pela Royal Society of Copenhagen. Degen pediu a Abel que desse um exemplo numérico de seu método e, ao tentar dar um exemplo, Abel descobriu o erro em seu artigo. Degen havia dado a Abel alguns conselhos importantes que o levariam a trabalhar em uma área da matemática, as integrais elípticas. Na Universidade de Christiania Abel foi apoiado pelo professor de astronomia, Christopher Hansteen, que o incentivou e ofereceu ajuda financeira. Ele foi cuidado como se fosse um filho do casal Hansteen. Em 1823, Abel publicou artigos sobre equações funcionais e integrais em uma nova revista científica iniciada por Hansteen. No terceiro artigo de Abel, que tratava das soluções de alguns

problemas por meio de integrais definidas, ele deu a primeira solução de uma equação integral.

Apesar da ajuda financeira vinda de uma pequena bolsa para visitar o professor Ferdinand Degen e outros matemáticos em Copenhague, Abel não conseguiu realizar tudo que havia planejado: visitar os melhores matemáticos da Alemanha e França. Mesmo assim, sua estadia de dois meses em Copenhague serviram não só para conhecer matemáticos e acadêmicos, mas principalmente para conhecer o amor de sua vida, Christine Kemp. Tentou uma bolsa maior junto a Universidade de Christiania, mas como não falava francês ou alemão e em parte para economizar dinheiro, decidiu permanecer por dois anos em Christiania, onde recebeu fundos para aprender os idiomas, antes de viajar.

Abel voltou a trabalhar em equações quinticas e, em 1824, ele provou a impossibilidade de resolver a equação geral do quinto grau em radicais. Ele publicou o trabalho em francês e às suas próprias custas, pois queria uma obra impressionante para levar consigo quando estivesse em suas viagens. Segundo [10], ele escolheu um panfleto como a maneira mais rápida de imprimi-lo e, para economizar nos custos de impressão, reduziu a prova para caber em meia folha de fôlio (seis páginas).

2.2 As dificuldades enfrentadas por Abel

Nesta época, Abel parece ter conhecido algo da obra de Ruffini, pois havia estudado a obra de Cauchy em 1815 enquanto era estudante de graduação e neste artigo há uma referência à obra de Ruffini.

Abel enviou o material produzido a vários matemáticos e também para Gauss, pois pretendia visitá-lo durante suas viagens em agosto de 1825. Foi nesse momento que ele recebe uma bolsa de estudos do governo norueguês para poder viajar ao exterior, onde visitou vários matemáticos. Em Copenhague, Abel recebeu uma carta de apresentação de August Crelle, um matemático alemão que fundou uma importante revista matemática, de quem ele tornou-se amigo quando se encontraram em Berlim. Abel, incentivado por Crelle, escreve um artigo com uma versão mais clara de seu trabalho sobre as equações quinticas, intitulado “*Recherches sur les fonctions elliptiques.*” O artigo foi publicado em 1827 no primeiro volume do chamado diário de Crelle, junto com outros seis artigos de Abel.

A viagem desejada por Abel não aconteceu, ele pretendia junto com Crelle visitar Gauss em Göttingen, no entanto chegou a ele a notícia de que Gauss não mostrou interesse em seu trabalho sobre as quinticas. Não se sabe ao certo porque Gauss teve essa atitude, pois ele não tinha conhecimento do trabalho de Abel. Segundo [10], a primeira possibilidade é que Gauss provou o resultado ele mesmo e estava disposto a deixar Abel levar o crédito. A outra explicação é que ele não deu muita importância à solubilidade por radicais. A segunda dessas explicações pode ser a melhor, dado o fato que Gauss escreveu em sua tese de 1801 que a solução de uma equação algébrica não era melhor do que inventar um símbolo para a raiz da equação e depois dizer que a equação tinha raiz igual ao símbolo.

Abel teve que continuar a viagem com seus amigos noruegueses para o norte da Itália

antes de cruzar os Alpes para França, pois Crelle foi detido em Berlim. Em Paris, ele ficou desapontado, pois percebeu que havia pouco interesse pelo seu trabalho. Abel escreveu de volta para Holmboe dizendo que os franceses são muito mais reservados e estranhos do que os alemães, que é extremamente difícil ganhar a intimidade deles. Todo iniciante tem muita dificuldade em ser notado em Paris. Abel disse ainda que tinha acabado de terminar um extenso tratado sobre uma certa classe de funções transcendentais para apresentá-lo ao Instituto, na próxima segunda-feira, mas ele o mostrou para Cauchy e Cauchy mal se dignou a olhar para o tratado.

Abel retorna de Berlim em 1826, depois de publicar alguns artigos para o *Crelle's Journal*, sem dinheiro e com a saúde precária. Em Berlim ele pediu dinheiro emprestado e continuou trabalhando nas funções elípticas. Abel transformou radicalmente a teoria das integrais elípticas na teoria das funções elípticas, usando suas funções inversas. Seu amigo, Crelle, até tentou fazer com que Abel ficasse em Berlim, para que pudesse encontrar um cargo acadêmico para ele e ofereceu a ele a editoria do Jornal de Crelle, mas Abel queria voltar para casa. Ele chegou a Christiania em maio de 1827 e recebeu uma pequena quantia em dinheiro da universidade, embora talvez tivesse que devolver depois. Com muitas dívidas ele foi ser tutor de crianças em idade escolar e sua noiva foi empregada como governanta de amigos da família de Abel em Froland. Abel foi nomeado professor substituto de Christopher Hansteen e passou a lecionar na universidade e também na academia militar.

Em 1828 lhe é mostrado um artigo de Jacobi sobre transformações de integrais elípticas, não demorou até que Abel demonstrasse que os resultados encontrados por Jacobi eram corolários de sua autoria e acrescentou uma nota nesse sentido. Ele estava trabalhando na verificação de quais equações eram solúveis por radicais, mas depois do ocorrido parou o que estava fazendo e foi “competir” com Jacobi na teoria das funções elípticas. O grande matemático Legendre viu as novas ideias de Abel e Jacobi nos jornais e disse que através de tais obras, os dois seriam colocados na classe dos principais analistas de nossos tempos. Abel não parava de desenvolver matemática da mais alta qualidade, enquanto sua saúde ficava cada vez mais abalada. Ele estava muito feliz, pois passaria as férias de verão de 1828 na companhia de sua esposa e amigos, mas logo a doença começou a tomar conta de seu corpo. É bom lembrar que fazia algum tempo que Abel começara a adoecer, mas ele não se preocupou, pois estava muito ocupado com o seu trabalho, o que fez agravar ainda mais seu caso.

Podemos dizer lendo a história desse gênio que a arrogância histórica e humana contribuíram para sua morte precoce, já que ele bateu em muitas portas e quase nunca elas foram abertas. A obra-prima que ele havia submetido à Academia de Paris parecia ter se perdido e então ele escreveu o resultado principal novamente [2]. O jornal tinha apenas duas páginas breves, mas de todas as suas muitas obras talvez a mais pungente. Chamou-o apenas de “Teorema A”. Não tinha introdução, não continha observações supérfluas, nem aplicações. Era um monumento resplandecente em suas linhas simples - o principal teorema de suas memórias de Paris, formulado em poucas palavras.

Abel viajou de trenó para visitar sua noiva novamente em Froland para o Natal de 1828.

Nessa viagem ele adoeceu e apesar de sua melhora que lhe deu a chance de aproveitar o Natal, ficou muito doente em seguida. Seu amigo de longa data Crelle fez de tudo para conseguir uma entrevista para Abel em Berlim e conseguiu mais já era tarde demais. Niels Henrik Abel morreu em 6 de abril de 1829, não tinha completado 27 anos de idade. Depois de duas semanas de sua morte na coluna obituário de Den Norske Rigstidende, Sivert Smith, proprietário da Froland Ironworks anunciou que o altamente estimado Niels Henrik Abel, amplamente famoso por sua excelência matemática, e Professor na Royal Frederik University, após 12 semanas de doença grave, morreu em sua casa. Abel já era brilhante muito antes de se tornar um estudante universitário, mas ninguém na Noruega tinha condições de acompanhar e entender o significado de suas realizações, extraordinário e incompreendido. Naquele abril de 1829 morre uma das mentes mais brilhantes da matemática.

As homenagens a Abel vieram na sua grande maioria após sua morte, bem como o reconhecimento devido a ele, o que torna tudo muito mais triste, sem falar na idade em que partiu, se com tão pouco tempo de vida Abel produziu material que os matemáticos estudam até hoje, imagine se tivesse vivido mais. Um livro de memórias de Paris escrito por Abel foi encontrado depois de uma longa busca por Cauchy em 1830, foi impresso em 1841, desapareceu novamente e só foi encontrado em 1952 em Florença. Também após sua morte um trabalho inédito sobre a solução algébrica de equações foi encontrado. Abel escreve a Crelle em 18 de outubro de 1828, o teorema: “Se cada três raízes de uma equação irreduzível de grau primo estão relacionadas entre si de tal forma que uma delas pode ser expressa racionalmente em termos das outras duas, então a equação é solúvel em radicais”.

2.3 Ruffini - o precursor

Figura 2.2: Paolo Ruffini.



Fonte: Retirado de [11].

Nesse momento, vamos contar um pouco da história de Paolo Ruffini, figura imprescindível para esse trabalho. Nasceu em 22 de setembro de 1765 em Valentano, Estados Papais (agora Itália) e morreu em 10 de maio de 1822 em Modena, Ducado de Modena (agora Itália). Paolo Ruffini foi um matemático italiano que provou que a equação quártica não podia ser resolvida antes de Abel.

O pai de Paolo Ruffini era médico em Valentano. Quando criança ele tinha o temperamento místico e parecia destinado ao sacerdócio. Na adolescência mudou-se com pais para Reggio, entrou na Universidade de Modena em 1783, lá estudou medicina, matemática, filosofia e literatura, aprendeu cálculo e geometria com os professores Paolo Cassiani e Luigi Fantini. Ruffini ainda estudante, assumiu o curso de fundamentos de análise no lugar de Cassiani que foi indicado para um outro cargo. O trabalho feito por Ruffini foi muito bem e em 15 de outubro de 1788 ele é nomeado professor de Fundamentos de Análise. O seu professor de geometria, Fantini, teve um problema de visão e Ruffini assume o curso de Elementos de Matemática em seu lugar. Ele também era médico e em 1791 recebe a licença para praticar medicina pelo tribunal médico colegiado de Modena. No contexto histórico essa era uma época de guerras após a Revolução Francesa e contra a sua vontade Ruffini foi nomeado representante do Conselho Junior da República Cisalpina, mas ele logo deixou essa posição e voltou para o seu trabalho científico. Para que isso acontecesse ele foi obrigado a fazer um juramento que não pode cumprir por motivos religiosos e como consequência disso ele perde o direito de lecionar.

Ruffini não teve muitos problemas para superar a perda de sua cátedra, era calmo e lidava bem com as adversidades, não lecionar significava mais tempo para praticar medicina e ajudar as pessoas, além de poder investir na prova da insolubilidade das quárticas por meio de radicais.

A resolução de uma equação polinomial por radicais significava encontrar uma fórmula para suas raízes em termos dos coeficientes, de modo que a fórmula envolvesse apenas as operações de adição, subtração, multiplicação, divisão e obtenção de raízes. As equações quadráticas eram conhecidas por serem solúveis por radicais desde a Babilônia. Os grandes matemáticos Scipione Del Ferro, Tartaglia e Cardano resolveram as cúbicas e Ferrari as quárticas, mas as quárticas ficaram sem solução por radicais por mais de 250 anos. Muitos matemáticos fizeram tentativas de resolver as equações de grau cinco por radicais, tais como: Tschirnhaus, Euler, Bézout, Vandermonde, Waring e Lagrange.

A impressão que se tem é que ninguém acreditava que a quártica pudesse ser resolvida por radicais. Em 1799 Ruffini publicou um livro sobre a teoria das equações com sua afirmação de que as quárticas não são solúveis por radicais com o título de Teoria das equações, ele mostra que a solução algébrica da equação geral de grau maior que quatro é impossível.

Ruffini usou a teoria dos grupos em seu trabalho, inventando ele mesmo o assunto. Lagrange utilizou permutações e grupos em seu trabalho, mas nunca escreveu sobre o assunto, enquanto que Ruffini foi o primeiro a introduzir a noção de ordem de um elemento, conjugação, decomposição cíclica de elementos de grupos de permutação e as noções de primitivo e imprimitivo. Ele provou alguns teoremas muito importantes nessa área: “A ordem de uma permutação é o mínimo múltiplo comum dos comprimentos na decomposição em ciclos disjuntos” é um deles,

o trabalho que ele fez é notável, mas a prova do teorema não teve resposta por parte dos matemáticos. Ele enviou o livro para muitos matemáticos de renome e o único que com certeza leu foi Pietro Paoli, influenciado por motivos patrióticos.

Ruffini publicou uma segunda prova em 1803, na tentativa de se fazer entender, com isso recebeu comentários de Malfati, mas ele não entendeu os argumentos de Ruffini. Ele continuou na busca de entendimento para seu trabalho pela comunidade matemática, bastava algum matemático ter escrito indicando que havia um erro ou algo faltando na sua prova e ele teria a chance de corrigi-la. O assunto sobre as quinticas não despertava o interesse de quase ninguém e então Ruffini pede ao Instituto de Paris para avaliar se a prova dada por ele era correta. Foram nomeados para a avaliação Lagrange, Legendre e Lacroix, que já não tinham demonstrado interesse pelo trabalho de Ruffini anteriormente, chegando ao ponto de Lagrange escrever no relatório que se um assunto não tem importância, não se dá atenção a ele.

O único que reconheceu a importância e correção foi Cauchy, dada sua reputação de não gostar de reconhecer o trabalho feito por outros matemáticos isso era surpreendente. De fato Cauchy havia escrito um grande trabalho sobre grupos de permutação entre 1813 e 1815 e nele generalizou alguns dos resultados de Ruffini. Esse grande matemático que lutou para ter uma resposta da comunidade matemática, deixa a Universidade de Modena para passar 7 anos ministrando aulas de matemática aplicada na escola militar de Modena e continuou a praticar medicina ajudando pobres e ricos.

Nesse período Napoleão perde a guerra e Ruffini volta a ocupar a reitoria da Universidade. Em 1817 houve uma epidemia de tifo e Ruffini continuou a tratar seus pacientes até que ele próprio adoeceu. Ele desistiu de sua cadeira de clínica médica em 1819, mas continuou seu trabalho científico.

Paolo Ruffini publicou trabalhos em muitas áreas além da matemática, para encerrar esse breve relato sobre a vida e obra desse grande cientista, uma pergunta importante devemos fazer: por que Abel levou os créditos sobre a impossibilidade de resolver as quinticas por radicais? Primeiro a comunidade matemática da época era considerada difícil de lidar e mais importante Abel “corrigiu” a prova mudando um pouco o foco dado por Ruffini. Ruffini faleceu em 10 de maio de 1822, no Ducado de Modena (agora Itália).

2.4 Ideias geométricas da antiguidade para a solução de equações quadráticas e cúbicas

Omar Khayyaam (1050 – 1123) fez a conexão entre álgebra e geometria. Ele é considerado um dos maiores matemáticos e poetas persas. Segundo Omar, álgebras são fatos geométricos que estão provados.

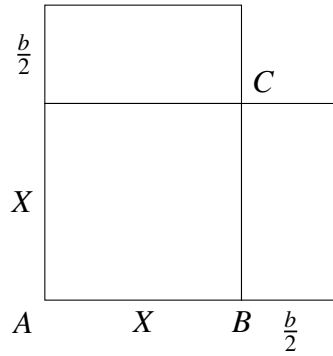
Matemáticos islâmicos na época de Omar Khayyam (1050–1123) possuíam técnicas geométricas para resolver equações quadráticas. Eles não usavam números negativos, então existiam diferentes tipos de métodos para resolver diferentes tipos de equações quadráticas. Para resolver

uma equação do tipo

$$X^2 + bX = c,$$

usamos a ideia geométrica de completar o quadrado.

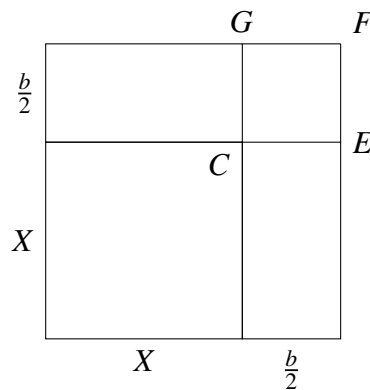
Figura 2.3: Ideia de completar o quadrado.



Fonte: Elaborado pelo autor (2023).

Observe a Figura 2.3. Comece com o quadrado de lado $ABCD$ de área X^2 , depois adicione a área bX a X^2 . Para manter o balanceamento, adicione essa área em proporções iguais a ambos os lados, isto é, adicione dois retângulos de lados $\frac{b}{2}$ e X . Agora, temos que a soma das áreas é $X^2 + bX$ que é igual a c . Complete o quadrado adicionando o quadrado $CEFG$ de área $\frac{b^2}{4}$, como mostrado na Figura 2.4.

Figura 2.4: Completando o quadrado.



Fonte: Elaborado pelo autor (2023).

Assim, temos que a área total do quadrado, depois de adicionar o quadrado $CEFG$ é

$$X^2 + bX = c + \left(\frac{b}{2}\right)^2.$$

Note a Figura 2.4, podemos reescrever tal área como

$$\begin{aligned} \left(X + \frac{b}{2}\right)^2 &= \frac{b^2}{4} + c \\ \left(X + \frac{b}{2}\right) &= \sqrt{\frac{b^2}{4} + c} \\ X &= +\sqrt{\frac{b^2}{4} + c} - \frac{b}{2} \end{aligned}$$

que é uma forma da fórmula quadrática.

