UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA

ANA NERY JESUS SANTOS

SOLUÇÃO DE EQUAÇÕES POLINOMIAIS POR MEIO DE RADICAIS

SÃO CRISTÓVÃO-SE
2019

ANA NERY JESUS SANTOS

SOLUÇÃO DE EQUAÇÕES POLINOMIAIS POR MEIO DE RADICAIS

Dissertação apresentada ao
Programa de Pós-Graduação em
Matemática, da Universidade
Federal de Sergipe, como
requisito parcial para obtenção do
título de Mestre em Matemática.

Orientador: Evilson da Silva Vieira

SÃO CRISTÓVÃO-SE
29 DE AGOSTO DE 2019

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE

Santos, Ana Nery Jesus
S237s Solução de equações polinomiais por meio de radicais / Ana Nery Jesus Santos ; orientador Evilson da Silva Vieira. – São Cristóvão, 2019.
96 f. : il.

Dissertação (mestrado em Matemática) – Universidade Federal de Sergipe, 2019.

1. Matemática. 2. Polinômios. 3. Teoria dos grupos. 4. Galois, Teoria de. 5. Anéis (Álgebra). 6. Equações – Soluções numéricas. I. Vieira, Evilson da Silva orient. II. Título.

CDU 512.6

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Solução de equações polinomiais por meio de radicais

por

Ana Nery Jesus Santos

Aprovada pela banca examinadora:

Prof. Evilson da Silva Vieira - UFS
Orientador

Prof. André Vinicius Santos Dória - UFS
Primeiro Examinador

Prof. Carlo Pietro Sousa da Silva - UFS
Segundo Examinador

São Cristóvão, 29 de Agosto de 2019

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

AGRADECIMENTOS

É com imensa satisfação que venho agradecer a todos que direta ou indiretamente contribuíram para a finalização desse trabalho.

Poucas pessoas sabem o quanto eu desejei voltar a estudar, a falta que senti desse mundo acadêmico que tanto me agrada, no entanto, nem tudo são flores... Hoje sem dedicação total aos estudos, senti como é difícil conciliar trabalho e estudo. Se eu já admirava quem o fazia, hoje admiro ainda mais.

Foram muitos percalços, no entanto de nada me arrependo. O conhecimento que adquiri, as pessoas que convivi e hoje tenho o prazer de chamar de "família do mestrado", fez cada noite de sono perdida e cada estresse valer a pena.

Sendo assim, agradeço sobretudo ao nosso PAI, pelo dom da vida e pela força, afinal foi sempre nele que confiei quando o fardo parecia mais pesado do que eu conseguiria suportar.

Agradeço à meu esposo, Pablo, pela infinita paciência e ajuda em todos os sentidos, principalmente pela força nas horas difíceis.

À minha mãe, Giselda, e minha família em geral, pela compreensão quanto às minhas ausências.

À todos os meus amigos, que não esqueceram de mim, mesmo eu estando tão ausente, e que torceram muito por essa minha realização.

Aos colegas de trabalho que sempre que possível me encorajava com lindas palavras. E também aos meus alunos, que compreenderam minha ausência, e me apoiavam.

Aos meus professores, tando do mestrado, quanto da minha vida acadêmica como um todo. Agradeço todos os ensinamentos.

À minha psicóloga, Ísis, que tantas vezes me acalmou e me fez voltar aos trilhos.

À meu orientador, Evilson, pelo rico ensinamento, horas de dedicação e paciência com meu jeito "estressado"de ser.

À meu parceiro de dissertação, Voni, conhecido como "pestinho", que tantas vezes me fez companhia noite a dentro sempre pronto pra me ajudar.

À meu parceiro de viagem, Maurício, que ajudou demais a tornar cada viagem menos cansativa e mais prazerosa.

E um agradecimento especial aos meus colegas de curso. Como foi importante todas aquelas manhãs de estudo. A diversão, o conhecimento. Levarei essa amizade pra minha vida, porque vocês são pessoas muito especiais.

Enfim, obrigada a cada um que tendo citado aqui ou não, e de alguma forma contribuiu para a realização desse sonho.

Muito obrigada.

Nunca deixem que lhe digam que não vale a pena acreditar nos sonhos que se tem, ou que seus planos nunca vão dar certo, ou que você nunca vai ser alguém...
(Renato Russo)
P.S. Mesmo que esse alguém seja você mesmo!
(Ana Nery)

RESUMO

Por muito tempo, os matemáticos dedicaram-se a encontrar soluções para eventuais problemas. Um dos que lhes intrigavam era a resolução de equações. Como fruto desses estudos, hoje temos fórmulas que solucionam qualquer equação polinomial de grau ≤ 4. No entanto, quando os desafios passaram a ser sobre equações de grau 5, chegou-se à conclusão que nem sempre era possível encontrar soluções expressas por meio de radicais.

Muitos matemáticos dedicaram-se a solucionar esse problema. Joseph Loius Lagrange em 1770 verificou que os artifícios usados nas equações de graus 3 e 4 não serviam para as de grau 5. Suspeitaram então que talvez não fosse sempre possível determinar tais soluções.

O matemático Niels Henrik Abel, em 1824 conseguiu comprovar essas suspeitas. Mas ficou a questão: Quando seria possível encontrar soluções por meio de radicais para equações de grau ≥ 5?

E, em 1843, chegou até a Academia de Ciências de Paris o trabalho do brilhante matemático Evariste Galois, que desenvolveu a importante teoria que leva seu nome, além da Teoria de Grupos, que explicam de forma belíssima essa questão.

Faremos aqui um estudo introdutório da Teoria dos Grupos, Extensões de Corpos e Teoria de Galois, que servirão de ferramentas para mostrar "a solução de equações polinomiais por meio de radicais".

Palavras-chave: Grupos; Polinômios; Extensões; Galois; Solubilidade por Radicais.

ABSTRACT

For many years, mathematicians have dedicated to finding solutions for eventual problems. One of those that intrigued them, it was the solution of equations. As a result of these studies, today we have formulas that solve any polynomial equation of degree ≤ 4. However, when the challenges came to be about equations of degree 5. It was concluded that it was not always possible to find solutions expressed by radicals.

Many mathematicians have dedicated to solve this problem. Josefh Louis Lagrange in 1770 found that the gimmicks used in the equations of degrees 3 and 4 did not fit for degrees 5. They suspected that it might not always be possible to determine the solutions.

In 1824, the mathematician, Niels Henrik Abel was able to prove these suspicious. But it stayed the question: When would it be possible to find solutions of radicals for equations of degree ≥ 5?

And in 1843, the mathematician Evariste Galois' brilliant work came to the Paris Academy of Sciences, who developed the important theory that bears his name, as well as the Group Theory, which beautifully explains this question.

We will do an introductory study of Group Theory, Field Extensions, and Galois Theory, which it will serve as tools for showing "the solution of polynomial equations through radicals".

Keywords: Extensions; Galois; Groups; Polynomials; Solubility by Radicals.

Sumário

Introdução

Desde sempre, o homem se propõe a encontrar soluções para seus problemas. Sejam problemas simples e cotidiano, como determinar áreas, que intrigavam povos antigos, sejam problemas mais complexos e atuais, como por exemplo, a garantia na segurança de sistemas bancários por meio de criptografia. Muitos desses problemas traduzem-se matematicamente em soluções de equações.

Nesse sentido, se faz necessário um breve conhecimento histórico sobre as equações polinomiais e os matemáticos que se destacaram nesse estudo.

Um Pouco de História

As primeira noções de equações datam de 1700 a.C., quando as utilizavam por meio de palavra sem os, hoje conhecidos, símbolos matemáticos. O famoso papiro Rhind, de 1650 a.C., é o primeiro registro do qual se tem notícia onde encontram-se as ideias das equações polinomiais. Os babilônicos, por volta de 1800 a.C., tratavam as equações numa linha algébrica, enquanto os gregos a faziam numa linha geométrica.

Deve-se ao matemático grego Diofanto as primeiras inclusões de símbolos no estudo das equações, por volta de 250 d.C.. E além dele, vários outros matemáticos se debruçaram no estudo e desenvolvimento das equações.

As equações como conhecemos hoje, com representação por meio de símbolos, tem seu uso recente, datado de cerca de 500 anos, e deve-se à matemáticos como François Viète e René Descarte.

Acredita-se que os babilônicos já utilizavam métodos de resolução para as equações de grau dois (ou equações quadráticas), por volta de 1800 a.C.. Os gregos, utilizavam a geometria para solucioná-las, inclusive para algumas equações de grau três (ou equação cúbica). Porém, deve-se aos árabes a fórmula que hoje conhecemos para resolução das equações quadráticas que serão apresentadas na seção 5.2.

Quanto às equações cúbicas, Scípio del Ferro e Niccolo Fontana (conhecido como Tartaglia) foram os responsáveis por descobrir suas soluções. Mais tarde, em 1545, esses métodos foram divulgados por Cardano, que também, divulgou o método de Ferrari para resolução das equações de grau quatro (ou equações quárticas).

Obviamente o próximo passo era encontrar as soluções das equações de grau cinco. E

muitos matemáticos tentaram. Euler, apesar de não conseguir, desenvolveu outro método para as quárticas. Lagrange, em 1770, tentou usar as técnicas usadas nas de graus três e quatro, e concluiu que não era possível usar nas de grau cinco.

Suspeitando de não ser possível encontrar tais soluções, o matemático Niels Henrik Abel, em 1824, acabou com tais suspeitas, e provou que de fato não era possível encontrar tais soluções por meio de radicais, ao menos de modo geral, visto que para algumas era possível determinar suas soluções.

A dúvida no entanto permaneceu quanto às equações de graus > 5. E então, quando seria possível encontrar soluções por meio de radicais para equações de grau ≥ 5?

Na busca por essa resposta, destacou-se um dos maiores matemáticos de todos os tempos, Evariste Galois. Sua contribuição é de tamanha importância, que cabe discorrer um pouco sobre sua biografia na seção .

Galois desenvolveu a chamada Teoria de Galois que usando uma outra teoria também desenvolvida por ele, a Teoria de Grupos, consegue explicar em quais circunstâncias uma equação de qualquer grau pode ou não apresentar soluções por meio de radicais. Seu trabalho, foi apresentado à Academia de Ciências de Paris em 1843.

Diante disso provou-se que equações de graus ≥ 5 de modo geral não são solúveis por radicais, e por isso é impossível definir uma fórmula que as resolvam. Porém existem equações de graus ≥ 5 que possui soluções por meio de radicais, e Galois explica a condição necessária para tal.

Aplicações e Relevância do Tema

Muitas são as áreas que atraem atenção dos amantes da Matemática. E cada uma delas tem suas beleza e importância. Encontrar solução de problemas é algo que permeia desde os primórdios até os dias de hoje. E na busca por soluções é que desenvolveu-se o estudo das equações, alicerce da Álgebra.

Atualmente o homem se dispõe a encontrar soluções de problemas dos mais diversos tipos e complexidade. Imaginemos, por exemplo, a importância de se criar um sistema de segurança de dados de um banco, por meio da criptografia, é de fato algo muito complexo e importante.

Muitos dos problemas são traduzidos em equações e sistemas de equações, muitas vezes, bem complexos. Essas traduções se devem a outra importante área da Matemática denominada Modelagem Matemática.

Se hoje temos problemas com equações tão complexas, é inevitável pensar que no princípio era bem diferente, hoje diríamos até fáceis, mas os matemáticos da época certamente não concordariam. Imaginemos as dificuldades pelas quais passaram para chegar na solução de uma equação quártica.

Na Álgebra, um dos mais importantes capítulos da sua história, se deve ao matemático

Galois, e é inegável o interesse de qualquer amante da Matemática em sua belíssima teoria.

E foi pensando na importância que as equações tiveram e têm até hoje, e mais ainda na magnitude da teoria que as cercam, que nos debruçarmos sobre esse tema. Diante disso, nos resta esperar que o leitor aprecie nosso trabalho e entenda os motivos pelos quais tantos tem verdadeira paixão por esse tema.

Descrição do Trabalho

Este trabalho abordará alguns aspectos teóricos que cercam a Teoria de Galois, não de forma completa, por se tratar de assuntos muito extensos, mas garantindo o conhecimento necessário para sua compreensão. Ressaltando que o leitor sempre que necessário, poderá recorrer às referências citadas.

No capítulo 1, apresentamos os principais conceitos da chamada Teoria de Grupos, também desenvolvida por Galois, especificamente para servir de ferramenta na Teoria de Galois, que será detalhada no capítulo 4.

O capítulo 2 trata das estruturas algébricas necessárias, especificamente dos Anéis de Polinômios, objeto central no estudo das equações polinomiais.

O estudo das extensões de corpos, necessário nas determinações de raízes de polinômios é tratado no capítulo 3. Continuando, no mesmo capítulo trazemos um breve estudo sobre as chamadas raízes complexas, com foco nas raízes n-ésimas da unidade.

Como já mencionado, no capítulo 4, apresentamos a belíssima Teoria de Galois, que basicamente transforma o problema de encontrar as raízes de um polinômio num problema de grupos, por meio da chamada *Correspondência de Galois*.

Como a solução que buscamos é a chamada solução por meio de radicais, no capítulo 5, definimos e discorremos sobre a solubilidade por meio de radicais. Além disso, de modo a expor os estudos desenvolvidos pelos matemáticos, mostramos a construção das fórmulas resolutivas das equações de graus ≤ 4. E findamos mostrando a impossibilidade de existir soluções para as equações de graus ≥ 5, com atenção especial para um caso prático que utiliza toda a teoria exposta até então.

Biografia de Evariste Galois

Evariste Galois nasceu em 25 de outubro de 1811 numa aldeia chamada Bourg-la-Reine, França, onde seu pai era prefeito. Desde sua infância enfrentou diversas dificuldades pessoais e acadêmicas. Porém, com algumas anotações, ele contribuiu consideravelmente para a Matemática, desenvolvendo a famosa "Teria de Galois".

Aos 12 anos já mostrava suas habilidades em Matemática (Álgebra e Geometria), além de se interessar pelo Latim e Grego. Aos 16 anos, foi recusado ao tentar entrar na escola Politécnica, eis seu primeiro fracasso. Aos dezessete anos entregou um artigo a

Cauchy sobre suas descobertas fundamentais, no entanto, Cauchy o perdeu antes mesmo de apresentá-lo na academia.

Após o suicídio de seu pai, Galois, desiludido, entrou na Escola Normal, no intuito de futuramente lecionar, mas não abandonou suas pesquisas. Em 1830, escreveu um artigo para o concurso de Matemática da Academia, entregou à Fourier, que morreu logo em seguida e seu artigo ficou perdido.

Diante de tantas frustrações, Galois foi expulso da Escola Normal, por se envolver nas causas de revolução em 1830, e entrou para a guarda nacional.

Em seguida, começou a estudar o trabalho de Lagrange sobre permutações de raízes onde surgiu, implicitamente, o conceito de "corpo", mais tarde foi definido de forma explícita por Dedekind. E a partir desse estudo, e dos estudos de Abel, Galois desenvolveu toda a teoria que leva seu nome e é objeto de estudo desse trabalho.

Na época, entregou seu trabalho à Poisson que o considerou "incompreensível", mas hoje são as ideias de Galois que chamamos de "Matemática Moderna".

Galois faleceu muito prematuramente, aos 20 anos numa manhã de 30 de maio de 1832 após receber um tiro fatal em um duelo por se envolver com uma mulher já comprometida. Na noite anterior ao duelo, ele passou horas fazendo anotações deixada numa carta à um amigo, com um pedido de que fosse entregue aos matemáticos da época.

Para mais detalhes sobre a vida de Galois, o leitor pode consultar [16].

Abordagem do tema na Educação Básica

O tema desse trabalho, pode facilmente ser encontrado no currículo da Educação Básica, obviamente, não com tantas riquezas de detalhes, mas com sua essência, a *solução de equações polinomiais*. Durante vários momentos dos Ensinos Fundamental e Médio, o aluno tem contato com a Álgebra e as equações polinomiais.

No sétimo ano do Ensino Fundamental, os alunos tem as primeiras noções de Álgebra, e consequentemente, o contato com suas primeiras equações polinomiais, as de grau um. Na BNCC (Base Nacional Comum Curricular), podemos constatar nas habilidades de números EF07MA16 e EF07MA18 tal presença, elas nos dizem que, o aluno deve:

"Reconhecer se duas expressões algébricas obtidas para descrever a regularidade de uma mesma sequência numérica são ou não equivalentes."

"Resolver e elaborar problemas que possam ser representados por equações polinomiais de 1º grau, redutíveis à forma $ax + b = c$, fazendo uso das propriedades da igualdade."

Ainda no Ensino Fundamental, os alunos, no oitavo ano, conhecem as equações polinomiais de primeiro grau com duas incógnitas e alguns casos de equações polinomiais de grau dois. Vejamos as habilidades EF08MA08 e EF08MA09:

"Resolver e elaborar problemas relacionados ao seu contexto próximo, que possam ser representados por sistemas de equações de 1º grau com duas incógnitas e interpretá-los,

utilizando, inclusive, o plano cartesiano como recurso."

"Resolver e elaborar, com e sem uso de tecnologias, problemas que possam ser representados por equações polinomiais de 2º grau do tipo $ax^2 = b$."

Por fim, no nono ano, ainda notamos a presença das equações polinomiais, por exemplo, na habilidade EF09MA09:

"Compreender os processos de fatoração de expressões algébricas, com base em suas relações com os produtos notáveis, para resolver e elaborar problemas que possam ser representados por equações polinomiais do 2º grau."

Não acaba no Ensino Fundamental o contato do aluno com a Álgebra e as equações polinomiais, durante todo o Ensino Médio elas estão presentes, vejamos, por exemplo, as habilidades EM13MAT401, EM13MAT501 e EM13MAT502:

"Converter representações algébricas de funções polinomiais de 1º grau em representações geométricas no plano cartesiano, distinguindo os casos nos quais o comportamento é proporcional, recorrendo ou não a softwares ou aplicativos de álgebra e geometria dinâmica."