Enquanto Omar Khayyaam forneceu tanto soluções algébricas quanto geométricas para equações quadráticas, ele achava que soluções algébricas para equações cúbicas gerais eram impossíveis e forneceu apenas soluções geométricas. Para as soluções geométricas ele empregou a ideia de intersectar cônicas para resolver equações cúbicas e deu uma classificação completa de equações até grau três com os métodos de resolução de cada uma. Como não eram usados números negativos, ele elencou 14 equações cúbicas que não eram redutíveis a uma forma linear ou quadrática. Elas são:

$$\begin{aligned} X^3 &= d \\ X^3 + cX &= d \\ X^3 + d &= cX \\ X^3 &= cX + d \\ X^3 + bX^2 &= d \\ X^3 &= bX^2 + d \\ X^3 + d &= bX^2 \\ X^3 + bX^2 + cX &= d \\ X^3 + bX^2 + d &= cX \\ X^3 + cX + d &= bX^2 \\ X^3 &= bX^2 + cX + d \\ X^3 + bX^2 &= cX + d \\ X^3 + cX &= bX^2 + d \\ X^3 + d &= bX^2 + cX \end{aligned}$$

Nem todas as raízes foram dadas, já que não eram aceitas raízes negativas.

Segundo o métodos de Khayyam, uma solução geométrica para uma equação cúbica do tipo

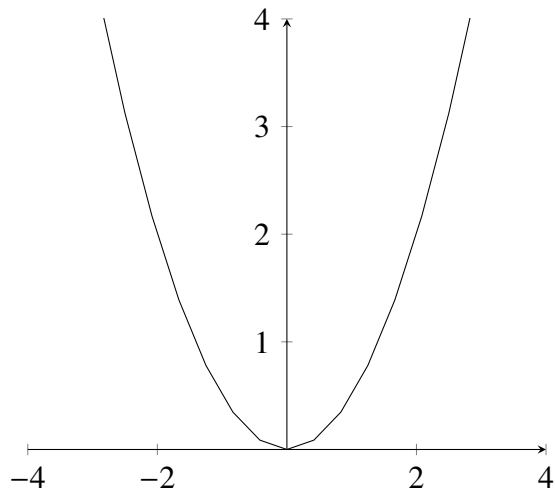
$$X^3 + c^2X = d.$$

envolve a interseção entre a parábola $X^2 = cY$ e o círculo $Y^2 = X(d - X)$.

Por exemplo, para resolver $X^3 + 4X = 16$ basta fazer a interseção entre a parábola $X^2 = 2Y$, ilustrada na Figura 2.5. e o círculo $Y^2 = X(4 - X)$, ilustrado na Figura 2.6.

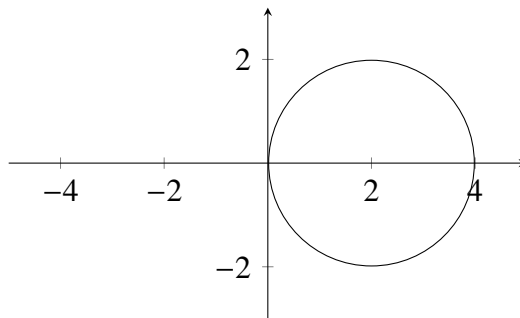
Intersectando essas duas cônicas, temos que a abscissa da interseção é 2, que é a solução desejada. A interseção pode ser visualizada na Figura 2.7.

Figura 2.5: Parábola $X^2 = 2Y$.



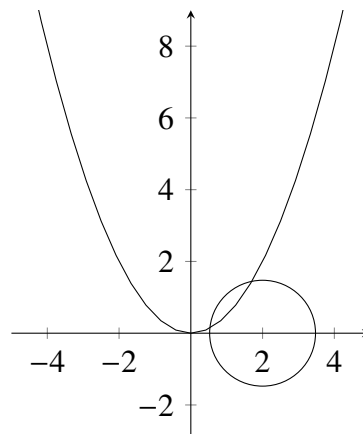
Fonte: Elaborado pelo autor (2023).

Figura 2.6: Círculo $X^2 + Y^2 = 4$.



Fonte: Elaborado pelo autor (2023).

Figura 2.7: Interseção ente a parábola e o círculo.



Fonte: Elaborado pelo autor (2023).

3 Resolução por radicais

Nesse momento vamos discorrer sobre a importância das equações algébricas, bem como maneiras de resolvê-las, com o intuito de proporcionar um melhor entendimento das descobertas tratadas até aqui.

As equações algébricas, exponenciais, diferenciais, trigonométricas ou de qualquer natureza, são uma das partes mais importantes da matemática. Quando pensamos em resolver um problema que pode ser solucionado por meio de operações básicas (adição, subtração, multiplicação, divisão e obtenção de raízes) ou radicais em função de seus coeficientes, de maneira direta ou indireta, estamos utilizando equações.

Dizemos que uma equação algébrica é solúvel por radicais quando as soluções destas são dadas por expressões algébricas, isto é, soma, multiplicação, potência e sua inversas: subtração, divisão e radiciação. Essa maneira de resolver as equações significa encontrar soluções por meio da manipulação de seus coeficientes através das quatro operações aritméticas e da extração de raízes.

As equações de segundo grau apareceram na matemática nas tabuletas de argila da Suméria, aproximadamente 1700 anos antes de Cristo e, ocasionalmente, levaram a radicais de números negativos; porém, não foram elas, em momento algum, que sugeriram o uso de números complexos. A rigor, uma equação era vista como a formulação matemática de um problema concreto; assim, se no processo de resolução aparecia uma raiz quadrada de um número negativo, isto era interpretado apenas como uma indicação de que o problema originalmente proposto não tinha solução.

Tentando resolver equações de grau três e quatro, os matemáticos acabavam caindo em outro problema, apareciam raízes de números negativos. Cardano se referia às raízes quadradas de números negativos como “*sofísticas*” e que seu resultado era “tão sutil quanto inútil”. Aparentemente, tratadas como uma anomalia, as raízes quadradas de números negativos foram denominadas pelos antigos algebristas por casos irreduzíveis das equações cúbicas.

Foi Rafael Bombelli, engenheiro hidráulico nascido na Bolonha, Itália, em 1530, quem conseguiu atravessar a barreira e chegar aos novos números. Conforme seu próprio relato em 1572 no livro *L'Algebra parte maggiore dell'Arithmetica*, sua ideia foi supor que os números $32 + \sqrt{-121}$ e $32 - \sqrt{-121}$ deveriam ser números da forma $a + \sqrt{-b}$ e $a - \sqrt{-b}$, respectivamente. Com algumas contas, ele chegou à conclusão que $a = 2$ e $b = 1$.

A partir da ideia pioneira de Bombelli, ainda demorou mais de dois séculos para que se

conseguisse, através de Euler, saber como extrair raízes de números complexos.

Nesse capítulo vamos exibir as soluções por meio de radicais de equações algébricas de graus 2, 3, 4 e 5. As principais referências utilizadas foram [5], [6] e [7].

3.1 Equação de grau 2

A fórmula geral para resolver as equações do 2º grau baseou-se na ideia de buscar uma maneira de reduzir o grau da equação do 2º grau para o 1º grau, através da extração de raízes quadradas. Considere a equação geral do 2º grau $aX^2 + bX + c = 0$, com coeficientes em \mathbb{C} e $a \neq 0$.

Subtraindo c em ambos os lados e dividindo por a , obtemos:

$$\frac{aX^2}{a} + \frac{bX}{a} = \frac{-c}{a},$$

ou seja,

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

A ideia agora é completar os quadrados do lado esquerdo da igualdade. Dessa forma devemos somar $\frac{b^2}{4a^2}$ dos dois lados da igualdade:

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

O lado esquerdo da igualdade pode ser escrito como $\left(X + \frac{b}{2a}\right)^2$ pois completamos a operação para que apareça um quadrado perfeito. O lado direito também pode ser reescrito efetuando a adição das duas frações:

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

Logo, temos a seguinte igualdade:

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}. \quad (3.1)$$

Extraindo a raiz quadrada dos dois lados da Equação (3.1):

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

obtemos

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

ou seja,

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

Esta é a famosa fórmula de Bhaskara, que não foi deduzida por ele, mas levou seu nome. Na época de Bhaskara não existia a simbologia utilizada agora.

3.2 Equação de grau 3

Citamos abaixo duas das principais personalidades responsáveis pela descoberta das soluções algébricas das equações cúbicas e quárticas. O primeiro é Niccolo Fontana (1499–1577), melhor conhecido por seu apelido, Tartaglia, que significa o gago. Quando os franceses atacaram a cidade natal de Tartaglia, Brescia, em 1512, um soldado o cortou horivelmente em sua face e mandíbula. Ele sobreviveu ao ataque, porém ficou com cicatrizes que o impediam de falar claramente. Pouco se sabe sobre sua educação anterior ou família, mas a história o descreve como um talentoso matemático, [12]. Existem alguns questionamentos acerca da originalidade de alguns dos trabalhos publicados por ele. *Quesiti et inventioni diverse* e uma tradução arquimediana, continham ambos trabalhos de outros publicados como sendo de Tartaglia. O que ele de fato possuía era uma solução original para um tipo de equação cúbica. Esse tipo de descoberta não era algo a se compartilhar, pois a habilidade de resolver equações que ninguém mais conseguia poderia significar vitória certa em desafios públicos com outros matemáticos. Esses sucessos poderiam acarretar em indicações acadêmicas de prestígio. Antes disso, o talentoso professor Scipione del Ferro havia descoberto uma solução algébrica para uma equação cúbica do tipo,

$$X^3 + bX = c,$$

chamada de cúbica “reduzida” pela ausência de um termo quadrático. Em seu leito de morte, ele passou seu segredo para um de seus alunos, Antonio Fior, que então desafiou Tartaglia. Tartaglia já conhecia a solução de equações cúbicas do tipo

$$X^3 + aX^2 = c,$$

e quando Fior o enviou trinta cúbicas reduzidas para resolver ele trabalhou incessantemente para descobrir a solução. Ele obteve sucesso em 12 de fevereiro de 1535 e foi capaz de resolver todos os problemas de Fior. Por outro lado, Fior não foi capaz de resolver nenhum dos problemas propostos por Tartaglia, que foi o vencedor do desafio. A notícia dessa vitória chegou até Cardano que prontamente o convidou para sua residência em Milão. Tartaglia planejava publicar sua resolução da cúbica, porém Cardano o persuadiu a revelar seu segredo com o juramento solene:

Eu juro a você pelo Evangelho Sagrado, e em minha fé como um cavalheiro, não apenas nunca publicar suas descobertas, se contá-las a mim, mas também prometo e assumo um compromisso de fé como um verdadeiro cristão de escrevê-las de modo cifrado para que ninguém as entenda depois de minha morte, [13].

Por conseguinte, em Milão, no dia 23 de março de 1539, Tartaglia contou seu segredo em um poema:

Quando o cubo e coisas juntas
São iguais a um número discreto,

Encontre outros dois números diferentes em um presente.
 Em seguida, você vai manter isso como um hábito
 Que o seu produto deve sempre ser igual
 Precisamente para o cubo de um terço das coisas.
 O restante, em seguida, como uma regra geral
 De suas raízes cúbicas subtraído
 Será igual à sua coisa principal, [14].

Tartaglia ficou furioso quando em 1545, Cardano publicou a solução da cúbica em seu livro *Ars Magna*, a “Grande Arte”. Tartaglia protestou alta e frequentemente, escrevendo diversas cartas ofensivas. Cardano não a respondeu nenhuma delas, porém foi defendido por seu aluno Ludovico Ferrari, que depois venceu Tartaglia em um desafio. Tartaglia contou sua versão da controvérsia com Cardano em seu livro *Qvestiti ed invenzioni diverse* em 1546.

O matemático Girolamo Cardano (1501 – 1576) de Milão pode ser considerado o “mais bizarro personagem de toda história da matemática”, [13]. Ele esteve envolvido na solução algébrica da equação cúbica, que foi o maior avanço matemático desde o tempo dos gregos. Era professor em Bolonha e Milão e um escritor produtivo. Seus escritos consistem de mais de sete mil páginas abordando tópicos como matemática, ciência, filosofia e religião. Muito do que sabemos sobre sua vida vem de seu próprio livro *De Vita Propria Liber* (“O livro da minha vida”), [15]. Cardano era médico que a princípio fora proibido de praticar medicina em Milão e acreditava que o motivo disso era por ele ser ilegítimo. Se mudou para Sacco, onde se casou e teve três filhos, porém sua vida particular foi trágica. Sua esposa morreu aos 31 anos de idade, um de seus filhos foi decapitado por matar a própria esposa, e outro deles era um criminoso. Cardano também foi preso em 1570 por escrever o horóscopo de Jesus. Excertos de seus próprios escritos apontam um estilo de vida inusitado. Ele era atormentado pela insônia e constantemente se machucava propositalmente pois “Eu considerava que o prazer consistia do alívio seguido da dor severa,” [15]. Era um astrólogo fervoroso e clarividente, acreditava em espíritos e afirmava possuir um espírito assistente com quem conversava.

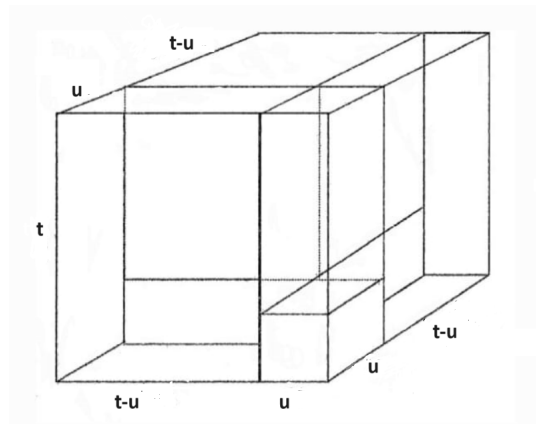
Fora o aspecto pessoal, a história do trabalho de Cardano nas equações cúbicas e quárticas é intrigante. Ele e seu aluno, Luigi Ferrari, progrediram significativamente a partir do que receberam de Tartaglia e foram capazes de apresentar soluções para equações cúbicas e quárticas gerais. Cardano publicou esses resultados em seu famoso livro *Ars Magna*, [15]. Tartaglia não ficou satisfeito. Ele disse que Cardano havia quebrado um juramento sagrado e era um canalha vil. Cardano jamais respondeu às acusações de Tartaglia.

Um esboço na margem de *Ars Magna* mostra que a solução de Cardano envolvia dividir o cubo em seis sólidos [16], conforme Figura 3.1.

O volume do cubo maior é t^3 e os seis sólidos são:

- Dois cubos, um com volume $(t - u)^3$ e outro com volume u^3 .
- Quatro prismas retangulares, dois com volume $ut(t - u)$, um com volume $u(t - u)^2$ e o último com volume $u^2(t - u)$.

Figura 3.1: Divisão do cubo e seis sólidos.



Fonte: Elaborado pelo autor (2023).

Algebricamente,

$$\begin{aligned} t^3 &= 2ut(t-u) + u(t-u)^2 + u^2(t-u) + (t-u)^3 + u^3 \\ t^3 - u^3 &= 2ut(t-u) + u(t-u)^2 + u^2(t-u) + (t-u)^3. \end{aligned} \quad (3.2)$$

A Equação (3.2) pode ser simplificada como

$$(t-u)^3 + 3ut(t-u) = t^3 - u^3.$$

Com isso, temos a seguinte equação cúbica

$$X^3 + cX - d = 0, \quad (3.3)$$

onde

$$X = t - u \quad (3.4)$$

$$c = 3ut \quad (3.5)$$

$$d = t^3 - u^3. \quad (3.6)$$

Se isolarmos u em (3.5), obtemos

$$u = \frac{c}{3t}.$$

Substitua esse valor de u em (3.6) para obter:

$$d = t^3 - \frac{c^3}{27t^3},$$

o que é equivalente a

$$\begin{aligned} 27dt^3 &= 27t^6 - c^3 \\ 27t^6 - 27dt^3 - c^3 &= 0. \end{aligned} \quad (3.7)$$

Para encontrar t devemos aplicar a fórmula de Bhaskara na Equação (3.7):

$$\begin{aligned} t^3 &= \frac{27d \pm \sqrt{(27d)^2 + 4 \cdot 27 \cdot c^3}}{54} \\ &= \frac{d}{2} \pm \sqrt{\frac{d^2}{4} + \frac{c^3}{27}}. \end{aligned} \quad (3.8)$$

Como $t^3 - u^3 = d$,

$$u^3 = t^3 - d = -\frac{d}{2} \pm \sqrt{\frac{d^2}{4} + \frac{c^3}{27}} \quad (3.9)$$

e como $X = t - u$, obtemos que a Equação (3.3) possui como soluções X_1 , X_2 e X_3 , chamadas de fórmulas de Cardano, que são obtidas combinando as expressões (3.8) e (3.9) e tomando a raiz cúbica.

$$X_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \quad (3.10)$$

$$X_2 = \zeta_3 \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \zeta_3^2 \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \quad (3.11)$$

$$X_3 = \zeta_3^2 \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \zeta_3 \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \quad (3.12)$$

em que $\zeta_3 = \frac{-1 + i\sqrt{3}}{2}$ é uma das raízes cúbicas da unidade.