"Investigar relações entre números expressos em tabelas para representá-los no plano cartesiano, identificando padrões e criando conjecturas para generalizar e expressar algebricamente essa generalização, reconhecendo quando essa representação é de função polinomial de 1º grau."

"Investigar relações entre números expressos em tabelas para representá-los no plano cartesiano, identificando padrões e criando conjecturas para generalizar e expressar algebricamente essa generalização, reconhecendo quando essa representação é de função polinomial de 2º grau do tipo $y = ax^2$."

Diante da necessidade e importância das equações polinomiais na Educação Básica, esse trabalho pode servir para o professor se aprofundar um pouco mais nessas teorias, de modo a compreendê-lo melhor e passar seus ensinamentos mais seguramente. É bem verdade que pouco do que apresentamos aqui o professor poderá repassar a seus alunos, no entanto, ele poderá falar da importância do tema, dos matemáticos que contribuíram, com ênfase a Galois, por exemplo, numa aula introdutória, como forma de instigar a curiosidade e busca pelo conhecimento por parte dos alunos.

Capítulo 1

Grupos

A Teoria dos Grupos, é um ramo da Matemática que estuda a estrutura algébrica denominada Grupo, sua utilidade perpassa várias outras ciências. Seu foco é trabalhar com "simetrias de uma estrutura", e desta forma, a vemos na Física, por exemplo: no estudo de Mecânica Quântica, Física de Partículas, Eletrônica de Circuitos; na Química, por exemplo: no estudo dos átomos, é possível inclusive com o uso da Teoria de Grupos, modelar a trajetória do elétron no átomo, ou ainda no estudo dos modelos de ligações químicas, associado à Teoria Quântica moderna; e nas mais diversas áreas, por exemplo: em jogos, como o cubo mágico (ou cubo de Rubik), onde a Teoria dos Grupos fornece ferramentas para sua resolução.

Na Álgebra Abstrata, os grupos são vistos como uma estrutura algébrica, que podemos dizer que servem de base para o estudo das demais, como anéis, corpos, espaços vetoriais e outros, basta que a ela sejam acrescidas algumas operações e axiomas.

A origem histórica do conceito de grupo é encontrada na Teoria de Galois, cujo teorema principal diz que *"um polinômio é solúvel por radicais se, e somente se seu grupo de Galois possui uma propriedade especial — o nome técnico é solúvel"*. Para conhecer mais do contexto histórico, o leitor pode ver [3].

Nosso principal objetivo nesse trabalho, em relação a grupos, é entender o conceito de grupos solúveis, uma vez que estes estão relacionados às equações polinomiais que possuem soluções por radicais. Para tanto, o que faremos é só expor algumas definições e exemplos, omitindo inclusive, algumas demonstrações, que poderão ser encontradas nas devidas referências, a título de curiosidade do leitor. Portanto não nos aprofundaremos de fato nessa teoria, que por completo é muito ampla.

1.1 Definição, exemplos e propriedades

Mostraremos aqui a definição formal de grupos, algumas propriedades que são imediatas da definição e uns poucos exemplos, dos quais discutiremos alguns mais afundo posteriormente.

Definição 1.1. Seja G um conjunto munido da operação $*$, dizemos que G é um grupo, e representamos por $(G, *)$ se a operação satisfaz as seguintes condições:

i. É associativa, ou seja,

$$a * (b * c) = (a * b) * c, \forall a, b, c \in G;$$

ii. Possui elemento neutro, ou seja,

$$\exists\ e \in G \text{ tal que, } e * a = a * e = a, \forall a \in G;$$

iii. Possui elemento inverso, ou seja,

$$\text{Dado } a \in G,\ \exists b \text{ tal que } a * b = b * a = e.$$

Comumente denotaremos o elemento inverso de a por a^{-1}.

O grupo será dito *abeliano* (em homenagem ao matemático N. H. Abel) ou *comutativo* se satisfaz:

$$a * b = b * a, \forall a, b \in G.$$

1.1.1 Propriedades

Com o intuito de facilitar nossas notações, usaremos apenas G para representar $(G, *)$. Algumas importantes propriedades podem ser mencionadas, vejamos:

Lema 1.2. *(Propriedades) Seja G um grupo, então:*

i. O elemento neutro é único;

ii. O elemento inverso é único;

iii. $(a^{-1})^{-1} = a$;

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

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

Demonstração. *i.* Supondo que não seja único, sejam $e,\ e' \in G$ elementos neutros distintos, então,

$$e = e * e' = e'$$

E temos uma contradição, logo o elemento neutro é único.

ii. Supondo que não seja único, seja $a \in G$ e sejam $b,\ b' \in G$ os elementos inversos de a, temos,

$$b = b * e = b * (a * b') = (b * a) * b' = e * b' = b'$$

E temos uma contradição, logo o elemento inverso é único.

iii. Ora, $a^{-1} * a = a * a^{-1} = e$, e então o inverso de a^{-1} é a, logo $(a^{-1})^{-1} = a$.

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

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

e

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

Mostrando assim o que queríamos.

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

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

De modo análogo prova-se que $a * x = b$ tem uma única solução, a saber, $a^{-1} * b$.

□

1.1.2 Exemplos de Grupos

i. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$, são exemplos de grupos aditivos abelianos.

ii. $(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$, são exemplos de grupos multiplicativos abelianos, cujos elementos admitem inverso multiplicativo.

iii. $(M_{m\times n}(\mathbb{K}), +)$ é um grupo aditivo abeliano. Trata-se do grupo das matrizes de ordem $m \times n$ de termos pertencentes à $\mathbb{K}$ onde $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.

iv. $(\mathrm{GL}_n(\mathbb{K}), \cdot)$ é um grupo multiplicativo não abeliano, trata-se do grupo das matrizes inversíveis de ordem n e elementos pertencentes a $\mathbb{K}$ onde $\mathbb{K} = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, esse grupo é chamado de grupo linear de grau n.

v. $(\mathbb{Z}_n, +)$ é um grupo aditivo abeliano das classes de resíduo módulo n, onde $\mathbb{Z}_n$ é o conjunto quociente de $\mathbb{Z}$ pela relação de congruência módulo n, e representado por $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$, ou de $\mathbb{Z}$ por $n\mathbb{Z}$. Para entender melhor este grupo, veja [1].

vi. $(\mathbb{Z}_p^*, \cdot)$ é um grupo multiplicativo, com p primo, cujos elementos admitem inverso multiplicativo.

vii. $(\text{Bij}(C), \circ)$ é um grupo geralmente não abeliano, onde $\text{Bij}(C) = \{f : C \to C | f$ é uma bijeção$\}$ e $\circ$ é a operação composição de funções. Caso C tenha exatos n elementos, denotamos $\text{Bij}(C)$ por S_n e o chamamos de *grupo das permutações* de n termos, e este terá exatamente $n!$ elementos.

1.1.3 Grupos das Permutações

O grupo das permutações de n elementos, como citados no exemplo (vii) da seção anterior, merece uma atenção especial. São os grupos das bijeções de um conjunto nele próprio. Vale ressaltar, que aqui faremos uma breve introdução. Porém, na seção 1.7, o leitor terá a oportunidade de se aprofundar nesse grupo em específico.

Denotaremos tais grupos por $(S_n, \circ)$, ou simplesmente S_n. A notação usual é a seguinte: dada $f \in S_n$ e $f(m) = i_m$, com $m \in \{1, 2, \ldots, n\}$, então:

$$f = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}.$$

Sendo assim, vejamos como seria o grupo S_3, a título de exemplo. Como sabemos, a quantidade de permutações possíveis de 3 elementos será 3!, representamos por, $\#S_3 = 3! = 6$, logo trata-se de um grupo com 6 elementos, são eles:

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

1.1.4 Grupo das Simetrias

Esse grupo pode ser interpretado como o conjunto das transformações de um objeto geométrico que não afetam a forma do objeto, como algumas rotações e reflexões. A exemplo temos o $S_\triangle$ o grupo das simetrias do triângulo equilátero, formada por:

$$S_\triangle = \{e, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}, R_1, R_2, R_3\}.$$

Para mais detalhes, consultar [1] e [3]; e $S_\square$, grupo das simetrias do quadrado. Vejamos o grupo das simetrias espaciais de um quadrado, chamaremos $(S_\square, \circ)$ ou simplesmente $S_\square$.

Dado um quadrado $P_1P_2P_3P_4$, com centro na origem do espaço, chamemos D_1, D_2, M e N suas diagonais e mediatrizes, como mostra a figura 1.1.

Notemos que as rotações no sentido anti-horário de ângulos zero, $\dfrac{\pi}{2}$, π e $\dfrac{3\pi}{2}$ preservam o quadrado. Chamemos tais transformações respectivamente de e, $R_{\frac{\pi}{2}}$, R_π e $R_{\frac{3\pi}{2}}$.

Outras transformações que preservam o quadrado são as rotações espaciais de ângulo π em torno dos eixos D_1, D_2, M e N. Chamemos-as de R_1, R_2, R_M e R_N.

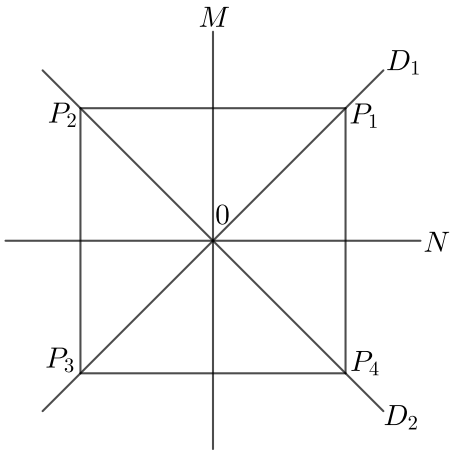

Figura 1.1: Quadrado $P_1P_2P_3P_4$

Assim temos que:

$$S_\square = \{e, R_{\frac{\pi}{2}}, R_\pi, R_{\frac{3\pi}{2}}, R_1, R_2, R_M, R_N\}$$

Esse grupo é não abeliano, basta observarmos, por exemplo que: $R_1 \circ R_M = R_{\frac{3\pi}{2}}$, enquanto que $R_M \circ R_1 = R_{\frac{\pi}{2}}$.

Notemos que S_4 tem quantidade de termos diferente da quantidade de termos de $S_\square$, pelo que vimos $\#S_4 = 4! = 24$ que é diferente de $\#S_\square = 8$.

Da generalização dos grupos das simetrias para um polígono regular qualquer de n lados, tem-se o grupo diedral. Podemos dizer que o grupo diedral, denotado por D_n, trata-se de um grupo de $2n$ elementos, fruto de rotações em torno do centro de $\dfrac{2k\pi}{n}$ radianos, com $k = 1, 2, \ldots, n-1$, e reflexões de π radianos em torno das retas que passam pelo seu centro e divide o polígono em duas partes simétricas. Para mais detalhes ver [3].

1.2 Subgrupo

Iniciemos essa seção com a definição formal de subgrupo, em seguida, traremos alguns exemplos.

Definição 1.3. Seja $(G, *)$ um grupo. Um subconjunto H de G, é chamado *subgrupo* de G, denotado por $H \leq G$, se H preserva a operação de G e é um grupo, veja a definição de grupo na seção 1.1.

A proposição seguinte apresenta critérios para que um subconjunto de G seja um subgrupo de G

Proposição 1.4. *Seja H um subconjunto não vazio de G. Então H é subgrupo de G se, e somente se, as duas condições seguintes são satisfeitas:*

i. $h_1 * h_2 \in H, \forall h_1, h_2 \in H$;

ii. $h^{-1} \in H, \forall h \in h$, *onde* h^{-1} *é o elemento inverso de* h.

Demonstração. Antes de iniciarmos a demonstração, vale ressaltar que, o inverso de um elemento no subgrupo é exatamente o mesmo no grupo, pela unicidade já demonstrada.

($\Longrightarrow$) Supondo $H \leq G$, o item *i.* segue imediatamente. Para o item *ii.*, seja $h \in H$, então $h \in G$, e também $h^{-1} \in G$. Como dito anteriormente, o inverso de $h \in H$ é necessariamente o mesmo de G, logo $h^{-1} \in H$, e provamos assim a ida.

($\Longleftarrow$) Supondo agora satisfeitas as condições *i.* e *ii.*, como H é um subconjunto de G, e a associatividade é válida para todo elemento de G, então vale para os elementos de H. Como H é não vazio, seja $h \in H$ de *ii.* temos que $h^{-1} \in H$ e então $h * h^{-1} = e$, portanto $e \in H$. Quanto à existência do inverso, esta já é garantido imediatamente de *ii.*. Dessa forma, verificamos as propriedades de grupos, portanto concluímos que $H \leq G$, e provamos assim a volta, concluindo nossa demonstração.

□

Exemplo 1.5. *i.* $\{e\}$ e G são subgrupos de G, chamados de subgrupos triviais.

ii. $(n\mathbb{Z}, +)$ é subgrupos de $(\mathbb{Z}, +)$, qualquer que seja n inteiro, onde $n\mathbb{Z}$ trata-se dos inteiros múltiplos de n.

iii. $\{e, R_\pi\}$ e $\{e, R_{\frac{\pi}{2}}, R_\pi, R_{\frac{3\pi}{2}}\}$ são subgrupos de $S_\square$

iv. O conjunto formado por interseções de subgrupos de G também é um subgrupo de G.

1.3 Ordem, geradores e grupos cíclicos

O conceito de *ordem* pode ser aplicado à um grupo ou à um elemento do grupo.

Definição 1.6. Se G é um grupo. A ordem de G, que denotamos por $|G|$, é a quantidade de elementos desse grupo, quando este grupo é finito. Quando o grupo G for infinito, denotamos $|G| = \infty$.

Exemplo 1.7. $|S_4| = 24$, bem como $|S_\square| = 8$, são exemplos de grupos finitos, já $|\mathbb{Z}| = \infty$, pois $(\mathbb{Z}, +)$ é um grupo infinito.

Definição 1.8. A ordem de um elemento $g \in G$, denotado por $\mathrm{o}(g)$, é o menor $n \in \mathbb{N}$ tal que $g^n = \underbrace{g * g * \cdots * g}_{n \text{ composições}} = e$, quando n existe, caso contrário, $\mathrm{o}(g) = \infty$.

Exemplo 1.9. No grupo S_3, temos que $\mathrm{o}(\beta) = 3$, pois $\beta^3 = e$, sendo o 3 o menor inteiro positivo onde essa condição é satisfeita.

Definição 1.10. Dizer que um grupo é gerado por um ou mais elementos, significa dizer que todos os elementos do grupo são determinados por meio de composições entre esses geradores.

Definição 1.11. Seja S um subconjunto não vazio de G, tal que todos os elementos de G são resultados das composições entre os elementos de S, então dizemos que G é gerado por S e denotamos, $G = \langle S \rangle$.

O grupo S_3, por exemplo é gerado por α e β, logo $S_3 = \langle \alpha, \beta \rangle$.

Definição 1.12. Quando um grupo G é gerado por um único elemento, $G = \langle g \rangle$, dizemos que G é um *grupo cíclico* e temos que $G = \{..., g^{-2}, g^{-1}, g^0, g, g^2, ...\}$, onde $g^0 = e$, ou ainda $G = \langle g \rangle = \{g^t | t \in \mathbb{Z}\}$.

Exemplo 1.13. O grupo $(\mathbb{Z}_n, +)$ é cíclico, e $Z_n = \langle m \rangle$, para todo m tal que $\text{mdc}(m, n) = 1$. O grupo $\mathbb{Z}$, é tal que $\mathbb{Z} = \langle 1 \rangle = \{..., 1^{-2}, 1^{-1}, 1^0, 1, 1^2, ...\} = \{..., -2, -1, 0, 1, 2, ...\}$, onde $1^0 = e$.

1.4 Teorema de Lagrange

Seja G um grupo e $H \leq G$, defina a relação de equivalência $\mathcal{R}$ sobre G:

$$y \ \mathcal{R} \ x \Leftrightarrow \exists \ h \in H \text{ tal que } y = xh.$$

Em [3] o leitor poderá buscar a definição de relação de equivalência.

Agora, constatemos que de fato $\mathcal{R}$ é uma relação de equivalência, verificando as três condições necessárias para tal:

Sejam $x, y, z \in G$ e $h \in H$, $\mathcal{R}$ é *reflexiva*, pois, para $h = e$,

$$x = xe \Longrightarrow x \ \mathcal{R} \ x.$$

É também simétrica, pois para $y \ \mathcal{R} \ x$, tem-se $y = xh$, e como $h^{-1} \in H$, pela definição de subgrupo, multiplicando ambos os lados da igualdade pela direita por h^{-1},

$$yh^{-1} = xhh^{-1} \Longrightarrow = yh^{-1} = xe \Longrightarrow x = yh^{-1}, \text{ ou seja, } x \ \mathcal{R} \ y.$$

Por fim, é transitiva, pois se $y \ \mathcal{R} \ x$ e $x \ \mathcal{R} \ z$, então,

$$y = xh \text{ e } x = zh', \text{ com } h, h' \in H$$

Substituindo,

$$y = (zh')h = z(h'h) = zh'', \text{ com } h'h = h'' \in H.$$

E então temos $y \mathcal{R} z$. Concluindo nosso propósito.

Assim a classe de equivalência de x será $\{y \in G | y \mathcal{R} x\} = \{xh | h \in H\}$. Denotaremos esse conjunto por xH e o chamaremos de *classe lateral à esquerda de H*. De modo análogo definimos $Hx = \{hx | h \in H\}$ como *classe lateral à direita de H*.