Observação 3.1. Por meio de uma mudança de variável podemos colocar o polinômio

$$X^3 + a_2X^2 + a_1X + a_0 = 0 \quad (3.13)$$

numa forma onde não figure o termo do segundo grau, conforme a Equação (3.3). De fato, basta substituir X por $Y + d$ na Equação (3.13) e após realizar os cálculos, substituir d por $-\frac{a_2}{3}$, e teremos uma expressão da forma

$$Y^3 + pY + q = 0, \quad (3.14)$$

onde $p = a_1 - \frac{a_2^2}{3}$ e $q = \frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0$, cujas soluções são X_1 , X_2 , X_3 dadas em (3.10), (3.11) e (3.12).

Muitas tentativas foram feitas para exprimir as raízes de equações do 3º grau com coeficientes racionais, irreduzíveis em $\mathbb{Q}[x]$ e possuindo todas as raízes reais em termos de radicais reais, todas fracassadas. Este caso é chamado de *caso irreduzível*, isto é, quando $\frac{q^2}{4} + \frac{p^3}{27} < 0$ e foi somente no século 19 que essa questão foi esclarecida, demonstrando-se através da Teoria de Galois que, nesse caso, é impossível exprimir as raízes da equação em apenas termos de radicais reais.

Na atualidade as fórmulas de Cardano têm mais interesse teórico e histórico do que prático. Para calcular boas aproximações de equações algébricas dispõe-se de métodos numéricos muito mais mais eficientes.

Exemplo 3.2. Vamos resolver a equação

$$X^3 - 9X^2 + 3X - 4 = 0 \quad (3.15)$$

usando as fórmulas de Cardano.

Substituindo

$$\begin{aligned} X &= Y - \frac{a_2}{3} \\ &= Y - \frac{-9}{3} \\ &= Y + 3, \end{aligned}$$

a Equação (3.15) se transforma em $Y^3 - 24Y - 49 = 0$ cujas solução são dadas pelas fórmulas de Cardano (3.10), (3.11) e (3.13):

$$\begin{aligned} X_1 &= \sqrt[3]{-\frac{-49}{2} + \sqrt{\frac{(-49)^2}{4} + \frac{(-24)^3}{27}}} + \sqrt[3]{-\frac{-49}{2} - \sqrt{\frac{(-49)^2}{4} + \frac{(-24)^3}{27}}} \\ X_2 &= \zeta_3 \sqrt[3]{-\frac{-49}{2} + \sqrt{\frac{(-49)^2}{4} + \frac{(-24)^3}{27}}} + \zeta_3^2 \sqrt[3]{-\frac{-49}{2} - \sqrt{\frac{(-49)^2}{4} + \frac{(-24)^3}{27}}} \\ X_3 &= \zeta_3^2 \sqrt[3]{-\frac{-49}{2} + \sqrt{\frac{(-49)^2}{4} + \frac{(-24)^3}{27}}} + \zeta_3 \sqrt[3]{-\frac{-49}{2} - \sqrt{\frac{(-49)^2}{4} + \frac{(-24)^3}{27}}}, \end{aligned}$$

em que $\zeta_3 = \frac{-1 + i\sqrt{3}}{2}$ é uma das raízes cúbicas da unidade.

3.3 Equação de grau 4

Ludovico Ferrari (1522-1560), nascido em Bolonha, era de família muito humilde e aos 15 anos de idade foi trabalhar como servo na residência de Cardano, o qual percebendo sua notável inteligência, o promoveu a seu secretário. Como já dissemos, os matemáticos daquela época tinham o costume de promover desafios e certo Zuanne de Tonini da Coi propôs a Cardano uma questão que envolvia a equação: $X^4 - 6X^2 - 60X + 36 = 0$. Após inúmeras tentativas, Cardano não obteve êxito e passou a questão a seu aluno Ferrari, que acabou por encontrar a fórmula geral para a solução das equações do 4º grau. Este método encontrado por Ferrari também foi publicado por Cardano na *Ars Magna*, em continuidade à solução das equações do 3º grau. Ferrari buscou reescrever a equação, usando as operações permitidas pelos axiomas de Euclides, de modo a obter quadrados perfeitos e assim reduzir o problema à resolução de uma equação do 2º grau que era possível usando a fórmula de Bhaskara. Este método permite a exibição das

quatro raízes da equação, assim como a fórmula de Bhaskara permite a exibição das duas raízes da equação do 2º grau.

Apresentaremos aqui o método de Ferrari para resolução da equação do 4º grau. Considere a equação:

$$X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 = 0. \quad (3.16)$$

Temos que

$$X^4 + a_3X^3 = -(a_2X^2 + a_1X + a_0). \quad (3.17)$$

Completando o quadrado no primeiro membro da Equação (3.16) e ajustando o segundo membro, temos

$$\left(X^2 + \frac{1}{2}a_3X\right)^2 = \left(\frac{1}{4}a_3^2 - a_2\right)X^2 - a_1X - a_0. \quad (3.18)$$

Se o segundo membro da Equação (3.18) fosse um quadrado perfeito, a resolução da Equação (3.18) recairia na resolução de duas equações do segundo grau. Desta forma, vamos transformar o segundo membro da Equação (3.18) em um quadrado perfeito, sem destruir o quadrado perfeito do primeiro membro.

Somando a expressão $Y^2 + 2Y\left(X^2 + \frac{1}{2}a_3X\right)$ a ambos os membros de (3.18), obtemos

$$\left[\left(X^2 + \frac{1}{2}a_3X\right) + Y\right]^2 = \left(2Y + \frac{1}{4}a_3^2 - a_2\right)X^2 + (Ya_3 - a_1)X + (Y^2 - a_0). \quad (3.19)$$

Vamos agora determinar os valores de Y que transformarão o segundo membro de (3.19) em um quadrado perfeito. Para que isto aconteça, devemos ter o discriminante do segundo membro de (3.19), como trinômio do segundo grau em X nulo, isto é,

$$(Ya_3 - a_1)^2 - 4 \cdot \left(2Y + \frac{1}{4}a_3^2 - a_2\right) \cdot (Y^2 - a_0) = 0. \quad (3.20)$$

Daí,

$$8Y^3 - 4a_2Y^2 + (2a_1a_3 - 8a_0)Y + (4a_0a_2 - a_0a_3^2 - a_1^2) = 0. \quad (3.21)$$

Escolhendo Y como sendo uma das raízes da Equação (3.21), a Equação (3.19) nos dá

$$\left[\left(X^2 + \frac{1}{2}a_3X\right) + Y\right]^2 = (\alpha X + \beta)^2, \quad (3.22)$$

com α e β convenientes. A Equação (3.22) se resolve mediante a resolução das duas seguintes equações do segundo grau:

$$\left(X^2 + \frac{1}{2}a_3X\right) + Y = (\alpha X + \beta) \quad \text{e} \quad \left(X^2 + \frac{1}{2}a_3X\right) + Y = -(\alpha X + \beta)$$

Como a Equação (3.16) é equivalente à Equação (3.22), temos que a resolução de uma equação do quarto grau pode ser reduzida à resolução de equações de graus dois e três.

Exemplo 3.3. Exemplo 2.8

$$X^4 - 2X^3 + 2X^2 - X - 2 = 0$$

Solução: Primeiramente, completando os quadrados temos

$$X^4 - 2X^3 = -2X^2 + X + 2.$$

Com isso, foi somado X^2 no primeiro e segundo membro, temos:

$$\begin{aligned} (X^2)^2 - 2 \cdot (X^2) \cdot (X + X^2) &= -2X^2 + X + 2 + X^2 \\ (X^2 - X)^2 &= -X + X + 2 \\ Y^2 + 2Y \cdot (X^2 - X)^2 &= -X^2 + X + 2 + Y^2 + 2Y(X^2 - X) \\ (Y + (X^2 - X))^2 &= (-1 + 2Y) \cdot X^2 + (1 - 2Y) \cdot X + 2 + Y^2 \end{aligned} \quad (3.23)$$

Resolvendo a equação do 2 grau do segundo membro de (3.23), temos

$$\begin{aligned} \Delta &= (1 - 2Y)^2 - 4 \cdot (-1 + 2Y) \cdot (2 + Y^2) \\ \Delta &= (1 - 2Y) \left[(1 - 2Y) + 4 \cdot (2 + Y^2) \right] \quad \text{onde } Y = \frac{1}{2}. \end{aligned}$$

Substituindo o $Y = \frac{1}{2}$ em (3.23)

$$\begin{aligned} \left(\frac{1}{2} + X^2 - X \right) &= 2 + \left(\frac{1}{2} \right)^2 = \frac{9}{4} \\ \left(\frac{1}{2} + X^2 - X \right) &= \pm \sqrt{\frac{9}{4}} = \pm \frac{3}{2} \end{aligned}$$

$$\begin{array}{ll} X^2 - X + \frac{1}{2} = \frac{3}{2} & \text{ou} \quad X^2 - X + \frac{1}{2} = \frac{3}{2} \\ X^2 - X - 1 = 0 & X^2 - X + 2 = 0 \\ \Delta = 1 - 4 \cdot 1 \cdot (-1) \Rightarrow \Delta = 5 & \Delta = 1 - 4 \cdot 1 \cdot 2 \Rightarrow \Delta = -7 \\ X = \frac{1 \pm \sqrt{5}}{2} & X = \frac{1 \pm \sqrt{-7}}{2} \Rightarrow X = \frac{1 \pm \sqrt{7}i}{2} \end{array}$$

Portanto, as raízes da equação são:

$$\left\{ \begin{array}{l} X_1 = \frac{1 + \sqrt{5}}{2} \\ X_2 = \frac{1 - \sqrt{5}}{2} \\ X_3 = \frac{1 + \sqrt{7}i}{2} \\ X_4 = \frac{1 - \sqrt{7}i}{2} \end{array} \right.$$

Observação 3.4. Os métodos resolutivos por radicais mostrados, permitem dizer que as equações de grau 2, 3 e 4 podem ser resolvidas com cálculos relativamente simples. É natural então que os matemáticos procurassem resolver as equações de quinto grau ou mais da mesma forma.

3.4 Equações de grau $n \geq 5$

Resolvidas as equações polinomiais, com coeficientes complexos, até o grau quarto, uma pergunta natural que se coloca é se as equações de grau maior do que 4 possuem sempre raízes complexas e, em tal caso, se há uma fórmula algébrica geral que expresse as raízes dessas equações em função dos seus coeficientes usando as operações algébricas racionais e raízes de graus naturais.

A primeira pergunta é respondida afirmativamente pelo Teorema Fundamental da Álgebra (Teorema A.31). A segunda pergunta foi respondida como negativa pelo matemático norueguês Niels Henrik Abel (1802-1829), em um artigo publicado em 1829, para as equações gerais de graus maiores ou iguais do que cinco.

Teorema 3.5. *(Teorema de Abel-Ruffini) Não existe fórmula para as soluções da equação geral de grau maior ou igual a 5 usando apenas as operações $+$, $-$, \times , \div e $\sqrt{\quad}$.*

A palavra “geral” é importante. Ela enfatiza que não existe uma fórmula que seja válida para uma escolha arbitrária de coeficientes. Contudo, o teorema não exclui a possibilidade de algumas equações possuírem soluções que possam ser escritas em termos das operações $+$, $-$, \times , \div , $\sqrt{\quad}$.

Na maioria dos livros didáticos, a demonstração deste importante resultado depende do conhecimento de uma poderosa vertente da matemática, chamada Teoria de Galois, desenvolvida quase exclusivamente por Évariste Galois no começo do século XIX. Essa teoria resolveu todos os problemas de insolubilidade de uma vez por todas, assim como outros problemas milenares. Porém, é um tanto avançada e geralmente ensinada no terceiro ou quarto ano de cursos especializados de matemática de nível superior.

A primeira demonstração completa de Abel do Teorema de Abel-Ruffini é alguns anos mais velha que a Teoria de Galois. Além disso, os trabalhos de Galois demoraram diversas décadas para serem amplamente conhecidos por outros matemáticos. Em outras palavras, nem Ruffini e nem Abel usaram os métodos desenvolvidos por Abel para provar que algumas equações eram insolúveis.

Por geralmente depender de matemática avançada, poucos membros da comunidade científica sabem desse teorema e seus princípios subjacentes. Porém, como Abel não demonstrou o resultado dessa forma, deve existir outra forma, talvez mais simples, de entender o motivo pelo qual a equação quártica geral não possui solução em termos de radicais. Em particular, as ideias de Galois, Abel e Ruffini se baseiam em um único e fundamental ponto: a simetria de uma equação algébrica sob a permutação de suas soluções. Baseado somente nessa simetria

fundamental, esboçaremos no Capítulo 4 uma prova do Teorema de Abel-Ruffini usando apenas conhecimentos elementares de números complexos, laços e permutações.

4 Uma demonstração do Teorema de Abel-Ruffini usando permutações e laços

A ideia de examinar permutações de raízes para estudar a (in-)solubilidade de equações algébricas teve sua origem em 1771 com os trabalhos pioneiros de J.-L. Lagrange [17]. As ideias de Lagrange amadureceram, e foram finalmente estendidas à equação quártica por Paul Ruffini no começo dos anos 1800. Apesar de, tecnicamente, Ruffini não ter provado o teorema que hoje carrega seu nome, seus resultados eram fortes o suficiente para levantar sérias dúvidas a respeito da possibilidade de se encontrar uma solução para a equação quártica geral. Finalmente, em 1824, N.-H. Abel escreveu a primeira demonstração completa do teorema. Ele recebeu postumamente o *Grand Prix de l'Académie des Sciences de Paris* em 1830 como forma de reconhecimento por seu trabalho. Esse mesmo ano marca a primeira publicação de É. Galois a respeito desses tópicos, no qual ele fornece as premissas do que hoje recebe o nome de Teoria de Galois, uma extensão inovadora e elegante de todos os resultados prévios. Ele morreu cedo, aos 20 anos em 1832, e seu trabalho também demorou décadas para ser completamente publicado e reconhecido como revolucionário. O objetivo desse capítulo é esboçar uma demonstração autocontida e acessível usando laços e permutações do Teorema de Abel-Ruffini, que afirma que a solução geral de uma equação algébrica de grau cinco ou mais não pode ser escrita usando radicais, ou seja, utilizando seus coeficientes e operações aritméticas $+$, $-$, \times , \div e $\sqrt{\quad}$. Este é o principal capítulo do nosso trabalho, que trata sobre uma abordagem e resultados recentes, publicados por Paul Ramond em 2022, [8].

4.1 Permutações, Laços, Raízes e F , G , H -funções

Vamos tratar de equações algébricas de grau $n \geq 2$. Tais equações têm sempre a forma

$$z^n + c_{n-1}z^{n-1} + \cdots + c_1z + c_0 = 0, \quad (4.1)$$

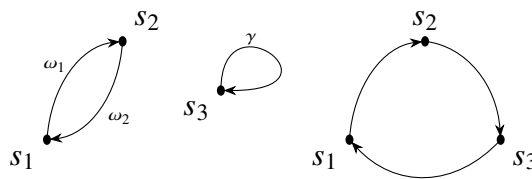
onde $z \in \mathbb{C}$ é a incógnita e os n números complexos (c_0, \dots, c_{n-1}) são os coeficientes. Notavelmente, a equação (4.1) sempre possui exatamente n soluções complexas se contadas com suas multiplicidades, fato conhecido como Teorema Fundamental da Álgebra (Teorema A.31). Essas soluções serão sempre denotadas por (s_1, \dots, s_n) , e usaremos s para nos referir a uma solução qualquer.

Permutações

A base de nossa estratégia será imaginar as soluções (s_1, \dots, s_n) no plano complexo e fazê-las trocarem de lugar, ou seja, permutá-las. Precisaremos de dois tipos de permutação:

- transposições, denotadas por (ij) , que trocam a posição de duas soluções, isto é, $s_i \leftrightarrow s_j$. A transposição (12) é ilustrada na Figura 4.1, duas curvas à esquerda.
- ciclos, denotados por (ijk) , que trocam ciclicamente a posição de três soluções, ou seja, $s_i \rightarrow s_j, s_j \rightarrow s_k$ e $s_k \rightarrow s_i$. O ciclo (123) é ilustrado na Figura 4.1, curva à direita.

Figura 4.1: As duas curvas à esquerda denotam a transposição (12) e curva à direita, o ciclo (123) , ambos permutando soluções (s_1, s_2, s_3) de uma equação algébrica de grau $n \geq 3$.



Fonte: Elaborado pelo autor (2023).

Observação 4.1. Duas permutações seguidas devem ser realizadas em sequência da esquerda para a direita. Por exemplo, $(12)(23)$ consiste em trocar s_1 com s_2 , depois s_2 com s_3 . Veja que o resultado é equivalente ao ciclo (132) , logo não existe um único jeito de escrever permutações. No entanto, permutações geralmente não comutam. De fato, $(12)(23) = (132)$ e $(23)(12) = (123)$, ou seja, $(12)(23) \neq (23)(12)$.

Laços

Uma forma de visualizar permutações de (s_1, \dots, s_n) é localizar essas soluções no plano complexo e fazê-las percorrer certos caminhos. No plano complexo, esses caminhos são curvas contínuas que não possuem auto-interseção e ligam dois pontos. Um caminho que fecha, isto é, que conecta um ponto a si mesmo, será chamado de laço e denotado por γ , já um caminho que conecta dois pontos distintos é chamado de caminho aberto e denotado por ω . Vamos usar esses caminhos para induzir permutações em (s_1, \dots, s_n) .

Exemplo 4.2. Na Figura 4.1 a transposição (12) é induzida pelos caminhos abertos ω_1 e ω_2 , que trocam s_1 e s_2 de lugar, enquanto s_3 percorre o laço γ . Ao tratar de permutações, vamos sempre imaginar as soluções percorrendo esses caminhos.

Raízes

Vamos agora examinar como as raízes de números complexos se movimentam no plano complexo.

Fixando um número complexo z , uma raiz de z é algum número $\zeta \in \mathbb{C}$ tal que $\zeta^k = z$ para algum $k \in \mathbb{N}$. Esse número complexo ζ recebe o nome de raiz k -ésima de z e pelo Teorema Fundamental da Álgebra (Teorema A.31) z admite exatamente k tais k -ésimas raízes.

Vamos usar a notação ambígua $\sqrt[k]{z}$ para denotar qualquer uma das raízes k -ésimas de z . Fixando $k \in \mathbb{N}$ e supondo que z percorre um laço γ , examinemos que tipo de caminho $\sqrt[k]{z}$ percorre. Para isso, utilizemos a forma polar de z : $z = r e^{i\theta}$ com $r = |z|$ e $\theta = \arg z$, a partir do qual podemos explicitar todas as raízes k -ésimas $(\zeta_1, \dots, \zeta_k)$ como

$$\zeta_\ell = r^{1/k} e^{i(\theta+2\pi\ell)/k}, \quad \ell \in \{1, \dots, k\}. \quad (4.2)$$

Da Equação (4.2) é possível observar que todas as raízes de z têm o mesmo módulo: $r^{1/k}$. Geometricamente, isso significa que todas as raízes estão sobre um mesmo círculo no plano complexo de raio $r^{1/k}$. Além disso, a Equação (4.2) produz

$$\arg \zeta_\ell = \frac{\theta}{k} + \ell \frac{2\pi}{k}, \quad (4.3)$$

o que significa que todas as raízes estão igualmente espaçadas nesse círculo, separadas por um ângulo de $2\pi/k$.

Agora suponha que z percorre o plano complexo, viajando em um laço γ que circunda uma vez (digamos) a origem, no sentido anti-horário (em vermelho, à esquerda na Figura 4.2). À medida que z percorre γ , suas raízes k -ésimas também se movem ao redor, e suas posições podem ser computadas a partir da equação (4.2) (veja os caminhos vermelhos à direita na Figura 4.2). Como γ é um laço, o raio r retorna ao seu valor original (isto é, antes do laço), e o mesmo ocorre com $r^{1/k}$. Em outras palavras, as raízes permanecem em seu círculo após o caminho γ (veja o círculo tracejado cinza à direita na Figura 4.2). No entanto, $\arg z$ foi de θ para $\theta + 2\pi$ (uma volta no sentido anti-horário). Portanto, a partir da Equação (4.3), cada raiz k -ésima ζ_ℓ se movimentou para seu vizinho mais próximo no sentido anti-horário, $\zeta_{\ell+1}$. Em particular, as raízes percorreram um caminho aberto. Se z não tivesse circundado a origem (em azul, à esquerda na Figura 4.2), seu argumento θ não teria sofrido nenhuma mudança líquida após o laço γ , e as raízes teriam percorrido seus próprios laços (em azul à direita na Figura 4.2).

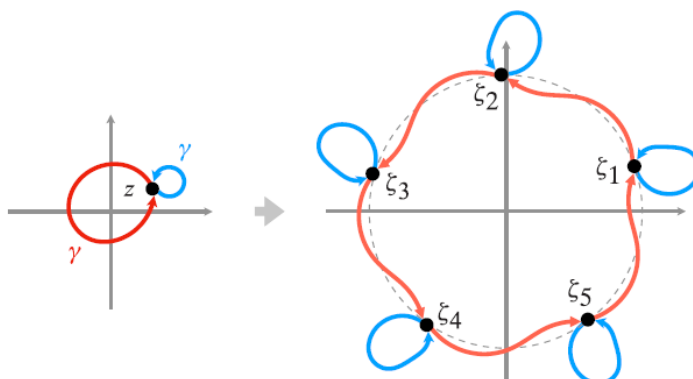
Quando z percorre um laço γ que não circunda a origem, suas raízes ζ_i também percorrem laços (à direita). No entanto, para o laço γ que circunda uma vez, as raízes então seguem os caminhos vermelhos, não fechados.

Observação 4.3. Vimos dois exemplos de laços percorridos por z e o resultado não é o mesmo para suas raízes $\sqrt[k]{z}$: em um caso as raízes seguem um laço (parte azul da Figura 4.2), no outro elas seguem um caminho aberto (parte vermelha da Figura 4.2). Conseqüentemente, concluímos que quando z percorre um laço, não necessariamente $\sqrt[k]{z}$ percorre um laço. Essa conclusão vale para qualquer tipo de raiz, ou seja, qualquer $k \in \mathbb{N}$ em $\sqrt[k]{z}$.

Provamos então o seguinte resultado:

Propriedade 4.4. Quando z percorre um laço, $\sqrt[k]{z}$ não necessariamente percorre um laço.

Figura 4.2: Quando z percorre um laço γ que não circunda a origem, suas raízes ζ_i também percorrem laços (à direita). No entanto, para o laço γ que circunda uma vez, as raízes então seguem os caminhos vermelhos, não fechados.



Fonte: Retirado de [8].

F , G , H -funções

Vamos examinar a existência de uma fórmula geral para as soluções da Equação (4.1) de grau n . Por “fórmula”, nos referimos a alguma igualdade

$$s = \Phi(c_0, \dots, c_{n-1}), \tag{4.4}$$

onde s é uma solução de (4.1) e Φ é alguma função de seus coeficientes (c_0, \dots, c_{n-1}) . O Teorema de Abel-Ruffini diz que para $n \geq 5$, não existe fórmula em termos de radicais, o que significa que Φ na equação (4.4) não pode ser construída apenas em termos

- dos coeficientes (c_0, \dots, c_{n-1}) ,
- das operações elementares $+$, $-$, \times , \div e $\sqrt{\quad}$.

Se nos restringimos à combinar os coeficientes (c_0, \dots, c_{n-1}) com as quatro operações elementares $+$, $-$, \times , \div , obtemos o que chamaremos uma F -fórmula, ou F -função.

Exemplo 4.5.

$$F = 1, F = -\frac{c_6}{2}, F = c_8^2 - 7c_2. \tag{4.5}$$

Estas são as peças fundamentais para a construção de fórmulas. Em particular, elas compreendem inteiros, os próprios coeficientes, assim como polinômios e funções racionais dos coeficientes. É evidente que se dois coeficientes percorrem um laço simultaneamente, a soma, diferença, produto e quociente deles também percorrem um laço. Como F -funções são construídas a partir apenas das quatro operações elementares, a mesma propriedade vale para as F -funções, ou seja, vale a seguinte propriedade:

Propriedade 4.6. Quando (c_0, \dots, c_{n-1}) percorrem um laço, F -funções também percorrem um laço.

Essa propriedade das F -funções não se aplica às \sqrt{F} -funções (raízes de F -funções), basta usar a Proposição 4.4. Em particular, se denotarmos por G -função uma combinação de F e \sqrt{F} -funções usando $+$, $-$, \times , \div , temos a seguinte propriedade:

Propriedade 4.7. Quando (c_0, \dots, c_{n-1}) percorrem um laço, G -funções não necessariamente percorrem um laço.

Uma G -função pode incluir expressões com um nível de raízes.

Exemplo 4.8.

$$G = -\frac{c_5}{2} + \frac{1}{2}\sqrt{c_4^2 - 4c_1}. \tag{4.6}$$

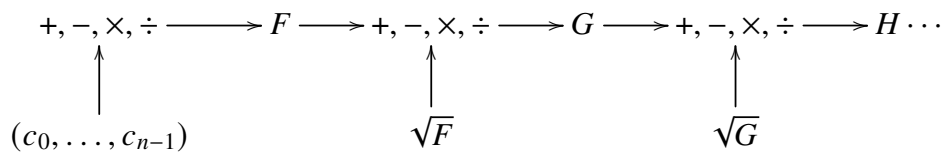
Podemos continuar com esse processo e construir fórmulas com um número cada vez maior de composição de raízes. Por exemplo, podemos combinar G e \sqrt{G} -funções com as 4 operações elementares para construir H -funções, que podem conter até dois níveis de raízes, e assim por diante, conforme resumo da Figura 4.3.

Exemplo 4.9.

$$H = c_4 - \sqrt[3]{7c_2} + \sqrt[5]{-\frac{c_0}{2} + \sqrt{c_1^2 - 4c_6}}. \tag{4.7}$$

Com essa nomenclatura, podemos construir expressões arbitrariamente complexas usando $+$, $-$, \times , \div e $\sqrt{\quad}$, e ao mesmo tempo saber quantas composições de raízes aparecem em cada fórmula. Reciprocamente, qualquer fórmula constituída de $+$, $-$, \times , \div e $\sqrt{\quad}$ pode ser construída usando esse procedimento.

Figura 4.3: Combinando coeficientes (c_0, \dots, c_{n-1}) com $+$, $-$, \times , \div define-se uma F -função. Combinando F -funções e suas raízes \sqrt{F} com $+$, $-$, \times , \div define-se uma G -função, e assim sucessivamente.



Fonte: Elaborado pelo autor (2023).

Assim, cobrimos todas as ferramentas que vamos utilizar: permutações de (s_1, \dots, s_n) , laços e F, G, H -funções. Agora aplicaremos esses conceitos à equação de grau n , começando com $n = 2$ para que possamos melhor compreender o Teorema de Abel-Ruffini quando $n = 5$.

4.2 A equação quadrática, cúbica e quártica

Começaremos explicando porque uma fórmula para a equação quadrática não pode ser escrita apenas com as quatro operações básicas. Ideias semelhantes serão então estendidas para

a cúbica e a quártica, fornecendo resultados de impossibilidade mais fortes a cada passo. Ao chegarmos na quártica, a estratégia usada nas provas já será familiar e permitirá o entendimento de como os resultados da equação quadrática, cúbica e quártica adiantam, de certo modo, a prova do Teorema de Abel-Ruffini. No caminho, também deduziremos as fórmulas da equação cúbica e da quártica. Estas serão importantes em um de nossos resultados provisórios e nos guiarão passo a passo para o Teorema de Abel-Ruffini.

4.2.1 A equação quadrática

Nosso caminho rumo ao Teorema de Abel-Ruffini se inicia com algumas considerações acerca da conhecida equação quadrática. Em particular, considerando $n = 2$, provaremos um primeiro resultado de impossibilidade que na realidade é válido para $n \geq 2$. As ideias desenvolvidas aqui são simples, mas indispensáveis à demonstração do Teorema de Abel-Ruffini.

Vamos considerar a equação quadrática geral

$$z^2 + c_1z + c_0 = 0. \quad (4.8)$$

Como mencionado anteriormente, o Teorema Fundamental da Álgebra garante que essa equação admite exatamente duas soluções complexas s_1 e s_2 . Podemos escrever a forma fatorada $(z - s_1)(z - s_2) = 0$, expandir esse produto e ordenar os termos por potências de z . Comparando essa expansão termo a termo com a Equação (4.8), obtemos das fórmulas de Vieta (A.3) que

$$c_1 = -(s_1 + s_2) \text{ e } c_0 = s_1s_2. \quad (4.9)$$

Da Equação (A.3) vemos que para $n \geq 2$ podemos permutar as soluções (s_1, \dots, s_n) da forma que quisermos e as fórmulas dos coeficientes são preservadas, o que revela uma propriedade fundamental:

Propriedade 4.10. Os coeficientes c_0, \dots, c_{n-1} são funções simétricas das soluções (s_1, \dots, s_n) , ou seja, tem-se que

$$c_i = f_i(s_1, \dots, s_n) \quad \forall i \in \{0, 1, \dots, n-1\},$$

e

$$c_i = f_i(\sigma(s_1), \dots, \sigma(s_n)) \quad \forall i \in \{0, 1, \dots, n-1\},$$

onde $\sigma: \{s_1, \dots, s_n\} \rightarrow \{s_1, \dots, s_n\}$ é uma permutação qualquer das soluções.

Em particular, para o caso $n = 2$, se permutarmos as soluções s_1 e s_2 as movendo continuamente pelo plano complexo (por exemplo, usando a transposição (12), descrita na Figura 4.1), então os coeficientes (c_0, c_1) vão cada um seguir um caminho, mas eventualmente eles devem retornar às suas posições iniciais, visto que são simétricos em (s_1, s_2) . Em outras palavras, (c_0, c_1) percorrerão um laço, conforme Figura 4.5.

A simetria das fórmulas de Vieta é um conceito central em nossa construção. Vamos então reformular-la de forma geométrica: *Quando (s_1, \dots, s_n) são permutadas, cada coeficiente (c_0, \dots, c_{n-1}) percorre um laço.*

Figura 4.4: A transposição (12) aplicada nas soluções (s_1, s_2) induz um laço nos coeficientes (c_0, c_1) .

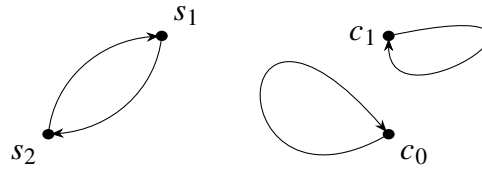


Figura 4.5: Elaborado pelo autor

Esse fato pode ser usado para demonstrar um primeiro resultado de impossibilidade como segue.

Teorema 4.11. *Não existe fórmula para a resolução de (4.1) utilizando apenas F -funções para $n \geq 2$.*

Demonstração. Primeiramente consideramos $n = 2$. Suponha que as soluções s_1 e s_2 da equação quadrática são dadas por duas fórmulas do tipo

$$s_1 = F_1(c_0, c_1) \text{ e } s_2 = F_2(c_0, c_1), \tag{4.10}$$

com F_1, F_2 duas F -funções, isto é, expressões envolvendo (c_0, c_1) e os símbolos $+, -, \times, \div$. Agora imagine (s_1, s_2) e (c_0, c_1) no plano complexo. Vamos realizar o seguinte processo:

- conectar as soluções s_1 e s_2 com caminhos que induzem a transposição (12) e fazê-las percorrer esses caminhos (ver Figura 4.5);
- conforme s_1 e s_2 se movimentam, c_0 e c_1 percorrem um laço cada, como visto anteriormente (ver Figura 4.5);
- enquanto c_0 e c_1 percorrem seus próprios laços, as duas F -funções F_1 e F_2 também percorrem um laço, como argumentamos anteriormente (ver Figura 4.6).

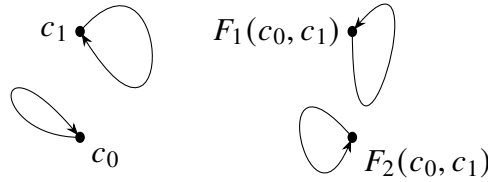
Ao fim desse processo, s_1 e s_2 foram permutadas, mas F_1 e F_2 percorreram um laço ainda. Consequentemente, F_1 e F_2 não podem ser iguais, respectivamente, à s_1 e s_2 e nenhuma fórmula como a Equação (4.10) existe.

Esta impossibilidade vale para qualquer grau $n \geq 2$. De fato, basta tomar duas das n soluções da equação de grau n e aplicar o raciocínio anterior.

□

O Teorema 4.11 nos diz que não há chance de encontrarmos uma fórmula para equações de grau $n \geq 2$ usando apenas F -funções.

Figura 4.6: Um laço percorrido por (c_0, c_1) induz um laço sobre as F -funções $F_1(c_0, c_1)$ e $F_2(c_0, c_1)$.



Fonte: Elaborado pelo autor (2023).

Observação 4.12. Vimos na Seção 3.1, que fazendo o completamento de quadrados obtemos as soluções s da Equação (4.8):

$$s = -\frac{c_1}{2} + \frac{1}{2}\sqrt{c_1^2 - 4c_0}. \quad (4.11)$$

Essa fórmula compreende ambas as soluções, uma para cada valor da raiz quadrada. Além disso, veja como a presença da raiz ratifica o resultado de impossibilidade dado pelo Teorema 4.11: é necessário utilizar uma \sqrt{F} -função para obter uma fórmula da equação quadrática. Entretanto, isto não exclui a possibilidade de certas equações quadráticas terem soluções que podem ser expressas apenas com as 4 operações fundamentais.

4.2.2 A equação cúbica

Vamos agora construir uma fórmula para as soluções da equação cúbica geral

$$z^3 + c_2z^2 + c_1z + c_0 = 0. \quad (4.12)$$

Sejam (s_1, s_2, s_3) suas três soluções complexas. Usando o que descobrimos anteriormente, consideramos agora também \sqrt{F} -funções para a construção das fórmulas. Logo, assumimos que existem fórmulas do tipo

$$s_i = G_i(c_0, c_1, c_2), \text{ para } i \in \{1, 2, 3\}, \quad (4.13)$$

com G_1, G_2, G_3 três G -funções (isto é, combinações de F e \sqrt{F} com $+$, $-$, \times , \div). O segundo resultado de impossibilidade que mostraremos é que fórmulas desse tipo não existem. Nossa estratégia anterior pode não funcionar, apesar dos coeficientes ainda percorrerem laços conforme permutamos as soluções, nada pode ser dito a respeito das G -funções nessas circunstâncias, como vimos anteriormente (Propriedade 4.7). Precisaremos adotar outra abordagem.

Considere a transposição (12) que induz um laço γ_1 em F e um caminho aberto ω_1 em \sqrt{F} . Considere também (23) induzindo um laço γ_2 em F e um caminho aberto ω_2 em \sqrt{F} .