Como consequência imediata o fato de $\mathcal{R}$ ser uma relação de equivalência, é que xH determina uma partição em G, ou seja:

i. se $x \in G$, então $xH \neq \varnothing$;

ii. se $x, y \in G$, então $xH = yH$ ou $xH \cap yH = \varnothing$;

iii. a união de todas as classes laterais é igual a G.

Definição 1.14. A quantidade de termos do conjunto das classes laterais à esquerda é chamado *índice* de H em G e denotamos por $(G : H)$.

Teorema 1.15. *(Teorema de Lagrange)*

Seja G um grupo finito e $H \leq G$. Então a ordem de H divide a ordem de G. Em particular, tem-se $|G| = |H|(G : H)$.

Demonstração. Faremos a demonstração usando as classes laterais à esquerda. O resultado para classes laterais à direita é similar.

Inicialmente, mostremos que $|xH| = |H|, \ \forall x \in G$, ou seja, a cardinalidade da classe lateral à esquerda de H é igual à sua própria ordem. Seja $x \in G$, definimos ϕ tal que,

$$\begin{array}{rccc} \phi: & H & \longrightarrow & xH \\ & h & \longmapsto & xh \end{array}$$

Seja $y \in xH$, então $\exists h' \in H$ tal que $y = xh'$, e então $\phi(h') = y$, e portanto ϕ é sobrejetiva.

Agora, para $\phi(h) = \phi(h')$, tem-se $xh = xh'$, e multiplicando ambos os lados da igualdade à esquerda por x^{-1} teremos, $x^{-1}xh = x^{-1}xh' \implies eh = eh' \implies h = h'$, logo ϕ é injetiva, portanto, bijetiva, garantido $|xH| = |H|$.

Sejam $x_1, x_2, \ldots, x_n \in G$, com cada um dos x_i representando uma classe distinta, a saber, $\{x_1H, x_2H, \ldots, x_nH\}$, que como já vimos, designam partições e temos que $x_iH \cap x_jH = \varnothing$ para $i \neq j$, como já estabelecido, e então $G = x_1H \dot{\cup} x_2H \dot{\cup} \cdots \dot{\cup} x_nH$ (união disjunta), e portanto,

$$|G| = |x_1H| + |x_2H| + \cdots + |x_nH|$$

E de acordo com o que demostramos, $|x_iH| = |H|$, logo, $|G| = n \cdot |H|$, o que já demonstra que a ordem de H divide a ordem de G, já que $n \in \mathbb{N}$. E de acordo com a definição de índice, temos que $n = (G : H)$ e então, $|G| = |H|(G : H)$.

□

Proposição 1.16. *Sobre grupos finitos:*

i. A ordem de um elemento do grupo divide a ordem do grupo;

ii. Se $g \in G$, então $g^{|G|} = e$;

iii. Todo grupo de ordem p com p primo, é um grupo cíclico;

iv. Seja G um grupo e $K \leq H \leq G$ então $(G : K) = (G : H)(H : K)$;

v. Se G é abeliano suas classes laterais à esquerda e à direita são iguais;

vi. Se $|G| \leq 5$, então G é abeliano.

Demonstração. O leitor pode consultar [1], para os itens *i.*, *iii.*, *iv.* e *v.*; [3] para o item *ii*; e [2] para o item *vi*.

□

Um importante teorema que utiliza o Teorema de Lagrange em sua demonstração é o Teorema de Cauchy.

Teorema 1.17. *(Cauchy) Seja p um divisor primo da ordem de um grupo finito G. Então existe $g \in G$ tal que $o(g) = p$.*

Demonstração. Ver demonstração em [2]. □

1.5 Subgrupos Normais

Definição 1.18. Seja G um grupo e $H \leq G$, H será dito *subgrupo normal* de G, e denotamos por $H \trianglelefteq G$ se suas classes laterais à esquerda forem iguais à classes laterais à direita, ou seja, $gH = Hg, \forall g \in G$. Outra maneira de identificar um subgrupo normal é verificando se $gHg^{-1} = H, \forall g \in G$.

Exemplo 1.19.

i. Os subgrupos triviais de G, a saber $\{e\}$ e G, são subgrupos normais de G;

ii. $Z(G) \trianglelefteq G$. E dado $H \leq Z(G)$, então $H \trianglelefteq G$.

iii. O comutador de um grupo, G' é subgrupo normal de G.

iv. Se G é abeliano, então todos os seus subgrupos são normais. A recíproca em geral é falsa;

Definição 1.20. Se $G \neq \{e\}$ é um grupo e seus únicos subgrupos normais são os triviais, então dizemos que G é um *grupo simples*.

Vale ressaltar que os únicos grupos simples abelianos são os cíclicos de ordem prima.

Proposição 1.21. *Se um grupo finito G com $H \leq G$ é tal que $(G : H) = 2$, então $H \trianglelefteq G$.*

Demonstração. Ver demonstração em [1]. □

1.5.1 Grupo Quociente

Definição 1.22. Seja G um grupo e $H \trianglelefteq G$. O grupo de todas as classes laterais de H em G, com a operação de G, é chamado *grupo quociente* de G por H, e denotamos por G/H ou $\frac{G}{H}$.

Vale ressaltar que:

Lema 1.23. *Se G é um grupo finito e $H \trianglelefteq G$ então* $\left|\frac{G}{H}\right| = \frac{|G|}{|H|}$.

Demonstração. Das definições de grupo quociente e de índice, temos que,

$$\left|\frac{G}{H}\right| = (G : H).$$

Do Teorema de Lagrange (Teorema 1.15), temos

$$|G| = |H|(G : H) \Longrightarrow (G : H) = \frac{|G|}{|H|}.$$

Logo,

$$\left|\frac{G}{H}\right| = (G : H) = \frac{|G|}{|H|} \Longrightarrow \left|\frac{G}{H}\right| = \frac{|G|}{|H|}.$$

Como queríamos demonstrar.

□

Cabe observar que, se G é abeliano e $H \leq G$, seu grupo quociente $\frac{G}{H}$ será abeliano. Bem como se G é cíclico, o quociente será cíclico, e consequentemente abeliano.

1.6 Homomorfismos de Grupos

Definição 1.24. Sejam $(G, \cdot)$ e $(\mathcal{H}, \times)$ grupos e ψ uma função tal que $\psi : G \to \mathcal{H}$. Essa função ψ é chamada de *homomorfismo de G em H* se,

$$\psi(x \cdot y) = \psi(x) \times \psi(y), \ \forall x, y \in G.$$

Se ψ é um homomorfismo bijetivo, dizemos que ψ é um isomorfismo e denotamos por $G \simeq \mathcal{H}$. Se ψ é um homomorfismo de um grupo nele mesmo, chamamos de endomorfismo. E se o endormorfismo é bijetivo, dizemos que ele é um automorfismo, no caso do conjunto dos automorfismos de um grupo G, denotamos por $Aut\ G$.

O isomorfismo preserva a estrutura do grupo. E o automorfismo, além de preservar a estrutura do grupo, se o grupo for finito, ele apenas modifica a posição de seus elementos, ou seja, permuta-os.

Exemplo 1.25. Se G é um grupo e $H \trianglelefteq G$, a função $\varphi : G \to G/H$, $\varphi(g) = gH$ é um homomorfismo chamado *projeção canônica*.

Proposição 1.26. *Seja G um grupo finito e $H \trianglelefteq G$, onde $\frac{G}{H}$ é abeliano. Existem subgrupos $H_i \in G$ com $i \in \{0, 1, \ldots, m\}$ tais que $H = H_0 \subset H_1 \subset \cdots \subset H_m = G$, e $\frac{H_i}{H_{i-1}}$ é cíclico para todo $i \in \{1, \ldots, m\}$.*

Demonstração. Se $H_0 \neq G$, então $\exists \alpha_1 \in G$ tal que $\alpha_1 \notin H_0$. Então tomemos $H_1 = \langle \alpha_1 \rangle H_0$. Analogamente, se $H_1 \neq G$, então $\exists \alpha_2 \in G$ tal que $\alpha_2 \notin H_1$. Então tomemos $H_2 = \langle \alpha_2 \rangle H_1$.

Repetindo esse procedimento sucessivamente, sabemos que ele finda em algum momento, visto que G é finito, então:

$$\frac{H_i}{H_{i-1}} \simeq \langle \alpha_i \rangle$$

Para todo $i \in \{1, \ldots, m\}$, logo $\frac{H_i}{H_{i-1}}$ é cíclico.

□

Definição 1.27. Seja σ um homomorfismo, tal que $\sigma : G \longrightarrow J$. O conjunto $\operatorname{Ker}\sigma = \{x \in G; \sigma(x) = e_J\}$, onde e_J é o elemento neutro de J, é chamado núcleo de σ.

Teorema 1.28. *(Teorema dos isomorfismos)*

Sejam G e H grupos e seja $\sigma : G \longrightarrow H$ um homomorfismo. Seja ainda $N = \operatorname{Ker}(\sigma) \subset G$, o núcleo do homomorfismo σ. Então a aplicação:

$$\begin{array}{ccc} \frac{G}{N} & \longrightarrow & J = Im(\sigma) \\ gN & \longmapsto & \sigma(g) \end{array},$$

onde $Im(\sigma)$ é a imagem de σ, é um isomorfismo, e então, $\frac{G}{\operatorname{Ker}(\sigma)} \simeq H$.

Demonstração. Ver demonstração em [1]. □

Antes de citarmos um exemplo de isomorfismo entre grupos, lembremos do grupo $S_\triangle$, ele é definido análogo à definição usada no grupo $S_\square$, sobre um triângulo como o da figura 1.2:

Assim temos que $S_\triangle = \{e, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}, R_1, R_2, R_3\}$.

Agora vejamos um exemplo de isomorfismos, o grupo $S_\triangle$ e o grupo S_3 são isomorfos, vejamos a bijeção φ:

$$\varphi : S_3 \to S_\triangle$$
$$e \mapsto e$$
$$\beta \mapsto R_{\frac{2\pi}{3}}$$

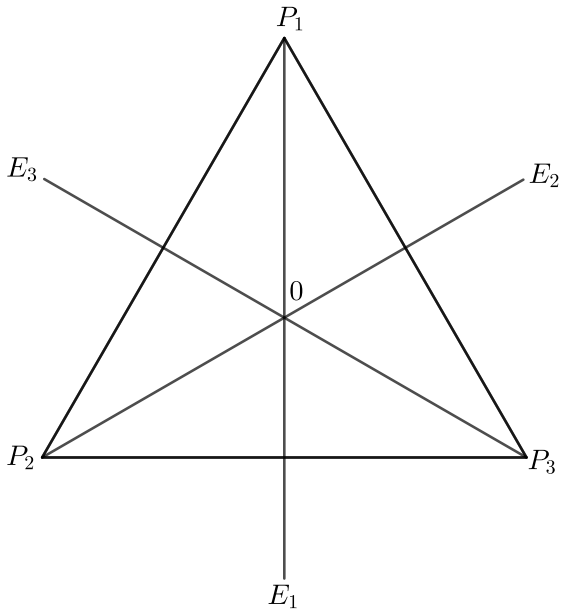

Figura 1.2: Triângulo $P_1P_2P_3$

$$\beta^2 \mapsto, R_{\frac{4\pi}{3}}$$
$$\alpha \mapsto R_3$$
$$\beta\alpha \mapsto R_2$$
$$\alpha\beta \mapsto R_1$$

Notemos que: $\varphi(\alpha \circ \beta^2) = \varphi(\beta\alpha) = R_2 = R_3 \circ R_{\frac{4\pi}{3}} = \varphi(\alpha) \circ \varphi(\beta^2)$. De modo análogo, fazemos o mesmo procedimento com o demais elementos de S_3, garantindo que a condição de homomorfismo é satisfeita, e claramente, pela própria definição, φ é bijetiva, portanto temos mesmo um isomorfismo, e então $S_3 \simeq S_\triangle$.

Um teorema muito importante pra nosso objetivo, é o *Teorema de Cayley*, antes de provarmos, vejamos a seguinte proposição:

Proposição 1.29. *Se G é um grupo, então* $\operatorname{Aut} G$ *é também um grupo com a operação composição de funções.*

Demonstração. Devemos mostrar que a operação composição de funções está bem definida e satisfaz as propriedades: associatividade, existência do elemento neutro e existência do elemento inverso.

Sejam $\sigma, \psi, \iota \in \operatorname{Aut} G$, então, da definição de automorfismo,

$$(\sigma \circ \psi)(x) = \sigma(\psi(x)) = \sigma(y), \text{ para } \psi(x) = y, \text{ tal que } x, y \in G$$

Ou seja, a composição de automorfismos é também um automorfismo, garantindo que a operação está bem definida.

Para garantir a associatividade devemos ter:

$$[\iota \circ (\sigma \circ \psi)](x) = [(\iota \circ \sigma) \circ \psi](x).$$

Usando a definição de automorfismo,

$$[\iota \circ (\sigma \circ \psi)](x) = \iota(x) \circ (\sigma \circ \psi)(x) = \iota(x) \circ \sigma(x) \circ \psi(x) = (\iota \circ \sigma)(x) \circ \psi(x) = [(\iota \circ \sigma) \circ \psi](x)$$

Agora, seja $\epsilon \in Aut\ G$ tal que $\epsilon(x) = x$, para todo $x \in G$, chamamos ϵ de identidade de $Aut\ G$, e como,

$$(\sigma \circ \epsilon)(x) = \sigma(\epsilon(x)) = \sigma(x)$$

e

$$(\epsilon \circ \sigma)(x) = \epsilon(\sigma(x)) = \sigma(x)$$

Temos que ϵ é o elemento neutro de $Aut\ G$.

Por fim, como o automorfismo é um isomorfismo, é portanto bijetivo, garantindo a existência do elemento inverso, finalizando assim nossa demonstração.

□

Teorema 1.30. *(Teorema de Cayley)*

Se G é um grupo tal que $|G| = n$ então G é isomorfo a um subgrupo de S_n.

Demonstração. Seja $g \in G$, definimos a aplicação σ_g de G em G como sendo:

$$\sigma_g(x) = gx,\ \forall x \in G$$

Notemos que, pela própria definição, σ_g é sobrejetiva. Sejam $x, y \in G$, para $\sigma_g(x) = \sigma_g(y)$, teremos $gx = gy \Longrightarrow x = y$, logo σ_g é injetiva e portanto bijetiva. Da definição de grupo das permutações vista no item *vii.* da seção 1.1.2, concluímos que $\sigma_g \in S(G)$, onde $S(G)$ é o grupo das permutações dos elementos de G.

Definimos agora a aplicação φ de G em $S(G)$, como sendo:

$$\varphi(g) = \sigma_g,\ \forall g \in G$$

Precisamos mostrar que φ é um homomorfismo injetor. Seja $a, b \in G$, temos que $\varphi(a \cdot b) = \sigma_{a \cdot b}$ e para $x \in G$ teremos:

$$\sigma_{a \cdot b}(x) = (a \cdot b)\ x = a\ (b \cdot x) = \sigma_a(b \cdot x) = \sigma_a(\sigma_b(x)) = \sigma_a \circ \sigma_b(x)$$

Logo,

$$\varphi(a \cdot b) = \sigma_a \circ \sigma_b = \varphi(a) \circ \varphi(b)$$

Assim mostramos que φ é um homomorfismo. Resta mostrar que este é injetivo. Para $\varphi(a) = \varphi(b)$ teremos $\sigma_a = \sigma_b$ e aplicando σ num dado $x \in G$ tem-se

$$\sigma_a(x) = \sigma_b(x) \Longrightarrow a \cdot x = b \cdot x \Longrightarrow a = b,$$

logo φ é um homomorfismo injetor. E dessa informação segue que G é isomorfo à um subgrupo de $S(G)$.

Por fim, para $|G| = n$ temos que $S(G) = S_n$, ou seja, G é isomorfo à um subgrupo de S_n, como queríamos demonstrar.

□

Exemplo 1.31. Vamos procurar todos os automorfismos de S_3.

Seja τ um automorfismo de S_3, então determinemos $\tau(\alpha)$ e $\tau(\beta)$. Assim para que a estrutura seja mantida, é necessário que $\tau(\alpha)$ tenha a mesma ordem de α, que nesse caso é 2, e da mesma forma $\tau(\beta)$ deve ter a mesma ordem de β, nesse caso 3. Calculando a ordem de cada termo de S_3 (omitimos tais cálculos), concluímos que, $\tau(\alpha)$ será α, $\alpha\beta$ ou $\beta\alpha = \alpha\beta^2$, enquanto que $\tau(\beta)$ será β ou β^2. Assim:

$$AutS_3 = \{\tau_{ij} : S_3 \to S_3; \tau_{ij}(e) = e, \tau_{ij}(\beta) = \beta^i, \tau_{ij}(\alpha) = \alpha\beta^j, \forall i \in \{1,2\} \text{ e } j \in \{0,1,2\}\}$$

Concluímos então que existem 6 automorfismos de S_3, são eles: de $\tau_{10}, \tau_{11}, \tau_{12}, \tau_{20}, \tau_{21}$ e τ_{22}. Não mostraremos todos detalhadamente, mas a título de exemplo, vejamos o que acontece com um desses automorfismo, τ_{12}.

Em τ_{12}, temos que $\tau_{12}(e) = e$, $\tau_{12}(\beta) = \beta$ e $\tau_{12}(\alpha) = \alpha\beta^2 = \beta\alpha$, então:

$$\begin{gathered}
\tau_{12} : S_3 \to S_3 \\
\tau_{12}(e) = e \\
\tau_{12}(\alpha\beta) = \tau_{12}(\alpha) \circ \tau_{12}(\beta) = \beta\alpha \circ \beta = \alpha \\
\tau_{12}(\alpha) = \beta\alpha \\
\tau_{12}(\beta) = \beta \\
\tau_{12}(\beta^2) = \tau_{12}(\beta) \circ \tau_{12}(\beta) = \beta \circ \beta = \beta^2 \\
\tau_{12}(\beta\alpha) = \tau_{12}(\beta) \circ \tau_{12}(\alpha) = \beta \circ \beta\alpha = \alpha\beta
\end{gathered}$$

Como esperado, τ_{12} é bijetivo, então, apenas permuta os 6 elementos de S_3.

1.7 Representação de Grupos através do grupo das permutações

Como vimos no teorema 1.30, qualquer grupo finito pode ser representado por um subgrupo de um grupo de permutações, e por isso, o grupo S_n merece uma atenção maior.

Na seção 1.1.3 já introduzimos as noções básicas do S_n, vejamos um pouco mais sobre esse grupo.

Considere o grupo de permutações S_3, com a notação apresentada na seção 1.1.3, podemos dizer que esse grupo é gerado pelo terceiro e quarto elemento, vale ressaltar que o conceito de geradores foi tratado na seção 1.3. São eles:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ e } \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

O elemento $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ indica as seguintes trocas de posições: a posição 1 foi para a posição 2, a 2 foi para a 1 e a 3 permaneceu inalterada. Focando apenas nas alterações temos $1 \to 2 \to 1$. De modo análogo, em $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ tem-se que $1 \to 2 \to 3 \to 1$.

Pensando numa composição: $\alpha\beta$, por exemplo, o processo é analisar posição por posição, aplicando inicialmente β depois α, e então: $1 \to 2 \to 1$, logo a posição 1 se manterá inalterada; $2 \to 3 \to 3$, ou seja $2 \to 3$; e $3 \to 1 \to 2$, ou seja $3 \to 2$. Conclusão: $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, logo $2 \to 3 \to 2$.

Com base nessa descrição, podemos usar uma outra forma de representação, a *representação via ciclos*. Tal representação pode ser feita da seguinte maneira:

Em β temos $1 \to 2 \to 3 \to 1$, via ciclos representamos $\beta = (123)$, e lemos, "A posição 1 vai para a 2 que por sua vez vai para a 3 que retorna para a 1". De modo análogo $\alpha = (12)$.

Vejamos outro exemplo, seja $s \in S_6$, tal que $s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$, representando via ciclos teremos, $s = (12)(456)$.

Agora, vejamos como operar com ciclos. Em $\alpha\beta = (12) \circ (123)$, iniciando por β, temos: $1 \to 2 \to 1$, note que é similar ao que já fizemos, e então:

$$\alpha\beta = (12) \circ (123) = (23)$$

De modo análogo, executando as operações de composição de funções entre α e β, determinamos todos os elementos de S_3:

$$\alpha^2 = (12) \circ (12) = e, \text{ onde } e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix};$$

$$\beta^2 = (123) \circ (123) = (132), \text{ logo } \beta^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix};$$

$$\beta^3 = \beta^2\beta = (132) \circ (123) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e;$$

$$\alpha\beta = (12) \circ (123) = (23), \text{ logo } \alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix};$$

$$\beta\alpha = (123) \circ (12) = (13), \text{ logo } \beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix};$$

$$\alpha\beta^2 = (12) \circ (132) = (13) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \beta\alpha;$$
$$\beta^2\alpha = (132) \circ (12) = (23) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \alpha\beta.$$

Dessa forma, confirmamos que α e β geram o S_3. E podemos reescrever S_3, como sendo $S_3 = \{e, \alpha\beta, \alpha, \beta, \beta^2, \beta\alpha\}$, onde e é o elemento neutro do grupo.

Definição 1.32. A ordem de um ciclo $(1, 2, ..., m)$ é dada pela quantidade m de termos, e falamos em m-ciclo. Se $m = 2$, teremos um 2-ciclo, mais comumente chamado de transposição.

Exemplo 1.33. Falamos que $\alpha = (12)$ é um uma transposição, e $\beta = (123)$ é um 3-ciclo. Já $s = (12)(456)$ não é um m-ciclo, qualquer que seja m.

Definição 1.34. Duas permutações são ditas disjuntas se ambas não movem um mesmo termo, caso contrário, é dito não-disjuntas.

Exemplo 1.35. Seja $a, b, c \in S_9$, tal que $a = (134)(68)$, $b = (59)$ e $c = (245)$, então a e b são disjuntas, já a e c não são, pois ambas movem o 4, assim como b e c que ambas movem o 5.

À cerca da representação via ciclos, vale salientar algumas importantes proposições:

Proposição 1.36. *Toda permutação é o produto de ciclos disjuntos de ordem ≥ 2; tal ordem é única a menos da ordem dos fatores.*

Demonstração. Ver demonstração em [1]. □

Proposição 1.37. *i. Todo elemento de S_n é um produto de transposições;*

ii. $S_n = \langle (12), (13), \dots (1n), \rangle$;

iii. $S_n = \langle (12), (23), \dots, (n-1\ n) \rangle$.

Demonstração. O leitor pode consultar a demonstração em [1]. □

Exemplo 1.38. Quanto ao item $i.$, podemos escrever $\beta = (123)$ como $\beta = (13)(12)$.

Proposição 1.39. *Os ciclos* (12) *e* $(12...n)$ *geram o grupo S_n.*

Demonstração. Ver demonstração em [2]. □

1.7.1 Analisando S_3

De modo a exemplificar algumas definições já vistas, como as de ordem de um grupo, subgrupos, grupo quociente, classes laterais e grupos normais, analisaremos o grupo S_3.

Sendo $S_3 = \{e, \alpha\beta, \alpha, \beta, \beta^2, \beta\alpha\}$, onde $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ e $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Temos que $|S_3| = 6$, logo seus subgrupos devem ter ordem n tal que n divide $|S_3|$, ou seja, eles terão ordens, $1, 2, 3$ ou 6.

Com ordem 1 e 6, temos os subgrupos triviais, respectivamente $\{e\}$ e S_3.

Para os subgrupos de ordem 2, sabemos que obrigatoriamente, um dos elementos é o e e o outro, pra que sejam satisfeitas as condições para ser grupo, deve ser um elemento a tal que seu elemento inverso seja ele próprio. Vejamos:

$\alpha\beta \circ \alpha\beta = e$,

$\alpha \circ \alpha = e$,

$\beta \circ \beta = \beta^2 \neq e$,

$\beta^2 \circ \beta^2 = \beta \neq e$,

$\beta\alpha \circ \beta\alpha = e$

Logo os subgrupos de S_3 com 2 elementos são $\{e, \alpha\beta\}$, $\{e, \alpha\}$ e $\{e, \beta\alpha\}$.

Quanto aos subgrupos de ordem 3, do item *iii* da proposição 1.16, temos que ele será cíclico, logo $\{e, a, a^2\}$ com $a^3 = e$, e facilmente notamos que $a = \beta$ e então o único subgrupo de S_3 de ordem 3 será: $\{e, \beta, \beta^2\}$.

Por fim, temos que os subgrupos de S_3 são: $H_1 = \{e\}; H_2 = \{e, \alpha\beta\}; H_3 = \{e, \alpha\}; H_4 = \{e, \beta\alpha\}; H_5 = \{e, \beta, \beta^2\}$; e $H_6 = S_3$.

Vejamos agora quais deles são subgrupos normais:

Como vimos no exemplo (i) de 1.19, H_1 e H_6 são subgrupos normais triviais. Do teorema 1.21, concluímos que $H_5 \trianglelefteq S_3$. Resta verificarmos os demais. Vejamos.

Temos que $|S_3 : H_i|$ com $i = 2, 3, 4$ é tal que $|S_3 : H_i| = |S_3|/|H_i| = 6/2 = 3$, logo H_i possui 3 classes laterais em S_3. Analisando H_2:

$eH = \alpha\beta H = \{e, \alpha\beta\}$

$\alpha H = \beta H = \{\alpha, \beta\}$

$\beta^2 H = \beta\alpha H = \{\beta^2, \beta\alpha\}$

Portanto as classes laterais serão: $\{\{e, \alpha\beta\}, \{\alpha, \beta\}, \{\beta^2, \beta\alpha\}\}$.

Agora vejamos:

$eH = \{e, \alpha\beta\} = He$

$\alpha H = \{\alpha, \beta\} \neq H\alpha = \{\alpha, \beta^2\}$

Nem precisamos continuar a verificar, já podemos afirmar que H_2 não é subgrupo normal de S_3.

De modo análogo, constatamos que H_3 e H_4 também não são normais. Portanto os subgrupos normais de S_3 são $H_1 = \{e\}; H_5 = \{e, \beta, \beta^2\}$; e $H_6 = S_3$.

1.7.2 O Subgrupo A_n de S_n

No estudo do grupo das permutações, não podemos deixar de chamar atenção pra um importante subgrupo, o chamado *grupo das permutações pares* ou *grupo alternante*. No entanto, devemos saber o que vem a ser uma permutação par ou ímpar, vejamos:

Definição 1.40. Uma permutação que pode ser escrita com uma quantidade par de transposições é dita, permutação par. Caso contrário, será uma permutação ímpar.

Vejamos alguns resultados frutos desta definição:

i. O produto de duas permutações pares será par;

ii. O produto de uma permutação par com uma ímpar (ou vice-versa) será ímpar;

iii. O produto de duas permutações ímpares será par.

Agora, reconhecendo uma permutação par, podemos definir o grupo alternante:

Definição 1.41. Seja S_n o grupo das permutações de n elementos, o subconjunto de S_n formado pelas permutações pares formam um grupo, denominado grupo alternante ou grupo das permutações pares, e denotamos por A_n, e então $A_n \leq S_n$.

O subgrupo A_n se faz muito importante para o futuro estudo dos chamados grupos solúveis. Vejamos uma importante proposição:

Proposição 1.42. *A_n é um subgrupo de S_n de índice 2, e como $|S_n| = n!$ então $|A_n| = \frac{n!}{2}$. E mais, temos que $A_n \trianglelefteq S_n$*

Demonstração. Sejam $\gamma,\ \eta \in A_n$, logo γ e η, são permutações pares. Da proposição 1.4, para mostrar que $A_n \leq S_n$, mostremos que $\gamma \circ \eta \in A_n$ e também $\eta^{-1} \in A_n$.

Do item (i) da definição 1.40, segue que o produto entre permutações pares será par, logo $\gamma \circ \eta \in A_n$.

Do item (i) da Proposição 1.37, sabemos que η é uma composição de transposições, então podemos escrever

$$\eta = (a_1 a_2)(a_3 a_4) \cdots (a_{n-1} a_n)$$

E sua inversa será

$$\eta^{-1} = (a_{n-1} a_n)^{-1} \cdots (a_3 a_4)^{-1} (a_1 a_2)^{-1}$$

Como a inversa de uma transposição é ela mesma, segue que

$$\eta^{-1} = (a_{n-1} a_n) \cdots (a_3 a_4)(a_1 a_2)$$

Mantendo assim a paridade, e portanto o inverso de uma permutação par é também par, ou seja, $\eta^{-1} \in A_n$ Enfim, provamos que $A_n \leq S_n$.

Sejam r a quantidade de permutações pares e s as de permutações ímpares de S_n. Seja ainda τ uma transposição de S_n, logo τ é ímpar.

Multiplicando τ por todas as permutações ímpares, de acordo com o resultado (iii) da Definição 1.40, obteremos permutações pares, logo $r \geq s$.

Analogamente, multiplicando τ por todas as permutações pares, de acordo com o resultado (ii) da Definição 1.40, obtemos permutações ímpares, logo $s \geq r$.

Como $r \geq s$ e $s \geq r$, então $r = s$. Assim $|S_n| = n! = r + s = 2r$, e portanto $|A_n| = r = \dfrac{n!}{2}$, consequentemente $(S_n : A_n) = 2$. E por fim, segue do Teorema 1.21 que $A_n \trianglelefteq S_n$.

□

Agora, sobre o A_n, podemos destacar uns importantes resultados.

Proposição 1.43. *O grupo A_n é um grupo simples para $n = 3$ e $n \geq 5$.*

Demonstração. Ver demonstração em [1]. □

Aproveitemos a oportunidade para definir o *grupo de Klein.*

Definição 1.44. Chamamos de grupo de Klein e denotamos por K, o subgrupo de S_4, tal que $K = \{e, (12)(34), (13)(24), (14)(23)\}$.

E agora, em posse de tal definição, vejamos a seguinte proposição:

Proposição 1.45. *Para $n = 4$, S_n tem como únicos subgrupos normais: $\{e\}$, K, A_n e S_n. E para $n = 3$ e $n \geq 5$ os únicos subgrupos normais são $\{e\}$, A_n e S_n.*

Demonstração. Consultar demonstração em [1]. □

1.8 Grupos solúveis

Antes de definir o que vem a ser um grupo solúvel, é importante destacarmos que esse é o principal subtema da Teoria de Grupos necessário ao tema do nosso trabalho, obviamente não podemos desmerecer os demais.

Definição 1.46. Um grupo G se diz *solúvel* se for possível construir uma subsérie normal, a saber:

$$e = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq ... \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

E ainda os grupos quocientes G_i/G_{i-1} forem abelianos, com $i \in \{1, 2, \ldots, n\}$.

Proposição 1.47. *i. Todo subgrupo de um grupo solúvel, é solúvel;*

ii. Todo quociente de um grupo solúvel é também solúvel;

iii. Seja G um grupo e $N \trianglelefteq G$, se G/N e N são solúveis então G é solúvel.

Demonstração. A demonstração o leitor pode ver em [2]. □

Exemplo 1.48. i. Todo grupo abeliano é solúvel;

ii. Todo p-grupo finito, com p primo, é solúvel;

iii. Todo grupo simples não-abeliano não é solúvel, em particular A_n é não solúvel para $n \geq 5$;

Eis algumas importantes conclusões sobre solubilidade de grupos:

Proposição 1.49. *i. O grupo S_n é solúvel para $n = 1, 2, 3, 4$;*

ii. O grupo S_n, $n \geq 5$ não é solúvel.

Demonstração. *i.* Para $n = 1$, $S_1 = \{e\}$, que é obviamente abeliano, e consequentemente solúvel, como vimos na item (i) do Exemplo 1.48;

Para $n = 2$, temos que $|S_2| = 2$, e do item *vi.* da proposição 1.16, temos que S_2 é abeliano, logo solúvel de acordo com o item *i.* do exemplo 1.48;

Para $n = 3$, temos que S_3 não é abeliano, mas, relembremos da análise que fizemos na seção 1.7.1 do grupo S_3, onde inclusive, determinamos seus subgrupos normais, podemos aplicar a definição de grupos solúveis, pensando na cadeia $\{e\} \trianglelefteq A_3 \trianglelefteq S_3$, onde o A_3 é o grupo das permutações pares de S_3 e é equivalente ao que chamamos de H_5. Notemos que $\left|\frac{S_3}{A_3}\right| = 2$ e $\left|\frac{A_3}{\{e\}}\right| = 3$, portanto ambos abelianos e então S_3 é solúvel;

Para $n = 4$, antes o leitor deve relembrar dois subgrupos normais de S_4, o subgrupo de Klein, K e o subgrupo das permutações pares A_4, que foi apresentado na seção 1.7.2. Tem-se que $|A_4| = 12$ e $|K| = 4$, portanto $\left|\frac{S_4}{A_4}\right| = 2$, $\left|\frac{A_4}{K}\right| = 3$ e $\left|\frac{K}{\{e\}}\right| = 4$, e então temos a seguinte subsérie normal: $\{e\} \trianglelefteq K \trianglelefteq A_4 \trianglelefteq S_4$, com quocientes abelianos, concluindo então que S_4 é solúvel.

ii. Como visto na proposição 1.45, o único subgrupo normal de S_n, para $n \geq 5$ é o A_n, que como vimos na Proposição 1.43 é simples, e do item *iii.* do Exemplo 1.48, é não solúvel. Por fim do item *i.* da Proposição 1.47, conclui-se que S_n é não solúvel para $n \geq 5$.

□

Capítulo 2

Anéis

Nesse capítulo nos apropriaremos da estrutura algébrica essencial ao nosso estudo, os *Anéis*. O estudo de anéis se faz essencial para o posterior estudo de anéis de polinômios, objeto importante no nosso tema central, bem como o estudo de corpo, um vez que é no corpo que encontraremos as soluções das equações polinomiais.

Definição 2.1. Uma estrutura algébrica formada por um conjunto não vazio, digamos A, munido de duas operações, a adição e a multiplicação, assim definidas:

$$\begin{array}{rccc} + : & A \times A & \to & A \\ & (a,b) & \mapsto & a+b \end{array} \qquad \begin{array}{rccc} \cdot : & A \times A & \to & A \\ & (a,b) & \mapsto & a \cdot b \end{array}$$

E que satisfaz as seguintes propriedades:

i. É associativa para adição, ou seja, $\forall a, b, c \in A$,

$(a+b)+c = a+(b+c)$;

ii. Possui elemento neutro da adição, ou seja, $\forall a \in A$,

$\exists\ 0 \in A$ tal que $a+0 = 0+a = a$;

iii. Possui elemento inverso da adição, ou seja, $\forall a \in A$,

$\exists\ b \in A$ tal que $a+b = b+a = 0$;

Convencionamos que o inverso aditivo de a é $-a$.

iv. É comutativa para adição, ou seja, $\forall a, b \in A$,

$a+b = b+a$;

v. É associativa para multiplicação, ou seja, $\forall a, b, c \in A$,

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

vi. A multiplicação é distributiva em relação à adição, ou seja, $\forall a, b, c \in A$,

$a \cdot (b+c) = a \cdot b + a \cdot c$, e

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

Tal estrutura é denominada *anel*, denotamos, $(A, +, \cdot)$.

Se o anel possui o elemento neutro da multiplicação, a saber 1, chamamos de *anel com unidade*, ou seja,

vii. $\exists\ 1 \in A$, tal que $a \cdot 1 = 1 \cdot a = a, \forall a \in A$.