Realizemos agora a seguinte sequência de transposições, chamada *comutador* de (12) e (23) e denotado por

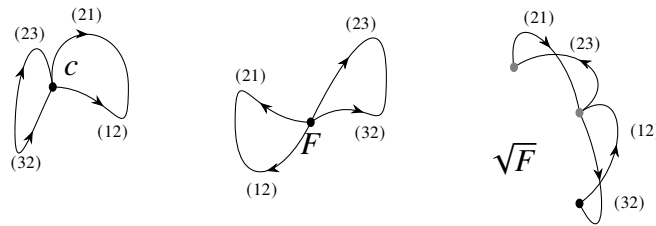
$$[(12), (23)] = (12)(23)(12)^{-1}(23)^{-1}. \tag{4.14}$$

Visto que $(12)^{-1} = (21)$ e $(23)^{-1} = (32)$, temos que $[(12), (23)] = (123)$. Na verdade, isso é válido para qualquer par de transposições [18]:

$$[(ij), (jk)] = (ijk). \tag{4.15}$$

Portanto, $[(12), (23)]$ permuta as soluções (s_1, s_2, s_3) , mas quais são seus efeitos sobre os números como F e \sqrt{F} ? Evidentemente, F percorre uma sequência de laços $\gamma_1\gamma_2\gamma_1^{-1}\gamma_2^{-1}$, que é em si um laço. Já o número \sqrt{F} percorre uma sequência de caminhos abertos $\omega_1\omega_2\omega_1^{-1}\omega_2^{-1}$ (visitando outras raízes), mas retorna ao ponto inicial por construção, ver Figura (4.7).

Figura 4.7: Efeito do comutador $[(12), (23)]$ num coeficiente c , numa F -função e numa \sqrt{F} -função. Ao fim do processo, F e \sqrt{F} percorreram laços. Note que o laço percorrido por \sqrt{F} é composto por 4 caminhos abertos.



Elaborado pelo autor (2023).

Com a permutação (123) escrita como o comutador $[(12), (23)]$, obtemos a mesma conclusão do caso quadrático: enquanto (s_1, s_2, s_3) sofre a permutação (123), F e \sqrt{F} percorrem um laço (e então qualquer G -função). Conseqüentemente, não podem existir igualdade como a Equação (4.13). Novamente esta conclusão vale para qualquer grau $n \geq 3$, basta tomar 3 soluções quaisquer e aplicar o raciocínio anterior. Portanto, temos o segundo resultado de impossibilidade.

Teorema 4.13. *Não existe fórmula para a resolução da equação geral (4.1) usando apenas G -funções para $n \geq 3$.*

Cabe enfatizar que nossa argumentação funciona apenas se aplicarmos o ciclo (123) na forma do comutador $[(12), (23)]$. Aplicando-o diretamente, não há garantia de que \sqrt{F} percorreria um laço. É o comutador que nos permite “descartar” um nível de raízes e, conseqüentemente, \sqrt{F} . Agora vamos testar esse resultado de impossibilidade resolvendo a cúbica explicitamente.

Observação 4.14. Note que as raízes X_1, X_2 e X_3 dadas em (3.10), (3.11) e (3.13) envolvem mais do que apenas F e \sqrt{F} -funções. De fato, as duas raízes cúbicas são \sqrt{G} -funções. A

fórmula cúbica contém, de certa forma, “dois níveis” de raízes, enquanto as G -funções contém apenas um, por definição. Esse tipo de expressão é uma composição de raízes. Nossa estratégia de comutadores foi apenas capaz de remover um nível de raízes. Veremos a seguir que dois comutadores serão capazes de remover dois níveis.

4.2.3 A equação quártica

Voltamos agora nossa atenção para a equação quártica

$$z^4 + c_3z^3 + c_2z^2 + c_1z + c_0 = 0. \quad (4.16)$$

Para a equação cúbica, vimos que G -funções não são suficientes para construirmos uma fórmula, são necessárias também \sqrt{G} -funções. Dessa forma, começamos assumindo a existência de fórmulas deste tipo para as quatro soluções

$$s_i = H_i(c_0, c_1, c_2, c_3) \text{ para } i \in \{1, 2, 3, 4\}, \quad (4.17)$$

onde H_i são H -funções, isto é, G e \sqrt{G} -funções combinadas com $+$, $-$, \times , \div . Seguindo o padrão dos resultados anteriores, é de se esperar que mesmo com a adição das \sqrt{G} -funções, ainda não conseguimos construir uma fórmula para a quártica. Provaremos isso construindo uma permutação apropriada de (s_1, s_2, s_3, s_4) .

Observação 4.15. Novamente, da mesma forma que o primeiro método não funcionou para a equação cúbica, o método da equação cúbica não será adequada para a quártica. De fato, o comutador de transposições induz um laço em F e \sqrt{F} , consequentemente em G . No entanto, um laço em G geralmente não induz um laço em \sqrt{G} , como visto anteriormente. Podemos resumir nossos métodos anteriores na Tabela 4.1.

| ingrediente | F -funções | G -funções |
|------------------|---------------|----------------------------|
| níveis de raízes | 0 | 1 |
| descartadas por | transposições | comutador de transposições |
| com o caminho | (12) | $[(12), (23)] = (123)$ |
| para grau | $n \geq 2$ | $n \geq 3$ |

Tabela 4.1: Resumo dos métodos utilizados para demonstrar os dois primeiros resultados de impossibilidade.

Agora, vamos considerar o comutador de, por exemplo, (123) e (234), escrito como um comutador deles mesmos, usando a equação (4.15). Vamos examinar essa possibilidade.

Primeiramente, observamos que $[(123), (234)]$ de fato permuta (s_1, s_2, s_3, s_4) , visto que

$$[(123), (234)] = (14)(23), \quad (4.18)$$

o que é um caso particular do resultado geral $[(ijk)(jkl)] = (il)(jk)$. Agora, examinemos como essa permutação afeta G e \sqrt{G} -funções:

- Primeiro aplicamos os ciclos $(123) = [(12), (23)]$ e depois $(234) = [(23), (34)]$. Como eles são comutadores, as G -funções percorrerão dois laços γ_1, γ_2 em sequência, retornando às suas posições originais. Contudo, quantidades como \sqrt{G} se moverão ao longo de dois caminhos geralmente abertos ω_1 e ω_2 . Tudo isso ocorre exatamente como no caso quártico.
- Depois disso, aplicamos os caminhos inversos na ordem oposta, ou seja, $(432) = [(43), (32)]$ seguido de $(321) = [(32), (21)]$. Durante esses dois caminhos, as G -funções percorrerão o caminho $\gamma_2^{-1}\gamma_1^{-1}$, isto é, os dois laços anteriores no sentido contrário. Da mesma forma, \sqrt{G} -funções vão percorrer $\omega_2^{-1}\omega_1^{-1}$.

Essa sequência é exatamente a mesma que no caso quártico, trocando apenas F -funções por G -funções. Em particular, G -funções percorrem o laço $\gamma = \gamma_1\gamma_2\gamma_1^{-1}\gamma_2^{-1}$ e \sqrt{G} -funções percorrem uma sequência de caminhos abertos $\omega_1\omega_2\omega_1^{-1}\omega_2^{-1}$ que retorna à posição original por construção. Em outras palavras, G e \sqrt{G} -funções percorrem um laço, donde concluímos que H -funções farão o mesmo. Chegamos então ao resultado desejado: enquanto (s_1, s_2, s_3, s_4) sofre a permutação $(14)(23)$ escrita como um comutador de comutadores, qualquer H -função percorre um laço. Consequentemente, não podem existir fórmulas como em (4.17) para a resolução da quártica. Esse resultado, novamente, é válido para qualquer equação de grau $n \geq 4$ e configura nosso terceiro resultado de impossibilidade.

Teorema 4.16. *Usando apenas H -funções, não é possível escrever uma fórmula da solução da equação (4.1) para $n \geq 4$.*

Em particular, podemos adicionar uma coluna à Tabela 4.1 para o novo ingrediente, H -funções:

| ingrediente | H -funções |
|------------------|---|
| níveis de raízes | 2 |
| descartadas por | comutador de comutador de transposições |
| com o caminho | $[[(12), (23)], [(23), (34)]] = (14)(23)$ |
| para grau | $n \geq 4$ |

Tabela 4.2: Extensão da Tabela 4.1 para H -funções e grau $n \geq 4$.

Observação 4.17. Vimos na Seção 3.3 que a solução de uma equação quártica $z^4 + c_3z^3 + c_2z^2 + c_1z + c_0 = 0$, pode ser reduzida à resolução de equações de grau dois e três. Considerando a mudança de variável da Seção 3.3, vemos que como Y é uma H -função, então a solução para z necessariamente envolverá \sqrt{H} -funções, que é algo que não incluímos na Equação (4.17). Isso confirma mais uma vez nosso resultado de impossibilidade.

4.3 A equação quártica

Nota-se que um padrão se tornou evidente. Para $n = 2, 3, 4$, comutadores podem ser usados para rejeitar fórmulas que não possuem composições de raízes suficientes em suas expressões.

No entanto, ainda éramos capazes de obter uma fórmula permitindo mais composições de raízes. Porém, para $n = 5$, isso não mais funciona, o que torna a quántica um caso especial. O objetivo dessa seção é aplicar esses métodos para o caso $n = 5$ e entender o motivo de podermos descartar não apenas 4 níveis de raízes, mas qualquer quantidade de raízes, implicando a inexistência de uma fórmula com radicais para a quántica.

Vamos supor que exista uma fórmula quántica

$$s_i = \Phi_i(c_0, \dots, c_4), \text{ para } i \in \{1, \dots, 5\}, \quad (4.19)$$

com cinco funções Φ_i feitas da combinação de H e \sqrt{H} -funções. Se seguirmos os métodos anteriores, resumidos na Tabela 4.1 e Tabela 4.2, é evidente que

1. todas as H -funções percorrerão um laço a partir da ação de um comutador de comutadores das soluções, como no caso quártico, porém
2. vamos precisar de mais um nível de comutadores para lidar com os termos \sqrt{H} .

Como agora temos cinco soluções para permutar, vamos considerar, por exemplo, as permutações (123) e (345) para construir um primeiro comutador [(123), (345)]. Verificamos que esse comutador é igual ao ciclo (235) e, portanto, permuta três de nossas soluções. Em geral, vale o resultado mais geral para $n = 5$:

$$[(ijk), (klm)] = (jkm). \quad (4.20)$$

Porém dessa vez, ao contrário dos casos anteriores, temos uma notável observação acerca da Equação (4.20): ela prova que qualquer ciclo (jkm) pode ser escrito como comutador de dois outros ciclos, a saber, (ijk) e (klm) . Como essa propriedade é válida para *qualquer* ciclo, é válida em particular para (ijk) e (klm) no membro esquerdo da Equação (4.20). Ou seja, essa fórmula pode ser aplicada a si mesmo sucessivamente, quantas vezes for necessário, nos permitindo escrever (jkm) como um comutador de quantos comutadores quisermos. Como uma quantidade $N \in \mathbb{N}$ de comutadores nos permite descartar N níveis de raízes em uma fórmula, podemos descartar qualquer número de raízes de uma potencial fórmula quántica. O Teorema de Abel-Ruffini segue imediatamente desse fato, porém vamos dar uma explicação mais detalhada.

Suponha que na fórmula quántica, Equação (4.19), usamos uma Φ -função construída com as quatro operações elementares e N níveis de raízes para alguns $N \in \mathbb{N}$. Como sempre, começamos escolhendo uma permutação de soluções, por exemplo (123), que descarta quaisquer F -funções. Agora, usando a Equação (4.20), escrevemos (123) como um comutador, por exemplo:

$$(123) = [(412), (253)]. \quad (4.21)$$

Quando aplicado às soluções (s_1, \dots, s_5) , esse comutador descarta um nível de raízes, as G -funções. Agora seguimos com o processo: escrevemos (412) e (253) que aparecem na Equação

(4.21) em si como comutadores usando a Equação (4.20). Obtemos (123) expresso como dois comutadores:

$$(123) = [[(341), (152)], [(425), (513)]], \quad (4.22)$$

o que remove H -funções. Iterando a Equação (4.20) mais $N - 2$ vezes, escrevemos (123) como uma combinação de N comutadores, que quando aplicada a (s_1, \dots, s_5) , as soluções s_1, s_2, s_3 serão permutadas, porém qualquer expressão com N níveis de raízes ou menos percorrerão um laço. Como uma Φ -função é composta de todos esses ingredientes, Φ_1, Φ_2, Φ_3 voltam às suas posições originais, o que contradiz a equação (4.19). Esse resultado se aplica para equações de qualquer grau $n \geq 5$ escolhendo 5 de suas soluções, como antes. Além disso, como N é arbitrário, concluímos que não há número de raízes que seja suficiente para escrever uma fórmula. Nossa conclusão é o Teorema de Abel-Ruffini (Teorema 3.5): *Não existe fórmula para a solução da equação geral de grau maior ou igual a cinco usando apenas as operações $+$, $-$, \times , \div e $\sqrt{\quad}$.*

Observação 4.18. Pode-se perguntar qual é o motivo da insolubilidade ocorrer primeiro em grau 5 e não 4 ou 6, por exemplo? Tudo se resume à possibilidade de escrever uma permutação de ao menos duas soluções como uma sequência de comutadores. Uma fórmula como a da Equação (4.20) só pode ser iterada infinitamente quando envolve cinco ou mais elementos. Para quatro elementos ou menos, qualquer sequência de comutadores de transposições e/ou ciclos necessariamente vai se degenerar à permutação trivial.

5 Considerações Finais

Este trabalho teve como objetivo apresentar uma demonstração mais acessível do Teorema de Abel-Ruffini, via permutações e laços. Apresentamos um pouco da trajetória e da vida de dois matemáticos Paolo Ruffini e Niels Henrik Abel, os quais foram incompreendidos e, mesmo passando por muitos reveses, contribuíram para a evolução e o sucesso da matemática que aplicamos em nossos dias. Abordamos sobre a importância das equações algébricas e um pouco da história de figuras responsáveis pela descoberta das soluções algébricas das equações cúbicas e quárticas. Além disso, expomos algumas das contribuições do matemático Girolamo Cardano, que esteve envolvido na solução algébrica da equação cúbica, a qual foi o maior avanço matemático desde o tempo dos gregos. Assim, chegamos até Niels Henrik Abel, autor do artigo sobre as equações gerais de graus maiores ou iguais a cinco, e descobridor do teorema, posteriormente intitulado Teorema de Abel-Ruffini, no qual afirma que não existe fórmula para as soluções da equação geral de grau maior ou igual a cinco usando apenas as operações elementares e radicais.

A demonstração do teorema não diz que todas as equações de grau maior ou igual a cinco são insolúveis, apenas diz que não existe uma fórmula válida para a equação geral usando apenas $+$, $-$, \times , \div e $\sqrt{\quad}$. De fato, algumas equações de grau $n \geq 5$ podem ser resolvidas explicitamente. A Teoria de Galois, por outro lado, é perfeitamente capaz de determinar quando uma equação é solúvel ou não. Por outro lado, a prova aqui apresentada pode ser estendida para compreender também funções contínuas de uma variável como exponenciais e trigonométricas na lista de ingredientes. Com efeito, assim como $+$, $-$, \times , \div , essas funções também percorrem um laço quando os coeficientes o fazem. A Teoria de Galois não é capaz de fazer essa extensão, posto que compreende apenas expressões em termos de radicais.

Esperamos que estudantes e professores que não estão familiarizados com a Teoria de Galois possam fazer uso deste trabalho para um melhor entendimento da demonstração do Teorema de Abel-Ruffini e, dessa forma, difundir o conhecimento adquirido.

Referências

- [1] RIGGS, L. J. *Polynomial equations and solvability: A historical perspective*. Tese (Doutorado) — Faculty of California State University, San Bernardino, 1996. Disponível em: <<https://scholarworks.lib.csusb.edu/etd-project/1186>>.
- [2] KATZ, V. J. *History of Mathematics: An Introduction*. New York: Addison-Wesley, 2014.
- [3] KILHIAN, K. Niels abel e as equações de grau maior ou igual a 5. Acessado em 20-05-2024. Disponível em: <<https://www.obaricentrodamente.com/2022/07/niel-abel-e-as-equacoes-de-grau-maior-ou-igual-a-5.html>>.
- [4] O'CONNOR, E. F. R. J. *Mac Tutor history of mathematics: Indexes of Biographies*. [S.l.]. Acessado em 20-05-2024. Disponível em: <<https://mathshistory.st-andrews.ac.uk/Biographies/Frege/>>.
- [5] SCHUVAAB, J. L. *Resolução de equações algébricas até quarto grau: uma abordagem histórica*. Tese (Doutorado) — Programa de Pós-graduação em. Educação para a Ciência e a Matemática, Universidade Estadual de Maringá, 2013.
- [6] REZENDE, J. de C. *Aplicações da raiz n -ésima da unidade*. Tese (Doutorado) — Programa de Pós- Graduação, UNESP-Rio Claro, 2017.
- [7] VILLELA, A. H. e M. L. T. *Polinômios e Equações Algébricas*. 1. ed. Rio de Janeiro: Editora SBM, 2012.
- [8] RAMOND, P. The abel–ruffini theorem: Complex but not complicated. *The American Mathematical Monthly*, Taylor & Francis, v. 129, n. 3, p. 231–245, 2022.
- [9] THAKUR, R. *Niels Henrik Abel by Rajesh Thakur: The Genius Mathematician Who Changed the Course of Numbers*. [S.l.]: Editora Prabhat Prakashan, 2017.
- [10] AYOUB, R. G. Paolo ruffini's contributions to the quintic. *Archive for History of Exact Sciences*, v. 23, p. 253–277, 1980. Acessado em 20-05-2024. Disponível em: <<https://api.semanticscholar.org/CorpusID:123447349>>.
- [11] NUCCIO, S. D. *Paolo Ruffini. Matematico e medico*. [S.l.]: Editora Aracne, 2016.