Se o anel é comutativo para multiplicação, chamamos de *anel comutativo*, ou seja,

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

E será chamado de *anel sem divisores de zero*, se satisfaz,

ix. Dados $a, b \in A, a \cdot b = 0 \Rightarrow a = 0$ ou $b = 0$.

Definição 2.2. Pensemos num anel que seja, simultaneamente comutativo, com unidade e sem divisores de zero, chamamos essa nova estrutura de *domínio de integridade*.

Definição 2.3. Agora, se acrescentarmos ao domínio de integridade a propriedade:

x. Para todo $a \in A - \{0\}, \exists\ b \in A, a \cdot b = b \cdot a = 1$.

Chamamos b de inverso multiplicativo de a, e mais comumente representaremos por a^{-1}, e dizemos que a é inversível.

Teremos a estrutura denominada *corpo*, na qual nos concentraremos em nosso trabalho.

Diante de tais definições, são exemplos de domínio: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$, consequentemente de anel. Destes, são corpos: $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$. Outro exemplo de corpo é o $\mathbb{Z}_n$ com n primo.

Definição 2.4. A característica de um anel, é o menor número $n \in \mathbb{N}$ tal que $\underbrace{x + x + \cdots + x}_{n\text{vezes}} = 0$ para algum x pertencente ao anel e $x \neq 0$. Caso esse número não exista, diremos que o anel tem *característica zero*.

Exemplo 2.5. Os corpos $\mathbb{Q}$ e $\mathbb{C}$ são corpos de característica zero, já $\mathbb{Z}_n$ é um exemplo de corpo de característica n, se n for primo.

Vale ressaltar que essa definição pode, obviamente, ser levada para o corpo, uma vez que um corpo é também um anel.

2.1 Anel de Polinômios

Como já deixamos claro, é de nosso interesse encontrar as soluções de uma equação polinomial, e obviamente, só se faz sentido falar em equações polinomiais depois de conhecer os *polinômios*, ou mais geral, *o anel dos polinômios*.

Definição 2.6. Seja $\mathbb{K}$ um corpo, chamamos de anel de polinômios sobre $\mathbb{K}$ na indeterminada x, e representamos por $\mathbb{K}[x]$ o conjunto de todos os polinômios na indeterminada x, que definiremos mais adiante em 2.7.

2.1.1 Polinômios de uma única variável

Veremos aqui a definição de polinômios, elementos do anel de polinômios, e algumas informações relevante ao nosso estudo, uma vez que trataremos de equações polinomiais. Importante falar que apesar de o estudo de polinômio abordar os de várias variáreis, aqui nos deteremos aos de uma única variável.

Definição 2.7. Seja $a_1, a_2, \ldots, a_n \in \mathbb{K}$, onde $\mathbb{K}$ é um corpo, chamamos de *polinômio sobre* $\mathbb{K}$ *em uma indeterminada* x a expressão:

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \tag{2.1}$$

ou ainda:

$$p(x) = \sum_{i=0}^{n} a_i x^i.$$

Dados dois polinômios:

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

e

$$q(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$$

Eles são ditos *iguais*, se $m = n$ e $a_i = b_i, \forall i \in \mathbb{N}$. Caso, em $p(x)$ todos os $a_i = 0$, dizemos que $p(x)$ é um *polinômio nulo.*

Qualquer que seja $a \in \mathbb{K}$, podemos indicar a pelo polinômio $p(x)$, onde $a_0 = a$ e $a_i = 0, \forall i \geq 1$, e o chamamos de *polinômio constante a.* Dessa forma, qualquer número a pode ser expresso como polinômio, na verdade, como um polinômio constante. E assim também podemos considerar que $\mathbb{K} \subset \mathbb{K}[x]$.

Definição 2.8. Seja $p(x)$ um polinômio como em (2.1), se $a_n \neq 0$, dizemos que *o grau do polinômio* $p(x)$ é n, e denotamos por $\partial p(x) = n$, ou seja, o grau de um polinômio é dado pela maior potência de sua indeterminada. E o grau será zero se o polinômio for constante.

Como já dito, o conjunto de todos os $p(x)$ com coeficientes em $\mathbb{K}$ chamamos de anel de polinômios, denotado por $\mathbb{K}[x]$. E então sua soma e produto devem ser bem definidas:

Sejam:

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

e

$$q(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$$

Ambos pertencentes à $\mathbb{K}[x]$, temos que, para adição:

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

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

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

onde $c_0 = a_0 b_0,\ c_1 = a_0 b_1 + a_1 b_0,\ c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0, \ldots, c_j = a_0 b_j + a_1 b_{j-1} + ... + a_{j-1} b_1 + a_j b_0, j \in \mathbb{N}$.

E por ser um anel, tem garantida todas as propriedades descrita no capítulo anterior. E mais, $\mathbb{K}[x]$ é um domínio de integridade, não se caracterizando como corpo por não ter todos seus elementos inversíveis. Na verdade, os únicos polinômios inversíveis de $\mathbb{K}[x]$ são os polinômios constantes e não nulos.

Quanto ao grau do polinômio resultante da adição ou multiplicação, temos que:

$$\partial(p(x) + q(x)) \leq \max\{\partial p(x), \partial q(x)\} = \max(m, n), \forall p(x), q(x) \in \mathbb{K}[x]$$

$$\partial(p(x) \cdot q(x)) = \partial p(x) + \partial q(x) = n + m, \forall p(x), q(x) \neq 0$$

Sejam $f(x), g(x) \in \mathbb{K}[x]$, dizemos que $f(x)$ divide $g(x)$ se $\exists h(x)$ tal que,

$$g(x) = f(x) \cdot h(x)$$

e denotamos por $f(x) \mid g(x)$. Dizemos também que $f(x)$ é divisor de $g(x)$ ou que $g(x)$ é divisível por $f(x)$. Caso contrário, teremos $f(x) \nmid g(x)$.

Exemplo 2.9. Dados os polinômios $f(x) = x - 1$ e $g(x) = x^2 - 1$, podemos afirmar que $f(x) \mid g(x)$, uma vez que $g(x) = (x - 1)(x + 1)$.

Definição 2.10. Dados dois polinômios $p(x), q(x) \in \mathbb{K}[x]$, definimos o máximo divisor comum (ou maior fator comum), como sendo o polinômio $d(x) \in \mathbb{K}[x]$ tal que $d(x) \mid p(x)$ e $d(x) \mid q(x)$, e denotamos por $\text{mdc}(p(x), q(x)) = d(x)$, e além disso, se existir um polinômio $e(x) \in \mathbb{K}[x]$ tal que $e(x) \mid p(x)$ e $e(x) \mid q(x)$, então $e(x) \mid d(x)$.

Vale ressaltar que sempre existirá esse polinômio $d(x)$, na pior das hipóteses ele será o polinômio constante $d(x) = 1$, e nesse caso, dizemos que $f(x)$ e $g(x)$ são coprimos, ou seja, não possuem fator comum, e denotamos por $\text{mdc}(p(x), q(x)) = 1$.

O domínio de polinômios $\mathbb{K}[x]$ é dito um *domínio Euclidiano*, pois obedece o *algoritmo da divisão* .

Teorema 2.11. *(Algoritmo da Divisão)*
Sejam $f(x), g(x) \in \mathbb{K}[x]$ e $g(x) \neq 0$, existem únicos $q(x), r(x) \in \mathbb{K}[x]$ tais que,

$$f(x) = q(x) \cdot g(x) + r(x)$$

onde $r(x) = 0$ ou $\partial r(x) < \partial g(x)$.

Demonstração. Ver demonstração em [2]. □

Definição 2.12. Chamamos de polinômio *mônico*, o polinômio $p(x)$ como em (2.1), onde $a_n = 1$.

Notemos que por tratarmos de polinômios sobre um corpo, sempre que $p(x)$ não for mônico, podemos multiplicá-lo pelo inverso multiplicativo de a_n, desta forma, passamos a ter um polinômio mônico, que mais adiante veremos ser importante nos nossos estudos.

Definição 2.13. Seja $p(x) \in \mathbb{K}[x]$, com $\mathbb{K}$ corpo, dizemos que $p(x)$ é *irredutível* sobre $\mathbb{K}[x]$ se não existirem $r(x), s(x) \in \mathbb{K}[x]$, com $\partial r(x), \partial s(x) < \partial p(x)$ tal que $p(x) = r(x).s(x)$, caso contrário, $p(x)$ será dito *redutível*.

Podemos associar a ideia de irredutibilidade de polinômios à ideia de números primos assim o polinômio irredutível está para os polinômios como os números primos estão para números inteiros.

Exemplo 2.14. O polinômio $p(x) = x^2 - 1$ é redutível sobre $\mathbb{R}$, pois $p(x) = (x-1)\cdot(x+1)$, ou seja, $p(x)$ é escrito como produto de polinômios de grau menores que o seu. Já $q(x) = x^2 + 1$ é irredutível sobre $\mathbb{R}$, uma vez que $q(x)$ não pode ser reescrito como produto entre polinômios de graus menores. Vale salientar que todo polinômio sobre $\mathbb{K}[x]$ de grau 1 é irredutível.

Teorema 2.15. *Seja $f(x) \in \mathbb{K}[x]$, como $\mathbb{K}$ é um corpo, então $f(x)$ pode ser escrito na forma:*

$$f(x) = a \cdot p_1(x) \cdots p_m(x),$$

onde $a \in \mathbb{K}$, com $a \neq 0$ e $p_1(x), p_2(x), \ldots, p_m(x)$ são polinômios irredutíveis sobre $\mathbb{K}$, não necessariamente distintos. Essa expressão é única a menos da ordem dos $p_1(x), p_2(x), \ldots, p_m(x)$. Portanto dizemos que essa fatoração é única.

Demonstração. Ver demonstração em [2]. □

Definição 2.16. Dado $p(x) \in \mathbb{K}[x]$ e não nulo, com $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, dizemos que $\alpha \in \mathbb{L}$, tal que $\mathbb{K} \subset \mathbb{L}$, é raiz de $p(x)$ se $p(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$.

Teorema 2.17. *Seja $p(x) \in \mathbb{K}[x]$, com $\partial p(x) = n$, então, $p(x)$ tem no máximo n raízes em $\mathbb{K}$.*

Demonstração. Ver demonstração em [3]. □

Exemplo 2.18. Por exemplo, $q(x) = x^2 - 1$ possui duas raízes em $\mathbb{R}$, já $p(x) = x^2 + 1$ não possui nenhuma raiz em $\mathbb{R}$, porém possui duas raízes no corpo $\mathbb{C}$, com $\mathbb{R} \subset \mathbb{C}$.

Na verdade podemos afirmar que $p(x)$ tem no máximo n raízes em qualquer corpo que contenha o corpo $\mathbb{K}$.

Seja $f(x) \in \mathbb{K}[x]$, onde $\partial f(x) = n$, se $f(x)$ for redutível de modo que seja escrito como produto entre polinômios mônicos de grau um, ou seja,

$$f(x) = a(x - \alpha_1) \cdot (x - \alpha_2) \cdots (x - \alpha_n)$$

com $a \in \mathbb{K}$, diremos que $\alpha_1, \alpha_2, \ldots, \alpha_n$ são as n raízes de $f(x)$, podendo cada termo $(x - \alpha_i)$ aparecer mais de uma vez. Se ocorrer, por exemplo, $f(x) = (x - \alpha_1)^2 \cdot (x - \alpha_2)^3$, diremos que $f(x)$ tem duas raízes iguais a α_1 e três iguais a α_2.

Definição 2.19. A quantidade de vezes que um mesmo α_i é raiz de $f(x)$ é chamada de *multiplicidade da raiz*

Em $f(x) = (x - \alpha_1)^2 \cdot (x - \alpha_2)^3$, α_1 tem multiplicidade 2 e α_2 tem multiplicidade 3.

Como trabalharemos em corpos de característica zero, que definimos anteriormente, podemos afirmar que todos os polinômios irredutíveis desse corpo é dito *polinômio separável* (para mais detalhes, o leitor pode consultar [6]).

Definição 2.20. Chamamos de polinômio separável, todo polinômio cujas raízes tem multiplicidade um, ditas *raízes simples*.

Sobre tal definição, vejamos a seguinte proposição, que requer do leitor o conhecimento prévio sobre derivadas de funções polinomiais:

Proposição 2.21. *Seja $f(x) \in \mathbb{K}[x]$, onde $\mathbb{K} \subset \mathbb{C}$, $\partial f(x) \geq 1$. Então,*

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

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

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

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

Se $k = 1$, reescrevendo $f'(x)$,

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

E para $k > 1$, podemos reescrever $f'(x)$

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

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

($\Longleftarrow$) Suponhamos que $f(x) = (x - \alpha)g(x)$ e $f'(x) = (x - \alpha)h(x)$, notemos que $\text{mdc}(f(x), f'(x)) \neq 1$. Derivando $f(x)$,

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

Pela suposição de $f'(x)$, sabemos que α é uma raiz, logo,

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

E portanto α também é raiz de $g(x)$, podemos então escrever

$$g(x) = (x - \alpha)^m p(x), \text{ onde } m \geq 1 \text{ é a multiplicidade de } \alpha \text{ em } g(x)$$

E substituindo em $f(x) = (x - \alpha)g(x)$,

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

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

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

□

Sempre que um polinômio $p(x)$ for irredutível, com $\partial p(x) \geq 2$, devemos estender o corpo, para que, nesse novo corpo, ele não só seja redutível, como ele possa ser escrito como produto de polinômios de grau um, sendo assim, o corpo possuirá todas as suas raízes, assim conseguimos determinar todas as raízes da equação polinomial $p(x) = 0$.

2.1.2 Verificando a irredutibilidade de polinômios

Identificar se um polinômio é ou não irredutível, não é uma tarefa simples. Veremos agora dois mecanismos que nos ajudam a fazer tal verificação.

Antes de mostrarmos os dois mecanismos, precisamos enunciar um importante lema, o *Lema de Gauss*.

Proposição 2.22. *(Lema de Gauss). Seja $f(x) \in \mathbb{Z}[x]$ tal que $f(x)$ é irredutível sobre $\mathbb{Z}$, então $f(x)$ é também irredutível sobre $\mathbb{Q}$.*

Demonstração. O leitor pode conferir essa demonstração em [2] □

Vamos então ao primeiro mecanismo, o *Critério de Eisenstein*.

Teorema 2.23. *(Critério de Eisenstein)*

Seja $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ um polinômio em $\mathbb{Z}[x]$. Suponha que exista um inteiro primo p, tal que:

i) $p \nmid a_n$

ii) $p \mid a_0, a_1, \ldots, a_{n-1}$

iii) $p^2 \nmid a_0$

Então $f(x)$ é irredutível sobre $\mathbb{Q}$.

Demonstração. Inicialmente, mostremos que $f(x)$ é irredutível sobre $\mathbb{Z}$. Supondo que $f(x)$ não seja irredutível sobre $\mathbb{Z}$, então podemos escrever,

$$f(x) = g(x)h(x), \text{ com } g(x), h(x) \in \mathbb{Z}[x], \text{ e } \partial g(x) \geq 1$$

Onde,

$$g(x) = b_r x^r + b_{r-1}x^{r-1} + \cdots + b_1 x + b_0$$

e

$$h(x) = c_s x^s + c_{s-1}x^{s-1} + \cdots + c_1 x + c_0$$

Da definição de produto entre polinômios e grau do polinômio, temos que

$$\partial f(x) = \partial g(x) + \partial h(x) \Longrightarrow n = r + s.$$

E mais,

$$\begin{aligned} a_n &= b_0 c_n + b_1 c_{n-1} + \cdots + b_n c_0 \\ &\vdots \\ a_0 &= b_0 c_0 \end{aligned}$$

Do item *ii.*, temos que, sendo p primo, $p \mid a_0 \implies p \mid b_0c_0$. No entanto, do item *iii.*, temos que $p^2 \nmid a_0 \implies p^2 \nmid b_0c_0$, portanto p não pode dividir simultaneamente b_0 e c_0. Suponhamos então, sem perda de generalidade, que $p \mid b_0$ e $p \nmid c_0$.

Apesar de $p \mid b_0$, não podemos dizer que p divide todos os $b_i,\ i \in \{1, 2, \ldots, b_r\}$, pois se assim fosse, teríamos $p \mid a_n$ o que contraria *i.*. Digamos então que b_k seja o primeiro b_i não divisível por p com $k < r$, então $p \mid a_k$, onde,

$$a_k = b_0c_k + \cdots + b_kc_0$$

Agora, notemos que $p \mid a_k$ (de acordo com *ii.*), mas como $p \nmid b_k$, devemos ter que $p \mid c_0$, o que é absurdo, já que supomos que $p \nmid c_0$. E então temos que $f(x)$ é irredutível sobre $\mathbb{Z}$.

Por fim, sendo $f(x)$ irredutível sobre $\mathbb{Z}$, de acordo com o Lema de Gauss (Proposição 2.22), segue que $f(x)$ é irredutível sobre $\mathbb{Q}$, como queríamos demonstrar. □

Exemplo 2.24. Seja $f(x) = 2x^3 + 9x^2 + 3x + 6$, indagamos se ele é ou não, irredutível sobre $\mathbb{Q}$. Pelo critério de Einstein para $p = 3$ temos que $p \nmid 2$, $p \mid 9, 3, 6$ e $p^2 = 9 \nmid 6$, portanto $f(x)$ é sim irredutível sobre $\mathbb{Q}$.

Vejamos agora um outro mecanismo, a *Redução módulo p*:

Proposição 2.25. *(Redução módulo p). Seja p um número primo e* $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ *o corpo contendo p elementos. Se* $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ *vamos definir o polinômio* $\bar{f}(x) \in \mathbb{Z}_p[x]$ *como:*

$$\bar{f}(x) = \bar{a}_nx^n + \bar{a}_{n-1}x^{n-1} + \cdots + \bar{a}_1x + \bar{a}_0,$$

onde $\bar{a}_1$ *é a classe de equivalência de* a_i *módulo p, cujo representante é* $a_i \in \mathbb{Z}$. *Então,*

i. $\phi : \begin{array}{c} \mathbb{Z}[x] \to \mathbb{Z}_p[x] \\ f(x) \to \bar{f}(x) \end{array}$ *define um homomorfismo sobrejetivo.*

ii. Se $p \nmid a_n$ *e* $\bar{f}(x)$ *é irredutível sobre* $\mathbb{Z}_p$ *então* $f(x)$ *é irredutível sobre* $\mathbb{Q}$.

Demonstração. O leitor pode consultar a demonstração em [2]. □

Exemplo 2.26. Seja $f(x) = x^2 + 15x + 8$, $f(x)$ é irredutível sobre $\mathbb{Q}$?

Pelo mecanismo de redução módulo p, para $p = 5$ e $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$, teremos $\bar{f}(x) = x^2 + \bar{3}$. Notemos que temos que $5 \nmid 1$, vejamos então se $\bar{f}(x) = x^2 + \bar{3}$ é irredutível sobre $\mathbb{Z}_5$. Substituindo os possíveis valores para x, vemos que, nenhum deles é raiz, logo, $f(x)$ é irredutível em $\mathbb{Z}_5$ consequentemente é também irredutível sobre $\mathbb{Q}$.

Capítulo 3

Extensão de Corpos

Imaginemos a seguinte equação, $x^3 - 1 = 0$, o polinômio desta equação possui seus coeficientes em $\mathbb{Q}$, e neste mesmo corpo possui uma dentre as três soluções, a saber $x = 1$, porém as demais soluções não se encontram neste corpo. E como nem sempre a solução de uma equação polinomial se encontra no corpo onde se encontra seus coeficientes, se necessário, precisamos fazer uma *extensão algébrica* do corpo, para que tenhamos nela todas as soluções da equação polinomial.

Definição 3.1. Uma *extensão de corpos* é uma ampliação de um corpo. Seja $\mathbb{K}$ e $\mathbb{L}$ dois corpos, tal que $\mathbb{K} \subset \mathbb{L}$, podemos afirmar que $\mathbb{L}$ é uma extensão de $\mathbb{K}$, e denotaremos por $\mathbb{L} \mid \mathbb{K}$. Chamaremos o corpo $\mathbb{K}$ de corpo base.

Exemplo 3.2. Eis alguns exemplos de extensão: $\mathbb{R} \mid \mathbb{Q}$ e $\mathbb{C} \mid \mathbb{R}$.

3.1 Extensões algébricas

Definição 3.3. Seja $\mathbb{L} \mid \mathbb{K}$ e $\alpha \in \mathbb{L}$, dizemos que α é *algébrico* sobre $\mathbb{K}$ se existir $f(x) \in \mathbb{K}[x] - \{0\}$ tal que $f(\alpha) = 0$. Caso não exista, diremos que α é *transcendente* sobre $\mathbb{K}$.

Exemplo 3.4. O elemento $\sqrt{2}$ é algébrico sobre $\mathbb{Q}$ uma vez que é raiz de $p(x) = x^2 - 2$ e $p(x) \in \mathbb{Q}[x]$. Já π é transcendente sobre $\mathbb{Q}$, pois não existe um polinômio $p(x) \in \mathbb{Q}[x]$ tal que $p(x) = 0$. Obviamente π é raiz de $p(x) = x - \pi$, porém $p(x) \notin \mathbb{Q}[x]$.

Definição 3.5. Seja $\mathbb{L}$ uma extensão do corpo $\mathbb{K}$. Se todo $\alpha \in \mathbb{L}$ é algébrico sobre $\mathbb{K}$, diremos que $\mathbb{L} \mid \mathbb{K}$ é uma *extensão algébrica*.

Para nosso propósito nos deteremos nas extensões algébricas simples.

Seja $p(x) = x^2 - 2$, claramente ele não possui raízes no corpo $\mathbb{Q}$, então se quisermos encontrar suas raízes, devemos pensar numa extensão de $\mathbb{Q}$, por exemplo, se admitirmos a extensão $\mathbb{R} \mid \mathbb{Q}$, certamente o polinômio terá em $\mathbb{R}$ suas raízes. No entanto, nosso objetivo é buscar o menor corpo possível que contenha essas raízes.

Exemplo 3.6. Seja $\mathbb{R}$ o corpo base, se à ele acrescentarmos o termo algébrico i, onde $i^2 = -1$, temos então $\mathbb{R}[i] = \mathbb{C}$, notemos que i é algébrico sobre $\mathbb{R}$, pois é solução de $q(x) = x^2 + 1$.

Definição 3.7. Seja $\alpha \in \mathbb{L}$ algébrico sobre $\mathbb{K}$ e seja $p(x) \in \mathbb{K}[x]$, mônico e de menor grau tal que $p(\alpha) = 0$. Pela minimalidade do grau, esse polinômio é portanto o único polinômio mônico irredutível em $\mathbb{K}[x]$ tal que $p(\alpha) = 0$, chamamos de *polinômio minimal* e o denotaremos por $P_{min}(\alpha, \mathbb{K})$.

3.2 Extensões Finitas

É importante notarmos que dada uma extensão $\mathbb{L} \mid \mathbb{K}$, as operações dos corpos $\mathbb{L}$ e $\mathbb{K}$ satisfazem as condições para definirmos um *espaço vetorial*, ou seja $\mathbb{L}$ possui a estrutura de espaço vetorial com o corpo $\mathbb{K}$ fazendo o papel de "escalares" nas operações. Recomendamos que o leitor se apodere de conhecimentos básicos de Álgebra Linear.

Vamos entender isso num exemplo prático. Na extensão $\mathbb{Q}[\sqrt{2}] \mid \mathbb{Q}$, o corpo $\mathbb{Q}[\sqrt{2}]$ é um $\mathbb{Q}$-espaço vetorial, cuja base é formada por 1 e $\sqrt{2}$, facilmente pode-se comprovar tal afirmação.

Definição 3.8. Se vermos a extensão como espaço vetorial sobre o corpo base, podemos então definir o *grau de uma extensão*, que nada mais é do que a dimensão de $\mathbb{L}$ sobre $\mathbb{K}$, e denotamos por $[\mathbb{L} : \mathbb{K}]$.

No exemplo da seção anterior, temos que $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$, pois como vimos sua base é $\{1, \sqrt{2}\}$.

Generalizando o exemplo acima, temos que $[\mathbb{Q}[\sqrt[n]{a}] : \mathbb{Q}] = n$, com n ímpar ou n par e $a > 0$, se $\sqrt[n]{a} \notin \mathbb{Q}$, sua base será:

$$\{1, \sqrt[n]{a}, \ \sqrt[n]{a^2}, ..., \ \sqrt[n]{a^{n-1}}\}$$

Proposição 3.9. *Seja $\mathbb{L} \mid \mathbb{K}$ uma extensão com $\alpha \in \mathbb{L}$ algébrico, e $p(x) = P_{min}(\alpha, \mathbb{K})$, então se $\partial p(x)$ é n então $[\mathbb{L} : \mathbb{K}] = n$.*

Demonstração. Ver demonstração em [2]. □

Definição 3.10. Uma extensão $\mathbb{L} \mid \mathbb{K}$ é dita finita se seu grau é finito, caso contrário é chamada extensão infinita.

Nos concentraremos nas extensões finitas. Agora, dada a extensão finita $\mathbb{L} \mid \mathbb{K}$, e seja $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$, chamamos $\mathbb{M}$ de *corpo intermediário*, e então, para determinarmos o grau da extensão $\mathbb{L} \mid \mathbb{K}$, recorremos à chamada *Lei da Torre*:

Proposição 3.11. *Seja* $\mathbb{L} \mid \mathbb{K}$ *uma extensão finita, com corpo intermediário* $\mathbb{M}$*, tal que* $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$*, então,*

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{M}][\mathbb{M} : \mathbb{K}]$$

Demonstração. Sendo $\mathbb{L} \mid \mathbb{K}$ uma extensão finita, então $\mathbb{L} \mid \mathbb{M}$ e $\mathbb{M} \mid \mathbb{K}$ também são.

Seja $\{x_1, x_2, \ldots, x_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{M}$, então $[\mathbb{L} : \mathbb{M}] = n$.

E seja $u \in \mathbb{L}$, então $\exists \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{M}$ tal que,

$$u = \sum_{i=1}^{n} \alpha_i x_i.$$

De modo análogo, seja $\{y_1, y_2, \ldots, y_m\}$ uma base de $\mathbb{M}$ sobre $\mathbb{K}$, então $[\mathbb{M} : \mathbb{K}] = m$.

Dessa forma, como $\alpha_i \in \mathbb{M}$, $\exists \beta_{ij} \in \mathbb{K}$ tal que

$$\alpha_i = \sum_{j=1}^{m} \beta_{ij} y_j.$$

Reescrevendo u:

$$u = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} \beta_{ij} y_j \right) x_i.$$

Desenvolvendo,

$$u = \sum_{j=1}^{m} \beta_{1j} y_j x_1 + \sum_{j=1}^{m} \beta_{2j} y_j x_2 + \cdots + \sum_{j=1}^{m} \beta_{nj} y_j x_n.$$

Note que u está escrito como uma soma de n parcelas, onde cada uma possui uma soma de outras m parcelas, ou seja, u é uma soma de $n \cdot m$ parcelas.

Isso nos garante que o conjunto

$$\{x_1 y_1, x_1 y_2, \ldots, x_1 y_m, x_2 y_1, x_2 y_2, \ldots, x_2 y_m, \ldots, x_n y_1, x_n y_2, \ldots, x_n y_m\}.$$

Que possui $n \cdot m$ elementos gera os elementos de $\mathbb{L}$ sobre $\mathbb{K}$. Resta-nos mostrar que esse conjunto é linearmente independente.

Para que esse conjunto seja linearmente independente, devemos ter,

$$\sum_{\substack{i,j=1 \\ j=m}}^{i=n} \beta_{ij} x_i y_j = 0 \iff \beta_{ij} = 0.$$

Ou seja, nos resta provar que $\beta_{ij} = 0$.

Reescrevendo,

$$\sum_{i=1}^{n} \left(\sum_{j=1}^{m} \beta_{j,i} y_j \right) x_i = 0 \ (*)$$

Como sabemos, $\{x_1, x_2, \ldots, x_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{M}$, logo, a igualdade $(*)$ é válida se, e somente se

$$\sum_{j=1}^{m} \beta_{j,i} y_j = 0 \ (**)$$

E novamente, como $\{y_1, y_2, \ldots, y_m\}$ é uma base de $\mathbb{M}$ sobre $\mathbb{K}$, logo, a igualdade $(**)$ é válida se, e somente se

$$\beta_{j,i} = 0,$$

como queríamos. Dessa forma, temos que o conjunto em questão, além de gerar os elementos de $\mathbb{L}$, é também linearmente independente, logo é uma base de $\mathbb{L} \mid \mathbb{K}$ que contem $n \cdot m$ termos. Portanto,

$$[\mathbb{L} : \mathbb{K}] = n \cdot m = [\mathbb{L} : \mathbb{M}][\mathbb{M} : \mathbb{K}],$$

como queríamos demonstrar.

□

Corolário 3.12. *Seja $\mathbb{L}/\mathbb{K}$ uma extensão com corpos intermediários da forma:*

$$\mathbb{K} = \mathbb{M}_0 \subset \mathbb{M}_1 \subset ... \subset \mathbb{M}_{n-1} \subset \mathbb{M}_n = \mathbb{L}.$$

Então,

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} = \mathbb{M}_n : \mathbb{M}_{n-1}][\mathbb{M}_{n-1} : \mathbb{M}_{n-2}]...[\mathbb{M}_2 : \mathbb{M}_1][\mathbb{M}_1 : \mathbb{M}_0 = \mathbb{K}].$$

Demonstração. A demonstração é imediata da proposição 3.11, aplicando-a várias vezes.

□

Definição 3.13. Dado $\alpha \in \mathbb{L} \mid \mathbb{K}$, definimos $\mathbb{K}[\alpha] = \{f(\alpha) : f(x) \in \mathbb{K}[x]\}$, e temos que $\mathbb{K}[\alpha]$ é um subdomínio de $\mathbb{L}$ que contém $\mathbb{K}$.

Exemplo 3.14. Verifiquemos que $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

Ora, pela definição

$$\mathbb{Q}[\sqrt{2}] = \{f(\sqrt{2}) : f(x) \in \mathbb{Q}[x]\}$$

E de acordo com o algoritmo da divisão euclidiana, que vimos na Definição 2.11, existem $q(x), r(x) \in \mathbb{Q}[x]$ tais que

$$f(x) = q(x) \cdot p(x) + r(x), \text{ onde } p(x) = x^2 - 2 \text{ e } r(x) = a + bx$$

Para $x = \sqrt{2}$ temos que,

$$f(\sqrt{2}) = q(\sqrt{2}) \cdot (2 - 2) + r(\sqrt{2}) \Rightarrow f(\sqrt{2}) = r(\sqrt{2}) = a + b\sqrt{2}.$$

De modo generalizado, se p é um primo positivo, n inteiro positivo ≥ 2, e $\alpha = \sqrt[n]{p} \in \mathbb{R}$. Então α é raiz do polinômio $x^n - p$ que é irredutível (pelo critério de Eisenstein, visto no Teorema 2.23). Assim $x^n - p = P_{min}(\alpha, \mathbb{Q})$, $\mathbb{Q}[x]$ é um subcorpo de $\mathbb{R}$ contendo $\mathbb{Q}$ e

$$\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Q} \text{ e } i = 0, 1, \ldots, n-1\}$$

Definição 3.15. Uma extensão $\mathbb{L} \mid \mathbb{K}$ é dita simples se $\mathbb{L} = \mathbb{K}[\alpha]$, para algum $\alpha \in \mathbb{L}$. Neste caso, α é chamado elemento primitivo de $\mathbb{L}$.

Teorema 3.16. *(Teorema do Elemento Primitivo) Seja* $\mathbb{L} = \mathbb{K}[\gamma_1, \gamma_2, \ldots, \gamma_n]$*, com* $\gamma_i \in \mathbb{L}$*, então* $\exists \beta \in \mathbb{L}$ *tal que* $\mathbb{L} = \mathbb{K}[\beta]$*.*

Demonstração. Ver demonstração em [5] ou [8]. □

Exemplo 3.17. Seja $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \mid \mathbb{Q}$, podemos reescrevê-la como sendo $\mathbb{Q}[\sqrt{2} + \sqrt{3}] \mid \mathbb{Q}$.

Exemplo 3.18. Qual o grau da extensão $\mathbb{Q}[\sqrt[3]{5}, \sqrt[5]{2}] \mid \mathbb{Q}$?

Podemos decompor essa extensão com os seguintes corpos intermediários: $\mathbb{Q} \subset \mathbb{Q}[\sqrt[5]{2}] \subset \mathbb{Q}[\sqrt[3]{5}, \sqrt[5]{2}]$, e então de acordo com a Proposição 3.11:

$$[\mathbb{Q}[\sqrt[3]{5}, \sqrt[5]{2}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt[3]{5}, \sqrt[5]{2}] : \mathbb{Q}[\sqrt[5]{2}]][\mathbb{Q}[\sqrt[5]{2}] : \mathbb{Q}] \Longrightarrow$$

$$[\mathbb{Q}[\sqrt[3]{5}, \sqrt[5]{2}] : \mathbb{Q}] = 3 \cdot 5 = 15$$

O leitor obviamente notou a presença dos números complexos em capítulos anteriores. Considerando que nosso propósito são as soluções de equações polinomiais, é muito comum que tais soluções pertençam à subcorpos de $\mathbb{C}$. nas próximas seções, pretendemos expor os números complexos, com foco nas raízes primitivas da unidade, dessa forma, podemos garantir a solução de quaisquer equações polinomiais.

3.3 Conhecendo os números complexos

Pode-se dizer que os números complexos surgiram da necessidade de resolução de equações como $x^2 + 1 = 0$, equação essa que obviamente não tinha soluções reais, uma vez que sua solução seria encontrada por meio da solução de raiz quadrada de um número negativo. Apesar disso, só no estudo das raízes cúbicas foi que surgiu a definição de *número complexo*, antes soluções que envolvesse raízes de números negativos eram chamados de *casos irredutíveis*.

A notação i para unidade imaginária, deve-se à Leonhard Euler. Além dele, outros matemáticos se dedicaram ao desenvolvimento do estudos sobre números complexos, Caspar Wessel, Jean Robert Argand e Carl Friedrich Gauss.

Podemos dizer que o conjunto dos números complexos, que forma o corpo, denotado por $\mathbb{C}$, é uma extensão de $\mathbb{R}$, ou seja $\mathbb{C} \mid \mathbb{R}$, uma vez que $\mathbb{R}[i] = \mathbb{C}$.

Definição 3.19. Um número complexo z, é todo número da forma $z = a + bi$, com $a, b \in \mathbb{R}$, onde i é a unidade imaginária caracterizada por $i^2 = -1$. Note que nos casos em que $b = 0$, teremos $z \in \mathbb{R}$, e por isso podemos afirmar que $\mathbb{R} \subset \mathbb{C}$, e $\mathbb{C} \mid \mathbb{R}$.

Seja $z = a + bi$ e $w = c + di$, definimos a adição e a multiplicação no corpo $\mathbb{C}$ como:

$$z + w = (a + bi) + (c + di) = (a + c) + (b + d)i$$

$$z \cdot w = (a + bi) \cdot (c + di) = (a \cdot c - b \cdot d) + (a \cdot d + b \cdot c)i$$

Podemos enxergar o número complexo também como um par ordenado, $z = (a, b)$ tal que a é a parte real e b é a parte imaginária. Por exemplo, se $z = 1 + \sqrt{3}i$ pode ser representado por $z = (1, \sqrt{3})$. Essa representação é útil para enxergarmos o número complexo geometricamente, no plano cartesiano, como sendo um vetor, veja a figura 3.1.