-
- [12] EVES, H. *An introduction to the history of mathematics*. 6. ed. New York: Saunders College Publishing, 1990.
- [13] EVES, H. *Journey through Genius: The Great Theorems of Mathematics*. 1. ed. New York: John Wiley Sons, Inc., 1991.
- [14] BOYER, U. C. M. C. B. *A history of mathematics*. 2. ed. New York: John Wiley Sons, Inc., 1991.
- [15] CARDANO, G. N. G. *De Vita Propria Liber*. 1. ed. Universidade de Lausanne: Apud Joannem Ravesteinium, 1654.
- [16] SMITH, D. E. *History of Mathematics, vol. II*. 1. ed. New York: Dover Publications, 1958.
- [17] LAGRANGE, J. L. de. *Réflexions sur la résolution algébrique des équations*. [s.n.], 1770. Acessado em 20-05-2024. Disponível em: <https://books.google.com.br/books?id=i_WGPgAACAAJ>.
- [18] LEQUAIN, A. G. e Y. A. E. *Elementos de Álgebra*. 7. ed. Rio de Janeiro: Editora IMPA, 2022.
- [19] GONCALVES, A. *Introdução à Álgebra*. 6. ed. Rio de Janeiro: Editora IMPA, 2006.
- [20] NETO, A. C. M. *Tópicos de Matemática Elementar 6: Polinômios*. Rio de Janeiro: SBM, 2016.
- [21] LIMA, E. L. *Análise Real, vol. 2: Funções de n Variáveis*. 6. ed. Rio de Janeiro: Editora IMPA, 2016.

A Polinômios

Neste apêndice apresentamos alguns resultados pertinentes no contexto deste trabalho. Apresentamos resultados envolvendo polinômios com coeficientes em \mathbb{Q} , \mathbb{R} e \mathbb{C} . Toda vez que uma propriedade for válida para polinômios sobre esses conjuntos, escreveremos apenas \mathbb{K} . Para redigir este apêndice usamos as seguintes referências: [19], [7] e [20].

A.1 Definições e propriedades básicas

Definição A.1. Uma sequência (a_0, a_1, a_2, \dots) de elementos de \mathbb{K} é dita quase toda nula se existir $n \geq -1$ tal que

$$a_{n+1} = a_{n+2} = a_{n+3} = \dots = 0.$$

Em palavras, uma sequência (a_0, a_1, a_2, \dots) é quase toda nula se todos os seus termos, de uma certa posição em diante, forem iguais a zero. Por exemplo, as sequências

$$(0, 0, 0, 0, 0, 0, \dots) \text{ e } (1, 2, 3, \dots, n, 0, 0, 0, \dots)$$

são quase todas nulas; por outro lado, a sequência $(2, 0, 2, 0, 2, \dots)$, com 2's e 0's se alternando indefinidamente, não é quase toda nula.

Definição A.2. Um polinômio sobre (ou com coeficientes em) \mathbb{K} é uma soma $f = f(X)$ do tipo

$$f(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + \dots = \sum_{k \geq 0} a_k X^k,$$

onde (a_0, a_1, a_2, \dots) é uma sequência quase toda nula de elementos de \mathbb{K} e X é um símbolo qualquer. Convencionamos $X^0 = 1$ e $X^1 = X$ no somatório acima.

Observação A.3. Na Definição A.2, X é um símbolo qualquer.

Assumiremos ainda que, os polinômios $f(X) = \sum_{k \geq 0} a_k X^k$ e $g(X) = \sum_{k \geq 0} b_k X^k$ sobre \mathbb{K} são **iguais** se, e só se, $a_k = b_k$, para todo $k \geq 0$.

Dado um polinômio $f(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + \dots$ sobre \mathbb{K} , adotamos as seguintes convenções:

1. Os elementos $a_i \in \mathbb{K}$ são chamados de **coeficientes** de f . As parcelas $a_i X^i$ são chamadas de termos e os termos $a_i X^i$, tais que $a_i \neq 0$ são chamados **monômios** de grau i do polinômio f .
2. Quando $a_i = 0$ omitiremos, sempre que for conveniente, o termo $a_i X^i$. Em particular, como a sequência (a_0, a_1, a_2, \dots) é quase toda nula, existe um inteiro $n \geq 0$ para o qual podemos escrever

$$f(X) = \sum_{k=0}^n a_k X^k.$$

3. Quando $a_i = \pm 1$, escreveremos $\pm X^i$ em vez de $(\pm 1)X^i$, para o termo correspondente de f .
4. O polinômio $0 = 0 + 0X + 0X^2 + \dots$ é denominado **polinômio identicamente nulo** sobre \mathbb{K} . Sempre que não houver confusão com $0 \in \mathbb{K}$, denotaremos o polinômio identicamente nulo sobre \mathbb{K} por 0 .
5. Mais geralmente, dado $\alpha \in \mathbb{K}$, denotamos o polinômio $\alpha + 0X + 0X^2 + \dots$ simplesmente por α e o denominamos o **polinômio constante** α ; em cada caso, o contexto deixará claro se estamos nos referindo ao polinômio constante e igual a α ou ao elemento $\alpha \in \mathbb{K}$.

Denotamos por $\mathbb{K}[X]$ o conjunto de todos os polinômios sobre \mathbb{K} . A partir do Item 5 acima, convencionamos que $\mathbb{K} \subset \mathbb{K}[X]$. Por outro lado, as inclusões $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ fornecem as inclusões $\mathbb{Q}[X] \subset \mathbb{R}[X] \subset \mathbb{C}[X]$.

Exemplo A.4. Se $f(X) = 1 - 4X^2 + \sqrt{11}X^4 - \frac{4}{5}X^6$, então $f \notin \mathbb{Q}[X]$ (uma vez que $\sqrt{11} \notin \mathbb{Q}$) mas $f \in \mathbb{R}[X]$. Já a expressão $g = X + X^3 + X^5 + X^7 + \dots$ não é um polinômio, uma vez que a sequência $(0, 1, 0, 1, \dots)$ não é quase toda nula.

A seguir vamos definir sobre $\mathbb{K}[X]$ operações

$$\oplus: \mathbb{K}[X] \times \mathbb{K}[X] \rightarrow \mathbb{K}[X] \quad \text{e} \quad \odot: \mathbb{K}[X] \times \mathbb{K}[X] \rightarrow \mathbb{K}[X]$$

denominadas, respectivamente, de **adição** e **multiplicação**. Para isso precisamos inicialmente do seguinte resultado auxiliar.

Lema A.5. Se $(a_k)_{k \geq 0}$ e $(b_k)_{k \geq 0}$, são sequências quase todas nulas de elementos de \mathbb{K} , então também são quase todas nulas as sequências $(a_k \pm b_k)_{k \geq 0}$ e $(c_k)_{k \geq 0}$, onde

$$c_k = \sum_{\substack{i+j=k \\ i,j \geq 0}} a_i b_j = \sum_{i=0}^k a_i b_{k-i}.$$

Demonstração. Mostremos primeiramente que a sequência $(a_k \pm b_k)_{k \geq 0}$ é quase toda nula. Sejam $m, n \in \mathbb{Z}_+$, o conjunto dos inteiros positivos, tais que $a_i = 0$ para $i > n$ e $b_j = 0$ para

$j > m$. Sem perda de generalidade, suponhamos $m \geq n$. Se $k > m$, então $a_k = b_k = 0$ e consequentemente $a_k \pm b_k = 0$.

Agora mostremos que a sequência $(c_k)_{k \geq 0}$ é quase toda nula. Sejam $m, n \in \mathbb{Z}_+$ tais que $a_i = 0$ para $i > n$ e $b_j = 0$ para $j > m$. Se $k > m + n$ e $i + j = k$, com $i, j \geq 0$, então $i > n$ ou $j > m$, do contrário, teríamos $k = i + j \leq n + m$, o que não é o caso. Mas, como $i > n \Rightarrow a_i = 0$ e $j > m \Rightarrow b_j = 0$, em qualquer caso temos $a_i b_j = 0$ e assim,

$$c_k = \sum_{\substack{i+j=k \\ i,j \geq 0}} a_i b_j = 0,$$

como queríamos demonstrar. □

A partir do Lema A.5 podemos apresentar a seguir as definições das operações de adição e multiplicação de polinômios.

Definição A.6. Dados em $\mathbb{K}[X]$ os polinômios

$$f(X) = \sum_{k \geq 0} a_k X^k \text{ e } g(X) = \sum_{k \geq 0} b_k X^k,$$

a **soma** e o **produto** de f e g , denotados respectivamente por $f \oplus g$ e $f \odot g$, são os polinômios

$$(f \oplus g)(X) = \sum_{k \geq 0} (a_k + b_k) X^k$$

e

$$(f \odot g)(X) = \sum_{k \geq 0} c_k X^k,$$

onde $c_k = \sum_{\substack{i+j=k \\ i,j \geq 0}} a_i b_j$.

Observação A.7. A fórmula para o coeficiente c_k de $f \odot g$ é necessária a fim de que valham a distributividade da operação \odot em relação à operação \oplus , assim como a regra de potenciação $X^m \odot X^n = X^{m+n}$. De fato, se tais propriedade forem válidas, então, calculando o produto

$$(a_0 + a_1 X + a_2 X^2 + \dots) \odot (b_0 + b_1 X + b_2 X^2 + \dots)$$

distributivamente obtemos

$$a_0 b_0 = \sum_{\substack{i+j=0 \\ i,j \geq 0}} a_i b_j$$

para coeficiente de X^0 ,

$$a_0 b_1 + a_1 b_0 = \sum_{\substack{i+j=1 \\ i,j \geq 0}} a_i b_j$$

para coeficiente de X ,

$$a_0 b_2 + a_1 b_1 + a_2 b_0 = \sum_{\substack{i+j=2 \\ i,j \geq 0}} a_i b_j$$

para coeficiente de X^2 , e assim por diante.

Proposição A.8. *Sejam f, g e h polinômios em $\mathbb{K}[X]$. Então valem as seguintes propriedades:*

1. **Comutatividade:** $f \oplus g = g \oplus f$ e $f \odot g = g \odot f$;
2. **Associatividade:** $(f \oplus g) \oplus h = f \oplus (g \oplus h)$ e $(f \odot g) \odot h = f \odot (g \odot h)$;
3. **Distributividade:** $f \odot (g \oplus h) = f \odot g \oplus f \odot h$.

Demonstração. Sejam $f(X) = \sum_{k=0}^n a_k X^k$, $g(X) = \sum_{k=0}^m b_k X^k$ e $h(X) = \sum_{k=0}^l c_k X^k$, polinômios em $\mathbb{K}[X]$.

1.1. Comutatividade da adição:

$$(f \oplus g)(X) = \sum_{k \geq 0} (a_k + b_k) X^k = \sum_{k \geq 0} (b_k + a_k) X^k = (g \oplus f)(X)$$

pois em \mathbb{K} , temos $a_i + b_j = b_j + a_i$, para quaisquer i e j .

1.2. Comutatividade da multiplicação:

$$(f \odot g)(X) = \sum_{k=0}^{n+m} \left(\sum_{\substack{i+j=k \\ i,j \geq 0}} a_i b_j \right) X^k = \sum_{k=0}^{n+m} \left(\sum_{\substack{i+j=k \\ i,j \geq 0}} b_i a_j \right) X^k = (g \odot f)(X),$$

pois em \mathbb{K} , temos $a_i b_j = b_j a_i$, para quaisquer i e j .

2.1. Associatividade da adição: Podemos supor que $n = m = l$, após reescrever $f(X)$, $g(X)$ e $h(X)$ com as mesmas potências de X :

$$\begin{aligned} ((f \oplus g) \oplus h)(X) &\stackrel{(1)}{=} \sum_{k=0}^n (a_k + b_k) X^k \oplus \sum_{k=0}^n c_k X^k \\ &\stackrel{(2)}{=} \sum_{k=0}^n ((a_k + b_k) + c_k) X^k \\ &\stackrel{(3)}{=} \sum_{k=0}^n (a_k + (b_k + c_k)) X^k \\ &\stackrel{(4)}{=} \sum_{k=0}^n a_k X^k \oplus \sum_{k=0}^n (b_k + c_k) X^k \\ &\stackrel{(5)}{=} (f \oplus (g \oplus h))(X), \end{aligned}$$

onde em (1) e (2) usamos a definição da adição em $\mathbb{K}[X]$; em (3), a associatividade da adição em \mathbb{K} ; e, em (4) e (5), novamente, a definição de adição em $\mathbb{K}[X]$.

2.2. Associatividade da multiplicação: Podemos supor que $n = m = l$, após reescrever

$f(X)$, $g(X)$ e $h(X)$ com as mesmas potências de X :

$$\begin{aligned}
 ((f \odot g) \odot h)(X) &\stackrel{(1)}{=} \sum_{k=0}^{n+m} \left(\sum_{\substack{h+i=k \\ h,i \geq 0}} a_h b_i \right) X^k \odot \sum_{k=0}^l c_k X^k \\
 &\stackrel{(2)}{=} \sum_{k=0}^{n+m+l} \left[\sum_{s=0}^k \left(\sum_{\substack{h+i=s \\ h,i \geq 0}} a_h b_i \right) c_{k-s} \right] X^k \\
 &\stackrel{(3)}{=} \sum_{k=0}^{n+m+l} \left(\sum_{\substack{i+j+h=k \\ h,i,j \geq 0}} a_h b_i c_j \right) X^k \\
 &\stackrel{(4)}{=} \sum_{k=0}^{n+m+l} \left[\sum_{s=0}^k \left(\sum_{\substack{i+j=s \\ i,j \geq 0}} b_i c_j \right) a_{k-s} \right] X^k \\
 &\stackrel{(5)}{=} \sum_{k=0}^{n+m} \left(\sum_{\substack{i+j=k \\ i,j \geq 0}} b_i c_j \right) X^k \odot \sum_{k=0}^l a_k X^k \\
 &\stackrel{(6)}{=} ((g \odot h) \odot f)(X) \\
 &\stackrel{(7)}{=} ((f \odot g) \odot h)(X),
 \end{aligned}$$

onde em (1) e (2) usamos a definição da multiplicação em $\mathbb{K}[X]$; em (3) e (4), a distributividade em \mathbb{K} ; em (5) e (6), novamente, a definição da multiplicação em $\mathbb{K}[X]$ e em (7), a comutatividade da multiplicação em $\mathbb{K}[X]$.

3. Distributividade: Podemos supor $l = m$, após reescrever $g(X)$ e $h(X)$ com as mesmas potências de X .

$$\begin{aligned}
 ((f \odot (g \oplus h))(X) &\stackrel{(1)}{=} \left(\sum_{k=0}^n a_k X^k \right) \odot \left(\sum_{k=0}^m (b_k + c_k) X^k \right) \\
 &\stackrel{(2)}{=} \sum_{k=0}^{n+m} \left(\sum_{\substack{i+j=k \\ i,j \geq 0}} a_i (b_j + c_j) \right) X^k \\
 &\stackrel{(3)}{=} \sum_{k=0}^{n+m} \left(\sum_{\substack{i+j=k \\ i,j \geq 0}} a_i b_j + a_i c_j \right) X^k \\
 &\stackrel{(4)}{=} \sum_{k=0}^{n+m} \left(\sum_{\substack{i+j=k \\ i,j \geq 0}} a_i b_j \right) X^k \oplus \sum_{k=0}^{n+m} \left(\sum_{\substack{i+j=k \\ i,j \geq 0}} a_i c_j \right) X^k \\
 &\stackrel{(5)}{=} ((f \odot g \oplus f \odot h))(X),
 \end{aligned}$$

onde em (1) usamos a definição da adição em $\mathbb{K}[X]$; em (2), a definição da multiplicação em $\mathbb{K}[X]$; em (3), a distributividade em \mathbb{K} ; em (4), a definição da adição em $\mathbb{K}[X]$; e, em (5), novamente, a definição da multiplicação em $\mathbb{K}[X]$. \square

Exemplo A.9. Considere os polinômios de coeficientes reais $f(X) = 4 - 2X + \sqrt{5}X^2$ e $g(X) = 5X - 3X^2$. Então

$$(f \oplus g)(X) = 4 + 3X + (\sqrt{5} - 3)X^2$$

e

$$\begin{aligned} (f \odot g)(X) &= (4 - 2X + \sqrt{5}X^2) \odot (5X - 3X^2) \\ &= [4 \odot (5X - 3X^2)] \oplus [-2X \odot (5X - 3X^2)] \oplus [\sqrt{5}X^2 \odot (5X - 3X^2)] \\ &= (20X - 12X^2) \oplus (-10X^2 + 12X^3) \oplus (5\sqrt{5}X^3 - 3\sqrt{5}X^4) \\ &= 20X - 22X^2 + (12 + 5\sqrt{5})X^3 - 3\sqrt{5}X^4. \end{aligned}$$

Observação A.10. Denotaremos, a partir de agora, as operações de adição e multiplicação de polinômios simplesmente por $+$ e \cdot . Assim, sempre que adicionarmos dois polinômios, os sinais $+$ representarão duas operações diferentes: a adição de elementos de \mathbb{K} , efetuada sobre os coeficientes dos polinômios em questão, e a adição de elementos de $\mathbb{K}[X]$. O contexto sempre deixará claro a qual operação o sinal $+$ se refere. Comentário análogo é válido para o sinal \cdot de multiplicação.