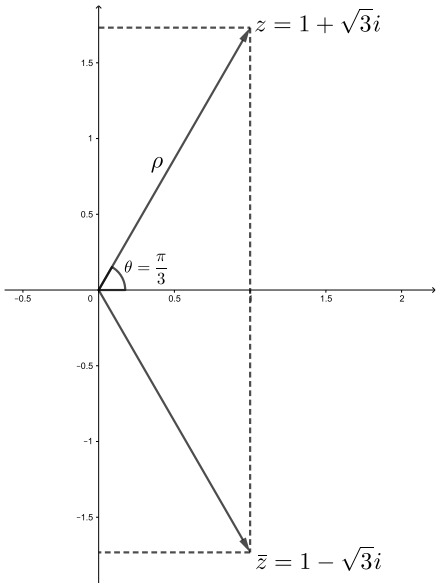

Figura 3.1: Representação geométrica do número complexo $z = 1 + \sqrt{3}i$

Diante de tal representação, podemos definir o *conjugado* de $z = a + bi$, como sendo $\bar{z} = a - bi$, que nada mais é do que z com a parte imaginária oposta, veja a figura 3.1.

Notemos que o vetor, numa visão trigonométrica, tem um "tamanho", comumente chamado de *módulo*, que denotaremos por ρ, e um ângulo, medido no sentido anti-horário em relação ao eixo x, chamado de *argumento* que representaremos por θ, observe na figura 3.1.

Os elementos ρ e θ são úteis para representar o número complexo na chamada forma *trigonométricas ou polar*. Apesar de existirem outras formas de representar um número complexo, focaremos nossa atenção na forma trigonométrica.

Agora observemos o triângulo retângulo de vértices nos pontos $(0, 0)$, $(1, 0)$ e $(1, \sqrt{3})$ (veja a figura 3.1). Usando as relações trigonométricas, temos que $\rho = \sqrt{a^2 + b^2}$, e

ainda, $\cos(\theta) = \frac{x}{\rho}$ e $\text{sen}(\theta) = \frac{y}{\rho}$, com $0 \leq \theta \leq 2\pi$. E então representamos z na forma trigonométrica como:

$$z = \rho\ (\cos(\theta) + i\,\text{sen}(\theta)).$$

Vejamos agora como procedemos com as operações de multiplicação, divisão, potenciação e radiciação, chamando atenção para esta última.

Dados $z_1 = \rho_1\ (\cos(\theta_1) + i\,\text{sen}(\theta_1))$ e $z_2 = \rho_2\ (\cos(\theta_2) + i\,\text{sen}(\theta_2))$, quanto à operações de multiplicação, temos que:

$$\begin{aligned}
z_1 z_2 &= [\rho_1\ (\cos(\theta_1) + i\,\text{sen}(\theta_1))] \cdot [\rho_2\ (\cos(\theta_2) + i\,\text{sen}(\theta_2))] \\
&= \rho_1\rho_2\ [(\cos(\theta_1) + i\,\text{sen}(\theta_1)) \cdot (\cos(\theta_2) + i\,\text{sen}(\theta_2))] \\
&= \rho_1\rho_2\ [\cos(\theta_1)\cos(\theta_2) + i\cos(\theta_1)\,\text{sen}(\theta_2) + i\,\text{sen}(\theta_1)\cos(\theta_2) + i^2\,\text{sen}(\theta_1)\,\text{sen}(\theta_2)] \\
&= \rho_1\rho_2\ [\cos(\theta_1)\cos(\theta_2) + i\cos(\theta_1)\,\text{sen}(\theta_2) + i\,\text{sen}(\theta_1)\cos(\theta_2) - \text{sen}(\theta_1)\,\text{sen}(\theta_2)] \\
&= \rho_1\rho_2\ [\cos(\theta_1)\cos(\theta_2) - \text{sen}(\theta_1)\,\text{sen}(\theta_2) + i(\cos(\theta_1)\,\text{sen}(\theta_2) + \text{sen}(\theta_1)\cos(\theta_2))]
\end{aligned}$$

Das relações trigonométricas, usando o seno e cosseno da soma de dois arcos:

$$\begin{aligned}
z_1 z_2 &= \rho_1\rho_2\ [\underbrace{\cos(\theta_1)\cos(\theta_2) - \text{sen}(\theta_1)\,\text{sen}(\theta_2)}_{\cos(\theta_1+\theta_2)} + \underbrace{i(\cos(\theta_1)\,\text{sen}(\theta_2) + \text{sen}(\theta_1)\cos(\theta_2))}_{\text{sen}(\theta_1+\theta_2)} \\
&= \rho_1\rho_2\ [\cos(\theta_1 + \theta_2) + i\,\text{sen}(\theta_1 + \theta_2)]
\end{aligned}$$

Antes de falarmos em divisão de um número complexo, devemos entender o conceito de inverso. Assim, seja $z = \rho\ (\cos(\theta) + i\,\text{sen}(\theta))$, seu inverso, que denotaremos por z^{-1}, será $z^{-1} = \mu(\cos(\beta) + i\,\text{sen}(\beta))$ tal que $z \cdot z^{-1} = 1$. Vale notar que podemos escrever $1 = 1 \cdot (\cos(2\pi) + i\,\text{sen}(2\pi))$, e então:

$$z \cdot z^{-1} = 1 \Longrightarrow$$

$$\rho\ (\cos(\theta) + i\,\text{sen}(\theta)) \cdot \mu(\cos(\beta) + i\,\text{sen}(\beta)) = 1 \cdot (\cos(2\pi) + i\,\text{sen}(2\pi)).$$

Usando a multiplicação que acabamos de mostrar:

$$\rho\mu[\cos(\theta + \beta) + i\,\text{sen}(\theta + \beta) = 1 \cdot (\cos(2\pi) + i\,\text{sen}(2\pi)) \Longrightarrow$$

$$\rho\mu = 1 \text{ e } \theta + \beta = 2\pi \Longrightarrow$$

$$\mu = \frac{1}{\rho} \text{ e } \beta = 2\pi - \theta = -\theta.$$

E então, concluímos que:

$$z^{-1} = \frac{1}{\rho}[\cos(-\theta) + i\,\mathrm{sen}(-\theta)].$$

Quanto à divisão de números complexos, dados os mesmos $z_1 = \rho_1\ (\cos(\theta_1) + i\,\mathrm{sen}(\theta_1))$ e $z_2 = \rho_2\ (\cos(\theta_2) + i\,\mathrm{sen}(\theta_2))$, desejamos saber o valor de $\frac{z_1}{z_2}$. Sabemos que podemos pensar a divisão como sendo o produto de z_1 pelo inverso de z_2, e então:

$$\begin{aligned}\frac{z_1}{z_2} &= z_1 \cdot z_2^{-1} = \rho_1\ (\cos(\theta_1) + i\,\mathrm{sen}(\theta_1)) \cdot \frac{1}{\rho_2}\,[\cos(-\theta_2) + i\,\mathrm{sen}(-\theta_2)] \\ &= \frac{\rho_1}{\rho_2}\,[\cos(\theta_1 - \theta_2) + i\,\mathrm{sen}(\theta_1 - \theta_2)].\end{aligned}$$

Sobre a potenciação de números complexos, podemos entendê-la por meio da multiplicação. Seja $z = \rho\ (\cos(\theta) + i\,\mathrm{sen}(\theta))$, temos que $\underbrace{z \cdot z \cdots z}_{n \text{ vezes}} = z^n$, onde $z^0 = 1$ e $z^n = z^{n-1} \cdot z$. Portanto:

$$\begin{aligned}z^n &= \underbrace{z \cdot z \cdots z}_{n \text{ vezes}} = \underbrace{\rho \cdot \rho \cdots \rho}_{n \text{ vezes}}\,[\cos(\underbrace{\theta + \theta + \cdots + \theta}_{n \text{ parcelas}}) + i\,\mathrm{sen}(\underbrace{\theta + \theta + \cdots + \theta}_{n \text{ parcelas}})] \\ &= \rho^n\ (\cos(n\theta) + i\,\mathrm{sen}(n\theta)).\end{aligned}$$

Como na potenciação, o expoente $n \in \mathbb{Z}$, caso $n < 0$, teremos:

$$\begin{aligned}z^{-n} &= (z^n)^{-1} = (\rho^n\ (\cos(n\theta) + i\,\mathrm{sen}(n\theta)))^{-1} \\ &= \frac{1}{\rho^n}[\cos(-n\theta) + i\,\mathrm{sen}(-n\theta)].\end{aligned}$$

Por fim, a radiciação de números complexos z, ou seja a raiz n-ésima de z, serão todos os números complexos que elevados a n resulta em z. Apesar de essa operação não está bem definida, ela pode ser vista como sendo as raízes da equação:

$$\omega^n = z,$$

onde ω é a solução procurada.

Ponhamos $\omega = \eta\ (\cos(\alpha) + i\,\mathrm{sen}(\alpha))$, teremos:

$$\eta^n\ (\cos(n\alpha) + i\,\mathrm{sen}(n\alpha)) = \rho\ (\cos(\theta) + i\,\mathrm{sen}(\theta)) \Longrightarrow$$

$$\Longrightarrow \eta^n = \rho \text{ e } n\alpha = \theta + 2k\pi,$$

com $k \in \mathbb{Z}$, e então:

$$\omega_k = \sqrt[n]{\rho}\ \left[\cos\left(\frac{\theta+2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{\theta+2k\pi}{n}\right)\right].$$

Notemos que se $z = 0$, então tem-se apenas uma solução $\omega = 0$, caso contrário, tem-se n soluções complexas, basta que tenhamos $k = 0, 1, 2, ..., n-1$.

Exemplo 3.20. Seja $z = -8 + 8\sqrt{3}i$, encontre todos as raízes quartas de z.

Inicialmente, determinemos a forma polar de z, para isto, temos que

$$\rho = \sqrt{(-8)^2 + (8\sqrt{3})^2} = \sqrt{256} \Longrightarrow \rho = 16$$

e

$$\cos(\theta) = -\frac{8}{16} \Longrightarrow \cos(\theta) = -\frac{1}{2}$$

Notemos que nesse caso, θ poderia assumir dois valores, $\frac{2\pi}{3}$, que indicaria que z está no segundo quadrante, ou $\frac{4\pi}{3}$, indicando que z está no terceiro quadrante. Vejamos então que, como $z = -8 + 8\sqrt{3}i$, suas coordenadas cartesianas são $(-8, 8\sqrt{3})$, donde identificamos que z está no segundo quadrante, e portanto, temos que $\theta = \frac{2\pi}{3}$. Logo,

$$z = 16\ \left[\cos\left(\frac{2\pi}{3}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{3}\right)\right]$$

Agora, usando a fórmula vista anteriormente:

$$\omega_k = \sqrt[4]{16}\ \left[\cos\left(\frac{\frac{2\pi}{3}+2k\pi}{4}\right) + i\,\mathrm{sen}\left(\frac{\frac{2\pi}{3}+2k\pi}{4}\right)\right] \Longrightarrow$$

$$\omega_k = 2\ \left[\cos\left(\frac{\pi(1+3k)}{6}\right) + i\,\mathrm{sen}\left(\frac{\pi(1+3k)}{6}\right)\right], k = 0, 1, 2, 3$$

Para $k = 0$:

$$\omega_0 = 2\ \left[\cos\left(\frac{\pi}{6}\right) + i\,\mathrm{sen}\left(\frac{\pi}{6}\right)\right] \Longrightarrow \omega_0 = \sqrt{3} + i$$

Para $k = 1$:

$$\omega_1 = 2\ \left[\cos\left(\frac{2\pi}{3}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{3}\right)\right] \Longrightarrow \omega_1 = -1 + i\sqrt{3}$$

Para $k = 2$:

$$\omega_2 = 2\ \left[\cos\left(\frac{7\pi}{6}\right) + i\,\mathrm{sen}\left(\frac{7\pi}{6}\right)\right] \Longrightarrow \omega_2 = -\sqrt{3} - i$$

Para $k = 3$:

$$\omega_3 = 2\ \left[\cos\left(\frac{5\pi}{3}\right) + i\,\mathrm{sen}\left(\frac{5\pi}{3}\right)\right] \Longrightarrow \omega_3 = 1 - i\sqrt{3}$$

Concluímos então que os quatro números complexos que elevados à quarta potência resulta em $z = -8 + 8\sqrt{3}i$ são:

$$\omega_0 = \sqrt{3} + i,\ \omega_1 = -1 + i\sqrt{3},\ \omega_2 = -\sqrt{3} - i,\ \omega_3 = 1 - i\sqrt{3}$$

Geometricamente podemos identificar no plano complexos os números $\omega_k,\ k = 0, 1, 2, 3$ como sendo os vértices de um quadrado, uma vez que por se tratar de uma raiz quarta, temos quatro resultado, e portanto, um polígono de quatro lados. Este quadrado deve está inscrito numa circunferência de centro na origem e raio $\rho = 2$, e assim identificamos $\omega_1 = (\sqrt{3}, 1),\ \omega_2 = (-1, \sqrt{3}),\ \omega_3 = (-\sqrt{3}, -1),\ e\ \omega_4 = (1, -\sqrt{3})$, vejamos a figura 3.2

Notemos que o ângulo de ω_1 está explícito, e os ângulos de $\omega_2,\ \omega_3,\ \omega_4$ que estão implícitos, são respectivamente: $\dfrac{\pi}{6} + \dfrac{\pi}{2},\ \dfrac{\pi}{6} + \pi,\ e\ \dfrac{\pi}{6} + \dfrac{3\pi}{2}$.

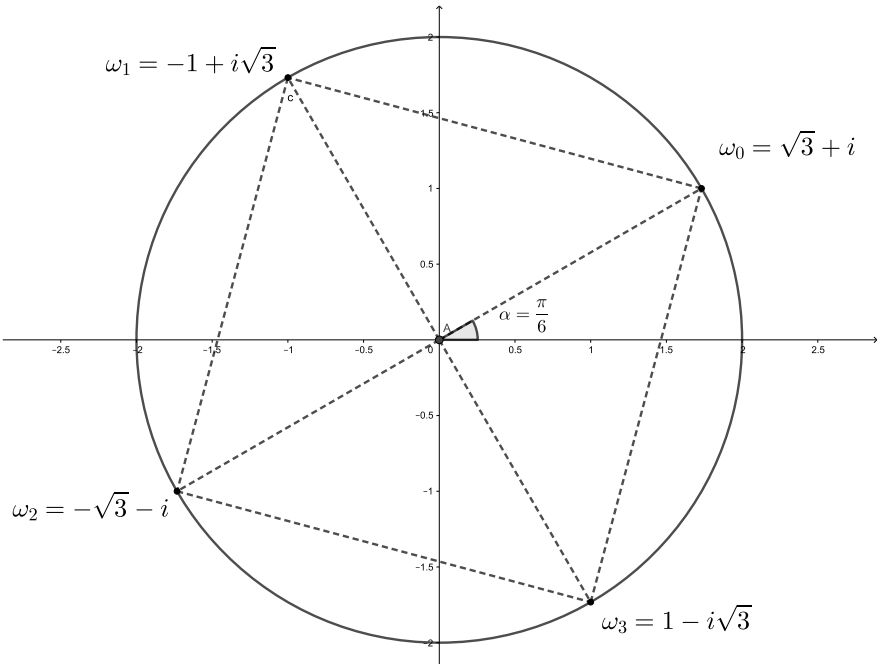

Figura 3.2: Representação geométrica de $\omega^4 = -8 + 8\sqrt{3}i$

3.4 Raízes n-ésimas da unidade

No exemplo que acabamos de estudar na seção anterior, encontramos as raízes quartas de um número complexo z. Como exemplo ilustrativo, agora vamos encontrar as raízes quintas de $z = 1$. Então, em outras palavras, desejamos encontrar todos os números

complexos z, tais que $w^5 = 1$. O procedimento é exatamente o mesmo do exemplo anterior.

Podemos agora generalizar, buscando as raízes n-ésimas de $z = 1$, ou seja, resolvermos $w^n = 1$. Chamamos esses números w de raízes n-ésimas da unidade, e denotaremos por ζ_n^k com $k = 0, 1, \ldots, n-1$. Vale ressaltar que $\zeta_n^0 = 1$.

Assim, $\zeta_n = \cos\left(\frac{2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2k\pi}{n}\right)$, $k = 0, 1, \ldots, n-1$. Geometricamente, as raízes n-ésimas da unidade, são vértices do polígono regular de n lados inscrito numa circunferência de raio 1.

Sabemos que a equação $w^n = 1$, exige n soluções, que serão obtidas como potências de ζ_n, são elas: $\{\zeta_n^0 = 1, \zeta_n^1 = \zeta_n,\ \zeta_n^2,\ \ldots,\ \zeta_n^{n-1}\}$. Dessa formar, se conhecermos uma dessas raízes, facilmente encontramos as demais. Notemos que então,

$$\zeta_n^k = \cos\left(\frac{2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2k\pi}{n}\right),\ k = 0, 1, \ldots, n-1$$

E mais, n é o menor inteiro, diferente de zero, tal que $\zeta_n^n = 1$.

Na notação que adotamos, ζ_n^k, tanto n quanto k são índices, no entanto, o índice k também pode ser entendido como potência. Dessa forma, todas as raízes n-ésima são potências de ζ_n. No entanto, ζ_n não é a única raiz com essa característica.

Definição 3.21. Dizemos que ζ_n^k é uma raiz primitiva n-ésima da unidade, quando todas as raízes são potências de ζ_n^k. Em particular, ζ_n é uma raiz primitiva n-ésima da unidade.

Numa raiz n-ésima primitiva da unidade, $b = n$ é o menor valor de b, diferente de zero, tal que $\left(\zeta_n^k\right)^b = 1$.