Observação A.11. Todas as definições acima podem ser estendidas para incluir polinômios de coeficientes inteiros. De agora em diante, sempre que necessário, denotaremos o conjunto de tais polinômios por $\mathbb{Z}[X]$.

Seja 0 o polinômio identicamente nulo. Então, $f + 0 = 0 + f = f$ para todo $f \in \mathbb{K}[X]$, o que significa que o polinômio identicamente nulo é o **elemento neutro** da adição de polinômios. Além disso, dado $f \in \mathbb{K}[X]$, existe um único polinômio $g \in \mathbb{K}[X]$ tal que $f + g = g + f = 0$. De fato, sendo $f(X) = a_0 + a_1X + a_2X^2 + \dots$, é imediato que

$$g(X) = -a_0 - a_1X - a_2X^2 - \dots$$

é esse único polinômio. De agora em diante, denotaremos esse polinômio por $-f$. Desse modo,

$$(-f)(X) = -a_0 - a_1X - a_2X^2 - \dots$$

e, para $f, g \in \mathbb{K}[X]$, é possível definir a diferença $f - g$ entre f e g por $f - g = f + (-g)$.

Se $\alpha \in \mathbb{K}$ e $g(X) = b_0 + b_1X + b_2X^2 + \dots \in \mathbb{K}[X]$, é imediata a verificação de que

$$\alpha \cdot g = \alpha b_0 + \alpha b_1X + \alpha b_2X^2 + \dots;$$

em particular, temos $1 \cdot g = g$ para todo $g \in \mathbb{K}[X]$, de maneira que o polinômio constante 1 é o elemento neutro da multiplicação de polinômios.

De agora em diante, para denotar o produto $f \cdot g$, de $f, g \in \mathbb{K}[X]$, escreveremos simplesmente fg , sempre que não houver perigo de confusão. Em particular, se $\alpha \in \mathbb{K}$, escreveremos αf para denotar o produto de α e f , onde α é um polinômio constante.

Definição A.12. Se $f(X) = a_0 + a_1X + \dots + a_nX^n \in \mathbb{K}[X] \setminus \{0\}$, com $a_n \neq 0$, dizemos que o inteiro não negativo n é o **grau** de f , e denotamos $\partial f = n$ (lê-se “o grau de f é igual a n ”).

Note que o grau não está definido para o polinômio identicamente nulo; por outro lado, $\partial f = 0$ para todo polinômio constante $f(X) = \alpha$, com $\alpha \in \mathbb{K} \setminus \{0\}$. De agora em diante, sempre que nos referirmos a $f \in \mathbb{K}[X] \setminus \{0\}$ escrevendo

$$f(X) = a_n X^n + \cdots + a_1 X + a_0$$

suporemos, salvo menção em contrário, que $a_n \neq 0$. Nesse caso, a_n será denominado o **coeficiente líder** de f . Finalmente, f será dito **mônico** quando tiver coeficiente líder 1.

A proposição a seguir estabelece duas propriedades muito importantes da noção de grau de polinômios sendo o item (b) conhecido como **propriedade multiplicativa do grau**.

Proposição A.13. Para $f, g \in \mathbb{K}[X] \setminus \{0\}$, temos:

$$(a) \quad \partial(f + g) \leq \max\{\partial f, \partial g\} \text{ se } f + g \neq 0.$$

$$(b) \quad fg \neq 0 \text{ e } \partial(fg) = \partial f + \partial g.$$

Demonstração. Sejam $\partial f = n$ e $\partial g = m$, com $f(X) = a_0 + a_1 X + \cdots + a_n X^n$ e $g(X) = b_0 + b_1 X + \cdots + b_m X^m$.

(a) Se $m \neq n$, podemos supor, sem perda de generalidade, que $m > n$. Então

$$(f + g)(X) = (a_0 + b_0) + \cdots + (a_n + b_n)X^n + b_{n+1}X^{n+1} + \cdots + b_m X^m,$$

de forma que $\partial(f + g) = m = \max\{\partial f, \partial g\}$. Se $m = n$ mas $f + g \neq 0$, então

$$(f + g)(X) = (a_0 + b_0) + \cdots + (a_n + b_n)X^n$$

e há duas possibilidades: $a_n + b_n = 0$ ou $a_n + b_n \neq 0$. No primeiro caso, $\partial(f + g) < n = \max\{\partial f, \partial g\}$. No segundo, $\partial(f + g) = n = \max\{\partial f, \partial g\}$. Em qualquer caso, ainda teremos $\partial(f + g) \leq \max\{\partial f, \partial g\}$.

(b) Seja $fg = c_0 + c_1 X + c_2 X^2 + \cdots$. Se $k > m + n$, vimos, na prova do Lema A.5, que $c_k = 0$. Portanto, se mostrarmos que $c_{m+n} \neq 0$ seguirá que $fg \neq 0$ e $\partial(fg) = m + n = \partial f + \partial g$. Mas, como $a_i = 0$ para $i > n$ e $b_j = 0$ para $j > m$, é imediato que

$$c_{m+n} = \sum_{\substack{i+j=m+n \\ i,j \geq 0}} a_i b_j = a_n b_m \neq 0.$$

□

A.2 Divisão euclidiana

Nesta seção apresentamos o conceito de divisibilidade em $\mathbb{K}[X]$ e mostramos que é possível fazer de modo único uma divisão com resto controlado em $\mathbb{K}[X]$.

Definição A.14. Sejam $f, g \in \mathbb{K}[X]$. Quando existe $h \in \mathbb{K}[X]$ tal que $f = gh$, dizemos que f é múltiplo de g . Nesse caso, se $g \neq 0$, dizemos que g divide f .

Exemplo A.15. Tanto $X^4 - 2X^2 + 2$ como $X^4 + 2X^2 + 2$ dividem $X^8 + 4$ em $\mathbb{Z}[X]$, pois $X^8 + 4 = (2 - 2X^2 + X^4)(2 + 2X^2 + X^4)$.

O seguinte resultado é uma consequência da Proposição A.13 item (b) (propriedade multiplicativa do grau) em $\mathbb{K}[X]$.

Proposição A.16. Dados $f, g \in \mathbb{K}[X] \setminus \{0\}$, se g divide f , então $\partial g \leq \partial f$.

Demonstração. Como g divide f e ambos são não nulos, então existe $h \in \mathbb{K} \setminus \{0\}$ tal que $f = gh$. Pelo item (b) da Proposição A.13, temos

$$\partial f = \partial gh = \partial g + \partial h \geq \partial g.$$

□

Apresentamos, na proposição seguinte, a divisão em $\mathbb{K}[X]$, conhecida como **divisão euclidiana**.

Proposição A.17. Se $f, g \in \mathbb{K}[X]$, com $g \neq 0$, então existem únicos $q, r \in \mathbb{K}[X]$ tais que

$$f = gq + r, \text{ com } r = 0 \text{ ou } 0 \leq \partial r < \partial g.$$

Demonstração. Seja $g(X) = b_0 + b_1X + \dots + b_mX^m$, onde b_m tem inverso $b_m^{-1} \in \mathbb{K}$.

Existência: Se $f(X) = 0$, então tome $q(X) = r(X) = 0$.

Suponhamos que $f(X) \neq 0$. Seja $n = \partial f$ e escreva $f(X) = a_0 + a_1X + \dots + a_nX^n$, com $a_n \neq 0$.

Se $n < m$, então tome $q(X) = 0$ e $r(X) = f(X)$.

Podemos supor $n \geq m$. A demonstração é por indução sobre $n = \partial f$. Se $n = 0$, então $0 = n \geq m = \partial g$, logo $m = 0$, $f(X) = a_0 \neq 0$, $g(X) = b_0$, com $b_0^{-1} \in \mathbb{K}$. Assim, $f(X) = a_0b_0^{-1}g$, com $q(X) = a_0b_0^{-1}$ e $r(X) = 0$.

Suponhamos o resultado válido para polinômios com grau menor do que $n = \partial f$. Vamos mostrar que vale para f .

Seja $f_1(X)$ o polinômio definido por $f_1(X) = f(X) - a_nb_m^{-1}X^{n-m}g(X)$. O polinômio $a_nb_m^{-1}X^{n-m}g(X)$ tem grau n e coeficiente líder a_n . Logo, $\partial f_1 < \partial f$. Por hipótese de indução, existem $q_1, r_1 \in \mathbb{K}[X]$ tais que

$$f_1 = q_1g + r_1,$$

onde $r_1 = 0$ ou $\partial r_1 < \partial g$. Logo,

$$\begin{aligned} f(X) &= f_1(X) + a_nb_m^{-1}X^{n-m}g(X) \\ &\stackrel{(1)}{=} (q_1(X)g(X) + r_1(X)) + a_nb_m^{-1}X^{n-m}g(X) \\ &\stackrel{(2)}{=} (q_1(X) + a_nb_m^{-1}X^{n-m})g(X) + r_1(X). \end{aligned}$$

onde, em (1), substituímos a expressão de $f_1(X)$ e, em (2), usamos a comutatividade da adição e a distributividade em $\mathbb{K}[X]$.

Tomamos $q(X) = q_1(X) + a_n b_m^{-1} x^{m-n}$ e $r(X) = r_1(X)$.

Unicidade: Sejam q_1, r_1, q_2, r_2 tais que

$$f(X) = q_1(X)g(X) + r_1(X) \stackrel{(3)}{=} q_2(X)g(X) + r_2(X), \text{ onde}$$

$$(4) \begin{cases} r_1(X) = 0 & \text{ou } \partial r_1 < \partial g \text{ e} \\ r_2(X) = 0 & \text{ou } \partial r_2 < \partial g. \end{cases}$$

De (3), segue que $(q_1(X) - q_2(X))g(X) = r_2(X) - r_1(X)$.

Se $q_1 \neq q_2$, então $q_1(X) - q_2(X) \neq 0$, assim, $r_2(X) - r_1(X) \neq 0$ e, da Proposição A.16 e do item (a) da Proposição A.13, obtemos

$$\partial g \leq \partial(r_2 - r_1) \leq \max\{\partial r_1, \partial r_2\} \stackrel{(4)}{<} \partial g,$$

uma contradição. Portanto, $q_1 = q_2$ e, conseqüentemente, $r_1 = r_2$. □

Definição A.18. Sejam f, g, q e r como na Proposição A.17. Chamamos f de **dividendo**, g de **divisor**, q de **quociente** e r de **resto**. Além disso, se $r = 0$, dizemos que f é divisível por g ou, o que é o mesmo, que g divide f , e denotamos por $g \mid f$.

Observação A.19. Na Proposição A.16 e Proposição A.17, se considerarmos que g tem coeficiente líder invertível então a divisão euclidiana é válida em $\mathbb{A}[X]$, onde \mathbb{A} é um anel. Lembramos que no anel \mathbb{Z} os únicos elementos que têm inverso são 1 e -1 . Em \mathbb{K} , todo elemento não nulo tem inverso.

A.3 Raízes de polinômios

Até este ponto, em nosso trabalho, temos considerado polinômios como expressões formais com as quais aprendemos a operar sem, no entanto, atribuir a **indeterminada** X um significado aritmético.

A partir desta seção, passamos a considerar a indeterminada X de um ponto de vista aritmético, apresentando o conceito de raiz de um polinômio e de função polinomial associada a um polinômio.

Definição A.20. Para $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{K}[X]$, a **função polinomial** associada a f é a função $\tilde{f}: \mathbb{K} \rightarrow \mathbb{K}$ dada, para $x \in \mathbb{K}$ por

$$\tilde{f}(x) = a_n x^n + \cdots + a_1 x + a_0.$$

Quando $f(X) = c$, note que a função polinomial associada \tilde{f} será a função constante $\tilde{f} = c$, para todo $x \in \mathbb{K}$, justificando o nome *constante* atribuído anteriormente a um polinômio de grau 0.

Definição A.21. Seja $f \in \mathbb{K}[X]$ um polinômio, com função polinomial associada $\tilde{f}: \mathbb{K} \rightarrow \mathbb{K}$. Um elemento $\alpha \in \mathbb{K}$ é uma raiz de f se $\tilde{f}(\alpha) = 0$.

Exemplo A.22. Seja $f(X) = X - 3 \in \mathbb{C}[X]$. É fácil verificar que $x = 3$ é a única raiz de f em \mathbb{C} . De fato, a função polinomial associada a f é

$$\begin{aligned}\tilde{f}: \mathbb{C} &\rightarrow \mathbb{C} \\ x &\mapsto x - 3\end{aligned}$$

logo, $\tilde{f}(x) = 0$ se, e somente se, $x = 3$.

O item (a) da Proposição A.23 é conhecida como o **teste da raiz**.

Proposição A.23. Se $f \in \mathbb{K}[X] \setminus \{0\}$ e $\alpha \in \mathbb{K}$, então:

- (a) α é raiz de f se, e só se, $(X - \alpha) \mid f(X)$ em $\mathbb{K}[X]$.
- (b) Se α for raiz de f , então existe um maior inteiro positivo m tal que $(X - \alpha)^m$ divide f . Ademais, sendo $f(X) = (X - \alpha)^m q(X)$, com $q \in \mathbb{K}[X]$, tem-se $\tilde{q}(\alpha) \neq 0$, onde $\tilde{q}: \mathbb{K} \rightarrow \mathbb{K}$ é a função polinomial associada a q .
- (c) Se $\alpha_1, \dots, \alpha_k$ forem raízes duas a duas distintas de f , então o polinômio $(X - \alpha_1) \cdots (X - \alpha_k)$ divide $f(X)$ em $\mathbb{K}[X]$.

Demonstração. (a) Segue da divisão euclidiana (Proposição A.17) a existência de polinômios $q, r \in \mathbb{K}[X]$ tais que

$$f(X) = (X - \alpha)q(X) + r(X),$$

com $r = 0$ ou $0 \leq \partial r < \partial(X - \alpha) = 1$. Portanto, $r(X) = c$, um polinômio constante. Por outro lado, sendo \tilde{f} e \tilde{q} as funções polinomiais respectivamente associadas a f e q , segue da igualdade acima que

$$\tilde{f}(\alpha) = (\alpha - \alpha)\tilde{q}(\alpha) + c = c,$$

ou seja, $f(X) = (X - \alpha)q(X) + \tilde{f}(\alpha)$. Assim,

$$\alpha \text{ é raiz de } f \Leftrightarrow \tilde{f}(\alpha) = 0 \Leftrightarrow f(X) = (X - \alpha)q(X).$$

- (b) Se $m > \partial f$, então $(X - \alpha)^m \nmid f(X)$, uma vez que $\partial(X - \alpha)^m = m > \partial f$. Daí e do item (a), existe um maior inteiro positivo m tal que $(X - \alpha)^m \mid f(X)$, digamos $f(X) = (X - \alpha)^m q(X)$. Passando para funções polinomiais, obtemos, a partir daí, a igualdade

$$\tilde{f}(x) = (x - \alpha)^m \tilde{q}(x), \forall x \in \mathbb{K};$$

se $\tilde{q}(\alpha) = 0$, seguiria de (a) que $q(X) = (X - \alpha)q_1(X)$, para algum polinômio $q_1 \in \mathbb{K}[X]$. Mas aí, teríamos

$$f(X) = (X - \alpha)^{m+1} q_1(X),$$

contrariando a maximalidade de m .

(c) Façamos a prova deste item para o caso $k = 2$, isto é, o caso em que f possui duas raízes distintas (a prova do caso geral é análoga). Como α_1 é raiz de f , pelo item (a) existe um polinômio $g \in \mathbb{K}[X]$ tal que $f(X) = (X - \alpha_1)g(X)$. Seja \tilde{g} a função polinomial associada ao polinômio g . Como $\alpha_1 \neq \alpha_2$ e α_2 também é raiz de f , segue da última igualdade que

$$0 = \tilde{f}(\alpha_2) = (\alpha_2 - \alpha_1)\tilde{g}(\alpha_2),$$

e α_2 é raiz de g . Daí, novamente pelo item (a), existe um polinômio $h \in \mathbb{K}[X]$ tal que $g(X) = (X - \alpha_2)h(X)$ e, assim,

$$f(X) = (X - \alpha_1)(X - \alpha_2)h(X).$$

□

Se $f(X) = (X - \alpha)^m q(X)$, com $\tilde{q}(\alpha) \neq 0$ como na Proposição A.23, então chamamos m de a **multiplicidade** de α como raiz de f . Em particular, se $m = 1$, α é uma raiz **simples** de f , já se $m > 1$, α é uma raiz **múltipla** de f .

Exemplo A.24. Sendo $f(X) = X^3 + 3X^2 + 11X + 5$ um polinômio de coeficientes reais, temos que 1 é raiz dupla e -5 é raiz simples de f , uma vez que $f(X) = (X - 1)^2[X - (-5)]$.

Uma consequência importante do teste da raiz e que está explicitada no corolário seguinte é que o número de raízes de um polinômio não identicamente nulo não pode exceder seu grau. Note que consideramos a multiplicidade das raízes.

Corolário A.25. *Se $f \in \mathbb{K}[X] \setminus \{0\}$, então f possui no máximo ∂f raízes em \mathbb{K} , contadas de acordo com suas multiplicidades.*

Demonstração. Façamos indução sobre o grau de f . Se $\partial f = 0$, então existe $c \in \mathbb{K} \setminus \{0\}$ tal que $f(X) = c$. Daí, a função polinomial associada \tilde{f} é a função constante $x \mapsto c$, e segue que o número de raízes de f é 0, igual a seu grau.

Seja, agora, f um polinômio de grau positivo e suponha a afirmação do enunciado válida para todos os polinômios não nulos de graus menores do que ∂f . Se f não tiver raízes em \mathbb{K} , nada há nada a fazer. Senão, seja $\alpha \in \mathbb{K}$ uma raiz de f e (de acordo com a Proposição A.23) m o maior natural tal que $f(X) = (X - \alpha)^m q(X)$, para algum polinômio $q \in \mathbb{K}[X]$. Como

$$\partial q = \partial f - m < \partial f,$$

segue da hipótese de indução que q tem no máximo ∂q raízes em \mathbb{K} , contadas de acordo com suas multiplicidades. Agora, se $\beta \neq \alpha$ é raiz de f , temos

$$0 = \tilde{f}(\beta) = (\beta - \alpha)^m \tilde{q}(\beta)$$

e, daí, β é raiz de q . Portanto, o número máximo de raízes de f é igual a m (a multiplicidade de α) mais o número de raízes de q , e segue, por hipótese de indução, que f possui no máximo

$$m + \partial q = \partial f$$

raízes em \mathbb{K} .

□

O Corolário A.25 pode ser usado em uma das formas a seguir.

Corolário A.26. Se $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{K}[X]$ admite pelo menos $n + 1$ raízes distintas em \mathbb{K} , então f é identicamente nulo, ou seja, $a_n = \cdots = a_0 = 0$.

Demonstração. Se $f \in \mathbb{K}[X] \setminus \{0\}$, então, pelo Corolário A.25, f teria no máximo n raízes em \mathbb{K} . □

Corolário A.27. Sejam $f(X) = a_n X^n + \cdots + a_1 X + a_0$ e $g(X) = b_m X^m + \cdots + b_1 X + b_0$ polinômios sobre \mathbb{K} , com $m \geq n$. Se $\tilde{f}(x) = \tilde{g}(x)$ para ao menos $m + 1$ valores distintos $x \in \mathbb{K}$, então $f = g$, ou seja, $m = n$ e $a_i = b_i$, para $0 \leq i \leq n$.

Demonstração. Basta aplicar o Corolário A.26 ao polinômio $f - g$, notando que a função polinomial associada a tal polinômio é $\tilde{f} - \tilde{g}$. □

Considere a aplicação

$$\begin{aligned} \mathbb{K}[X] &\rightarrow \Phi \\ f &\mapsto \tilde{f} \end{aligned} \tag{A.1}$$

onde Φ é o conjunto das funções de \mathbb{K} em \mathbb{K} . O Corolário A.27 garante que a aplicação (A.1) é injetiva, ou seja, se $f, g \in \mathbb{K}[X]$ e $\tilde{f}, \tilde{g} \in \Phi$, então $\tilde{f} = \tilde{g} \Rightarrow f = g$.

Assim, quando quisermos nos referir quer seja a um polinômio sobre \mathbb{K} , quer seja à função polinomial associada a esse polinômio, escreveremos apenas f . De modo particular, ao escrevermos $f(X)$, estaremos fazendo referência ao polinômio f ; ao escrevermos $f(x)$, estaremos fazendo referência ao elemento de \mathbb{K} , imagem de $x \in \mathbb{K}$ pela função polinomial associada ao polinômio f . Em qualquer caso, o contexto deixará claro a que estamos nos referindo.

Observação A.28. O Corolário A.27 garante que os coeficientes de um polinômio $f \in \mathbb{K}[X]$ são determinados pelos valores $f(x)$, com $x \in \mathbb{K}$.

A.4 O Teorema Fundamental da Álgebra

Como caso particular do Corolário A.25, todo polinômio de coeficientes complexos e grau n possui no máximo n raízes complexas. Por outro lado, o polinômio $f(X) = X^2 - 2 \in \mathbb{Q}[X]$ tem coeficientes racionais mas não admite raízes racionais; da mesma forma, o polinômio $g(X) = X^2 + 1 \in \mathbb{R}[X]$ tem coeficientes reais mas não admite raízes reais. Em ambos os casos, o fato de tais polinômios não admitirem raízes em \mathbb{Q} ou \mathbb{R} se deve a *deficiências* de tais conjuntos numéricos, no sentido de que, neles, não é possível realizarmos certas extrações de raízes.

Em sua tese de doutoramento, em 1799, o matemático alemão Carl F. Gauss mostrou, contrariamente aos casos examinados acima, que todo polinômio sobre \mathbb{C} admite raízes também em \mathbb{C} . Esse é o conteúdo do teorema a seguir, conhecido na literatura como o **Teorema Fundamental da Álgebra**. A demonstração que apresentamos é devida a Jean-Baptiste le Rond d'Alembert, matemático francês do século XVIII, na qual é necessária dois lemas que daremos a seguir.

Lema A.29. Dado um polinômio $f \in \mathbb{C}[X] \setminus \mathbb{C}$, existe $z_0 \in \mathbb{C}$ tal que

$$|f(z_0)| \leq |f(z)|, \forall z \in \mathbb{C}.$$

Demonstração. Basta provar o resultado para polinômios mônicos. Por comodidade de notação, escrevamos $f(z) = a_n z^n + \dots + a_1 z + a_0$ para denotar a função polinomial associada a f . Pelas desigualdades triangulares [7, p. 15-16], temos para todo $z \in \mathbb{C}$,

$$|f(z)| = |z|^n \left| 1 + \frac{a_{n-1}}{z} + \frac{a_{n-2}}{z^2} + \dots + \frac{a_0}{z^n} \right| \geq |z|^n \left(1 - \frac{|a_{n-1}|}{|z|} - \frac{|a_{n-2}|}{|z|^2} - \dots - \frac{|a_0|}{|z|^n} \right),$$

mostrando que

$$\lim_{|z| \rightarrow +\infty} |f(z)| = +\infty.$$

Assim, existe $R > 0$, tal que $|f(z)| > |f(0)|$ para todo z com $|z| > R$. Se $D_f = \{z \in \mathbb{C}; |z| \leq R\}$, pelo Teorema de Weierstrass [21, p. 19], temos a existência de $z_0 \in D_f$, tal que $|f(z_0)| \leq |f(z)|$ para todo $z \in D_f$. Como $|f(z_0)| \leq |f(0)|$, temos que $|f(z_0)| \leq |f(z)|$ para todo $z \in \mathbb{C}$. \square

Lema A.30. Seja $f \in \mathbb{C}[X] \setminus \mathbb{C}$. Se $z_0 \in \mathbb{C}$ é tal que $f(z_0) \neq 0$, então existe $z_1 \in \mathbb{C}$ tal que $|f(z_1)| < |f(z_0)|$.

Demonstração. Aqui também basta provar o resultado para polinômios mônicos. Seja $f(x) = x + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ e sejam z_0 e h números complexos tais que $f(z_0) \neq 0$ e h a ser determinado de modo que $|f(z_0 + h)| < |f(z_0)|$.

Com o auxílio do binômio de Newton, podemos escrever

$$f(z_0 + h) = (z_0 + h)^n + a_{n-1}(z_0 + h)^{n-1} + \dots + a_0 = f(z_0) + q(h),$$

onde q é um polinômio não identicamente nulo, pois f é um polinômio não constante, de grau n e sem termo constante. Seja bx^n o termo de menor grau em q . Assim, podemos escrever $q(x) = bx^n + x^{m+1}r(x)$, onde r é um outro polinômio.

Podemos escolher o argumento de h de modo que $\lambda = \frac{bh}{f(z_0)}$ tenha argumento igual a π (lembre que $f(z_0) \neq 0$). Portanto, λ é um número real negativo. Podemos garantir que a desigualdade $-1 \leq \lambda \leq 0$ se mantém para $|h|$ suficientemente pequeno. Tomamos, ainda, $|h|$ suficientemente pequeno para que $|h^{m+1}r(h)| < |bh^m|$. Pela desigualdade triangular [7, p. 15], para todo $h \in \mathbb{C}$, nas condições acima, temos que

$$\begin{aligned} |f(z_0 + h)| &= |f(z_0) + bh^m + h^{m+1}r(h)| \\ &\leq |f(z_0) + bh^m| + |h^{m+1}r(h)| \\ &\stackrel{(1)}{=} |f(z_0)| - |bh^m| + |h^{m+1}r(h)| \\ &< |f(z_0)|. \end{aligned}$$

Portanto, existe $z_1 = z_0 + h$, com h como acima, tal que $|f(z_1)| < |f(z_0)|$.

Observamos que em (1) usamos o seguinte resultado, que pode ser encontrado em [7, p. 18]: Dados $z, w \in \mathbb{C}$ e $t \in \mathbb{R}$, então, $|z + w| = |z| - |w|$ se, e somente se, $w = tz$, $-1 \leq t \leq 0$. \square

Munidos do Lema A.29 e Lema A.30 estamos em condições de enunciar e demonstrar o **Teorema Fundamental da Álgebra**.

Teorema A.31 (Teorema Fundamental da Álgebra). *Todo polinômio $f \in \mathbb{C}[X] \setminus \mathbb{C}$ possui ao menos uma raiz complexa.*

Demonstração. Seja $f \in \mathbb{C}[X] \setminus \mathbb{C}$. Pelo Lema A.29, temos a existência de $z_0 \in \mathbb{C}$ tal que $|f(z_0)| \leq |f(z)|$ para todo $z \in \mathbb{C}$. Se $f(z_0) \neq 0$, então, pelo Lema A.30, existe $z_1 \in \mathbb{C}$ tal que $|f(z_1)| < |f(z_0)|$, o que é um absurdo. Portanto, $f(z_0) = 0$. \square

O Corolário A.32 fornece uma consequência imediata do Teorema Fundamental da Álgebra.

Corolário A.32. *Se $f(X) = a_n X^n + \dots + a_1 X + a_0$ é um polinômio de coeficientes complexos e grau $n \geq 1$, então existem n números complexos z_1, \dots, z_n tais que*

$$f(X) = a_n(X - z_1) \dots (X - z_n).$$

A expressão acima é a **forma fatorada** do polinômio f .

Demonstração. Façamos a prova por indução sobre o grau n de f , sendo o caso $n = 1$ imediato. Suponha, pois, $n > 1$ e o corolário válido para todo polinômio de coeficientes complexos de grau $n - 1$.

Se $z_1 \in \mathbb{C}$ é uma raiz de f , o teste da raiz garante a existência de um polinômio g , também de coeficientes complexos, tal que $f(X) = (X - z_1)g(X)$. Note que g tem grau $n - 1$ e coeficiente líder a_n ; portanto, por hipótese de indução existem $z_2, \dots, z_n \in \mathbb{C}$ tais que $g(X) = a_n(X - z_2) \dots (X - z_n)$. Logo, $f(X) = (X - z_1)g(X) = a_n(X - z_2) \dots (X - z_n)$, o que conclui a prova. \square

Exemplo A.33. Dado $f(X) = X^2 + 1$, os números $-i, i \in \mathbb{C}$ são tais que $(X + i)(X - i) = X(X - i) + i(X - i) = X^2 - iX + iX - i^2 = X^2 + 1 = f(X)$. Logo, $f(X) = (X + i)(X - i)$ é a forma fatorada de f para $z_1 = -i$ e $z_2 = i$.

Retornando ao caso geral, seja $f(X) = a_n X^n + \dots + a_1 X + a_0$ um polinômio não nulo sobre \mathbb{K} . Se existirem elementos $\alpha_1, \dots, \alpha_m \in \mathbb{K}$ para os quais

$$f(X) = a_n(X - \alpha_1) \dots (X - \alpha_m)$$

também diremos que tal expressão é a **forma fatorada** de f sobre \mathbb{K} .

Considerando que alguns dos α_j podem se repetir, depois de reordená-los, se necessário, e considerando apenas os α_j distintos, podemos concluir que existem $1 \leq m \leq n$ e k_1, \dots, k_m inteiros positivos tais que

$$f(X) = a_n(X - \alpha_1)^{k_1} \dots (X - \alpha_m)^{k_m},$$

com $k_1 + \dots + k_m = n$ e $\alpha_1, \dots, \alpha_m$ elementos dois a dois distintos de \mathbb{K} .

Exemplo A.34. A forma fatorada de $f(X) = X^6 - 13X^5 + 67X^4 - 171X^3 + 216X^2 - 108X$ é $f(X) = (X - 0)(X - 2)(X - 2)(X - 3)(X - 3)(X - 3) = X(X - 2)(X - 2)(X - 3)(X - 3)(X - 3)$. Tomando $k_1 = 1$, $k_2 = 2$ e $k_3 = 3$ e, $\alpha_1 = 0$, $\alpha_2 = 2$ e $\alpha_3 = 3$ podemos escrever $f(X) = X(X - 2)^2(X - 3)^3$.

A.5 Relações entre coeficientes e raízes

Nesta seção apresentamos importantes relações entre as raízes de um polinômio em várias indeterminadas, comumente chamadas de *relações entre coeficientes e raízes* de um polinômio.

Definição A.35. Um polinômio $f \in \mathbb{K}[X_1, \dots, X_n]$ é **simétrico** quando

$$f(X_1, X_2, \dots, X_n) = F(X_{\sigma(1)}, X_{\sigma(2)}, \dots, X_{\sigma(n)},)$$

para todas as bijeções $\sigma : I_n \rightarrow I_n$, onde $I_n = \{1, \dots, n\}$.

Dentre os polinômios simétricos destacamos os da definição a seguir.

Definição A.36. Para $0 \leq j \leq n$, o j -ésimo **polinômio simétrico elementar** em X_1, \dots, X_n , denotado por $s_j = s_j(X_1, \dots, X_n)$, é definido como

$$s_j(X_1, \dots, X_n) = \begin{cases} 1, & \text{se } j = 0 \\ \sum_{1 \leq i_1 < \dots < i_j \leq n} X_{i_1} X_{i_2} \dots X_{i_j}, & \text{se } 1 \leq j \leq n \end{cases}.$$

No caso $n = 3$, por exemplo, temos

$$s_0 = 1, \quad s_1 = X_1 + X_2 + X_3, \quad s_2 = X_1 X_2 + X_2 X_3 + X_1 X_3, \quad s_3 = X_1 X_2 X_3.$$

Proposição A.37. Se $f(X) = a_n X^n + \dots + a_1 X + a_0 \in \mathbb{K}[X] \setminus \mathbb{K}$ se fatora completamente sobre \mathbb{K} , com raízes $\alpha_1, \dots, \alpha_n$, então, para $1 \leq j \leq n$, temos

$$s_j(\alpha_1, \dots, \alpha_n) = (-1)^j \frac{a_{n-j}}{a_n}. \quad (\text{A.2})$$

Demonstração. Por simplicidade de notação, denote $s_j(\alpha_1, \dots, \alpha_n)$ simplesmente por $s_j(\alpha_i)$. Escrevendo $f(X) = a_n(X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n)$ e expandindo os parênteses, obtemos

$$f(X) = a_n X^n - a_n s_1(\alpha_i) X^{n-1} + a_n s_2(\alpha_i) X^{n-2} - \dots + a_n (-1) s_n(\alpha_i).$$

Igualando os coeficientes correspondentes nessa expressão para f e naquela do enunciado, obtemos o resultado desejado. \square

Em outras palavras,

$$\frac{a_{n-1}}{a_n} = - \sum_i \alpha_i \quad \text{e} \quad a_0 = (-1)^n \prod_i \alpha_i, \quad (\text{A.3})$$

para qualquer $n \geq 2$.

As igualdades provenientes de (A.2), que relacionam coeficientes e raízes de um polinômio f não constante, são conhecidas como as **relações de Girard** ou **fórmulas de Vieta**. Elas nos permitem conhecer, com relação às raízes de f , a sua soma, a soma de seus produtos dois a dois, a soma de seus produtos três a três e assim por diante, além da soma de seus quadrados e a soma de seus inversos.

Embora as fórmulas de Vieta sejam úteis na resolução de vários tipos de problemas envolvendo as raízes de um polinômio, elas não são suficientes para determinar suas raízes.

Exemplo A.38. Sejam α_1 , α_2 e α_3 as raízes complexas do polinômio $f(X) = X^3 + 3X^2 - 2$. Pelas relações de Girard, temos

$$\alpha_1 + \alpha_2 + \alpha_3 = -3, \quad \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = 0 \quad \text{e} \quad \alpha_1\alpha_2\alpha_3 = 2.$$

Multiplicando a segunda igualdade acima por α_2 , obtemos $\alpha_1\alpha_2^2 + \alpha_1\alpha_2\alpha_3 + \alpha_2^2\alpha_3 = 0$ e, como $\alpha_1\alpha_2\alpha_3 = 2$, podemos escrever $\alpha_2^2(\alpha_1 + \alpha_3) + 2 = 0$. Agora, como $\alpha_1 + \alpha_3 = -3 - \alpha_2$, temos que $\alpha_2^2(-3 - \alpha_2) + 2 = 0$, o que é equivalente à $f(\alpha_2) = 0$. De modo análogo, ao tentarmos determinar α_1 e α_3 , obtemos expressões equivalentes a $f(\alpha_1) = 0$ e $f(\alpha_3) = 0$. Mas, para fins de determinação das raízes de f não há diferença entre as expressões $f(\alpha_1)$, $f(\alpha_2)$, $f(\alpha_3)$ e $f(X)$.

Nas notações da Proposição A.37, nos referimos a $s_j(\alpha_1, \dots, \alpha_n) \in \mathbb{K}$ como a j -ésima **soma simétrica elementar** das raízes de f . Sempre que $\alpha_1, \dots, \alpha_n$ estiverem subentendidos e não houver perigo de confusão com o polinômio simétrico elementar $s_j = s_j(\alpha_1, \dots, \alpha_n)$, denotaremos a soma simétrica elementar $s_j(\alpha_1, \dots, \alpha_n)$ simplesmente por s_j .