Proposição 3.22. *Seja $\zeta_n^k \in \mathbb{C}$, $n \geq 2$ e $k \in \mathbb{Z}$. Assim ζ_n^k é uma raiz n-ésima primitiva da unidade, se e somente se,* $\mathrm{mdc}(k, n) = 1$.

Demonstração. ($\Longrightarrow$) Se ζ_n^k é uma raiz n-ésima primitiva da unidade, suponhamos por absurdo que $\mathrm{mdc}(k, n) = c \neq 1$. Então $\exists a \in \mathbb{N}$ tal que $n = c \cdot a$, e então,

$$(\zeta_n^k)^a = (\zeta_n^{\frac{k}{c}\cdot c})^a = (\zeta_n^{c\cdot a})^{\frac{k}{c}} = (\zeta_n^n)^{\frac{k}{c}}.$$

Como sabemos, $\zeta_n^n = 1$, logo,

$$(\zeta_n^k)^a = 1^{\frac{k}{c}} = 1 \Longrightarrow (\zeta_n^k)^a = 1.$$

Da suposição, $\mathrm{mdc}(k, n) = c \Longrightarrow \mathrm{mdc}(k, c \cdot a) = c$, então $a < n$, pois $c \neq 1$, configurando assim um absurdo, uma vez que n é o menor inteiro tal que $\zeta_n^n = 1$. Portanto $\mathrm{mdc}(k, n) = 1$.

($\Longleftarrow$) Agora, suponha que $\mathrm{mdc}(k, n) = 1$, e que $(\zeta_n^k)^b = 1$, com $b \in \mathbb{N}$. Segue que $n \mid kb$. E como $\mathrm{mdc}(k, n) = 1$, temos que $n \mid b$, então b é no mínimo n, ou seja $b \geq n$. Portanto ζ_n^k é de fato uma raiz n-ésima primitiva da unidade, como queríamos demonstrar.

□

Dessa proposição, podemos concluir que o número de raízes n-ésimas primitiva da unidade é dada por $\phi(n)$, onde $\phi : \mathbb{N} \longrightarrow \mathbb{N}$ é a função Totiente de Euler, definida da seguinte forma:

$$\phi(n) = \{\text{quantidade de números naturais } m \text{ tais que } 0 < m < n;\ \text{mdc}(m,n) = 1,\ m \in \mathbb{Z}\}.$$

Exemplo 3.23. Encontre as raízes sextas da unidade.

Em outras palavras devemos resolver $w^6 = 1$. A princípio, calculando ζ_6, teremos:

$$\zeta_6^k = \cos\left(\frac{2k\pi}{6}\right) + i\,\text{sen}\left(\frac{2k\pi}{6}\right),\ k = 0, 1, ..., 5.$$

E de acordo com a proposição, os coprimos de 6 são 1 e 5, portanto só será raiz primitiva, ζ_6 e ζ_6^5, determinados quando $k = 1$ e $k = 5$, respectivamente. Trabalhemos com $k = 1$:

$$\begin{aligned}\zeta_6 &= \cos\left(\frac{2\pi}{6}\right) + i\,\text{sen}\left(\frac{2\pi}{6}\right)\\ &= \cos\left(\frac{\pi}{3}\right) + i\,\text{sen}\left(\frac{\pi}{3}\right)\\ &= \frac{1}{2} + \frac{\sqrt{3}}{2}i.\end{aligned}$$

As demais soluções, que poderão ser encontradas facilmente, porém omitiremos os cálculos, serão: $\zeta_6^0 = 1$, $\zeta_6^2 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, $\zeta_6^3 = -1$, $\zeta_6^4 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$, $\zeta_6^5 = \frac{1}{2} - \frac{\sqrt{3}}{2}i$. Vejamos geometricamente a figura 3.3:

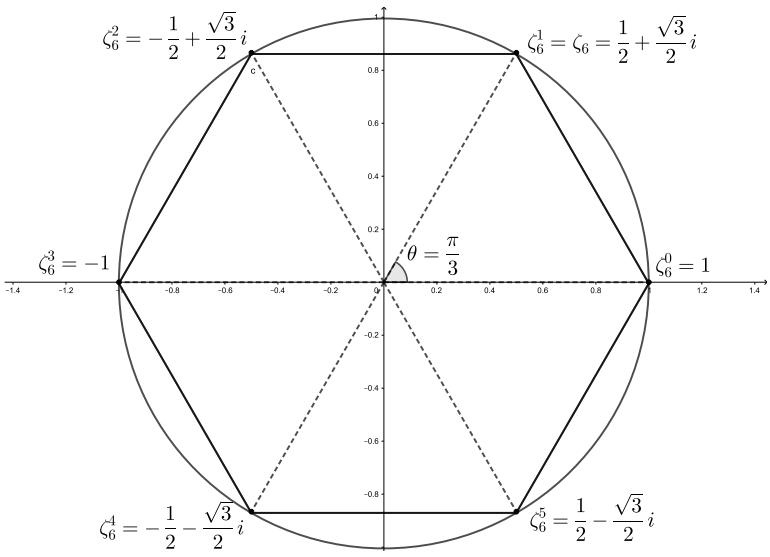

Figura 3.3: Representação geométrica de $z^6 = 1$

Enfim, associando o conceito de extensões algébricas e raízes n-ésimas, temos o seguinte teorema:

Teorema 3.24. *Se ζ_n é uma raiz n-ésima da unidade, então $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \phi(n)$.*

Demonstração. Ver demonstração em [6] ou [10]. □

Em particular, se n é primo, a extensão terá grau $n - 1$.

3.5 Soluções de equações do tipo $x^n = \alpha$

Como já sabemos, dada uma equação polinomial com coeficientes reais, nem sempre conseguimos encontrar suas soluções dentro desse mesmo corpo. Porém, certamente encontramos todas no corpo dos complexos.

Dada uma equação do tipo $x^n = \alpha$, com $\alpha \in \mathbb{C}$ e n inteiro positivo, é sempre possível identificar uma raiz ω, e a partir dela, usando as raízes n-ésimas da unidade, determina-se as demais:

$$\{\ \omega\zeta_n^0 = \omega, \omega\zeta_n,\ \omega\zeta_n^2,\ ...,\ \omega\zeta_n^{n-1}\}.$$

Exemplo 3.25. Determine as soluções de $x^8 = 2$.

Poderíamos resolver essa equação de modo análogo à forma como resolvemos $z^6 = 1$ na seção anterior, no entanto, a maneira que acabamos de apresentar é bem mais prática, vejamos.

Inicialmente, devemos determinar ζ_8:

$$\begin{aligned}
\zeta_8 &= \cos\left(\frac{2\pi}{8}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{8}\right) \\
&= \cos\left(\frac{\pi}{4}\right) + i\,\mathrm{sen}\left(\frac{\pi}{4}\right) \\
&= \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i
\end{aligned}$$

Além disso, temos $\omega = \sqrt[8]{2}$, e então as soluções serão:

$$\begin{gathered}
\omega\zeta_8^0 = \sqrt[8]{2} \cdot (1) = \sqrt[8]{2} \\
\omega\zeta_8 = \sqrt[8]{2} \cdot \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right) \\
\omega\zeta_8^2 = \sqrt[8]{2} \cdot (i) = \sqrt[8]{2}i \\
\omega\zeta_8^3 = \sqrt[8]{2} \cdot \left(-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right) \\
\omega\zeta_8^4 = \sqrt[8]{2} \cdot (-1) = -\sqrt[8]{2} \\
\omega\zeta_8^5 = \sqrt[8]{2} \cdot \left(-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right) \\
\omega\zeta_8^6 = \sqrt[8]{2} \cdot (-i) = -\sqrt[8]{2}i \\
\omega\zeta_8^7 = \sqrt[8]{2} \cdot \left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)
\end{gathered}$$

Visualizemos essa solução geometricamente, na figura 3.4, temos então que as raízes são os vértices do polígono regular de oito lados, o octógono, inscrito numa circunferência de raio $\sqrt[8]{2}$.

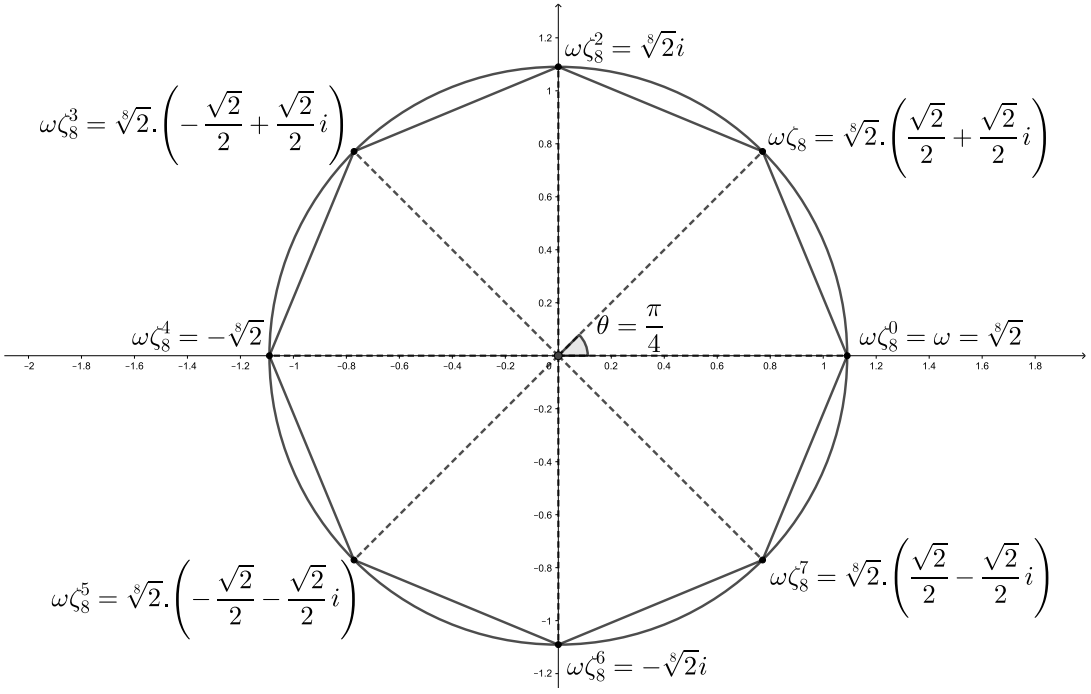

Figura 3.4: Representação geométrica de $x^8 = 2$

Capítulo 4

Teoria de Galois

No presente capítulo, trataremos do mais importante objeto necessário ao nosso objetivo, a Teoria de Galois, que basicamente serve para transformar o problema de encontrar raízes por meio de radicais, em um problema de grupos.

4.1 Corpo de Decomposição

Como vimos, na Definição de 2.15, um polinômio mônico pode ser reescrito como um produto de polinômios de grau um, desde que esteja num corpo que possua todas suas raízes.

Definição 4.1. Seja $f(x) \in \mathbb{K}[x]$. O menor subcorpo de $\mathbb{C}$ que contém $\mathbb{K}$ e todas as raízes de $f(x)$, é chamado corpo de decomposição do polinômio $f(x)$, e denotaremos por $\mathbb{L} = \text{Gal}(f, \mathbb{K})$.

Podemos obter o corpo de decomposição de $f(x)$ por meio de um processo recursivo que chamamos de adjunção de raízes:

$$\mathbb{K}_0 = \mathbb{K} \subset \mathbb{K}_1 = \mathbb{K}[\alpha_1] \subset \mathbb{K}_2 = \mathbb{K}_1[\alpha_2] \subset ... \subset \mathbb{K}_r = \mathbb{K}_{r-1}[\alpha_r],$$

onde $\alpha_i,\ i = 1, 2, ..., r$ são as distintas raízes de $f(x)$, $\mathbb{K}_r$ é o menor subcorpo de $\mathbb{C}$ contendo $\mathbb{K}$ e as raízes $\alpha_1, ..., \alpha_i$ e portanto $\mathbb{K}_r = \text{Gal}(f, \mathbb{K})$, ou seja, $\mathbb{K}_r = \mathbb{K}[\alpha_1, ..., \alpha_r]$.

Exemplo 4.2. Determine o $\text{Gal}(x^3 - 2, \mathbb{Q})$. Obviamente trata-se de um subcorpo de $\mathbb{C}$, mas, como determiná-lo?

Sabemos que esse polinômio pertence à $\mathbb{Q}[x]$, e é irredutível no mesmo, portanto para que este se decomponha por completo, devemos estender esse corpo. Notemos que $\sqrt[3]{2}$ é uma das raízes desse polinômio, e então na extensão $\mathbb{Q}[\sqrt[3]{2}] \mid \mathbb{Q}$ ele é redutível, porém não totalmente decomposto, uma vez que nele não se encontra as outras duas raízes do polinômio. Então necessitamos fazer uma outra extensão que contenha as outras duas raízes do polinômio, ela será do tipo $\mathbb{Q}[\sqrt[3]{2}, \zeta_3] \mid \mathbb{Q}[\sqrt[3]{2}]$, onde $\zeta_3 = -\frac{1}{2} + \frac{\sqrt{3}i}{2} \in \mathbb{C}$. Note que nessa extensão temos as três raízes do polinômio, a saber, $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta_3$ e $\sqrt[3]{2}\zeta_3^2$, onde $\zeta_3^2 = -\frac{1}{2} - \frac{\sqrt{3}i}{2}$. Portanto concluímos que $\text{Gal}(x^3 - 2, \mathbb{Q}) = \mathbb{Q}[\sqrt[3]{2}, \zeta_3]$.

Generalizando o exemplo acima, temos que $\mathrm{Gal}(x^n - a, \mathbb{Q}) = \mathbb{Q}[\sqrt[n]{a}, \zeta_n]$, sempre que a for positivo ou n for ímpar.

Ainda sobre corpo de decomposição, segue um importante teorema:

Teorema 4.3. *Seja $f(x) \in \mathbb{K}[x]$ um polinômio de grau $n > 0$ e $\mathbb{L}$ seu corpo de decomposição, então $[\mathbb{L} : \mathbb{K}] \leq n!$.*

Demonstração. Provemos por indução. Para $n = 1$, temos que $f(x) = ax+b$, com $a, b \in \mathbb{K}$ e $a \neq 0$. Seja α a raiz de $f(x)$, tem-se que $\alpha = -\dfrac{b}{a}$, e então $\alpha \in \mathbb{K}$, logo $\mathbb{K}(\alpha) = \mathbb{K}$ e $[\mathbb{K} : \mathbb{K}] = 1 \leq 1!$.

Suponhamos que a afirmação seja verdadeira para $n = k - 1$.

Seja então $\alpha_1, \alpha_2, \ldots, \alpha_k$ as raízes de $f(x) \in \mathbb{K}$, então

$$f(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_k)$$

e seu corpo de decomposição será $\mathbb{L} = \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_k)$.

Reescrevendo $f(x)$ como sendo $f(x) = (x - \alpha_1)g(x)$, com $g(x) \in \mathbb{K}(\alpha_1)$ e $g(x) = (x - \alpha_2)(x - \alpha_3) \ldots (x - \alpha_k)$, seu corpo de decomposição será

$$\mathbb{K}(\alpha_1)(\alpha_2, \alpha_3, \ldots, \alpha_k) = \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_k) = \mathbb{L}$$

Notemos que $\partial g(x) = n - 1$, e então, usando a hipótese de indução,

$$[\mathbb{L} : \mathbb{K}(\alpha_1)] \leq (n - 1)!$$

Pela lei da torre, vista na proposição 3.11,

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}(\alpha_1)]\ [\mathbb{K}(\alpha_1) : \mathbb{K}] \leq (n - 1)!\ [\mathbb{K}(\alpha_1) : \mathbb{K}].$$

Agora pela própria construção, tem-se que α_1 é raiz de um polinômio de grau n, e pelo que vimos sobre polinômio minimal na seção 3.1, sabemos que o grau do polinômio minimal de α_1 é $\leq n$, e então:

$$[\mathbb{L} : \mathbb{K}] = (n - 1)! \cdot n \Longrightarrow [\mathbb{L} : \mathbb{K}] = n!$$

□

Vejamos um exemplo: Seja $f(x) = (x^7 - 5)$ um polinômio de coeficientes em $\mathbb{Q}$, de grau 7, segundo o teorema acima, a extensão em que $f(x)$ se decompõe tem grau $\leq 7!$, comprovemos. O corpo de decomposição de $f(x)$ é $\mathbb{Q}[\sqrt[7]{5}, \zeta_7]$ (ver Exemplo 4.2). Temos que $[\mathbb{Q}[\sqrt[7]{5}] : \mathbb{Q}] = 7$ e $[\mathbb{Q}[\zeta_7] : \mathbb{Q}] = 6$ (ver Teorema 3.24), e então a Lei da Torre (ver Proposição 3.11) garante que $[\mathbb{Q}[\sqrt[7]{5}, \zeta_7] : \mathbb{Q}] = 7.6 = 42 \leq 7!$

4.2 Extensões Normais e Galoisianas

Definição 4.4. Seja $\mathbb{L} \mid \mathbb{K}$ uma extensão algébrica, chamamos de *extensão normal*, se todo polinômio irredutível em $\mathbb{K}$ que tenha uma raiz em $\mathbb{L}$, possuir todas as suas raízes em $\mathbb{L}$.

Do exemplo citado na seção anterior, podemos afirmar que a extensão $\mathbb{Q}[\sqrt[3]{2}, \zeta_3] \mid \mathbb{Q}$ é uma extensão normal, enquanto que $\mathbb{Q}[\sqrt[3]{2}] \mid \mathbb{Q}$, não é, pois um polinômio que contenha uma raiz em $\mathbb{Q}[\sqrt[3]{2}]$ seria $x^3 - 2$, porém ele não possui suas outras raízes nessa mesma extensão, diferente do que acontece na extensão $\mathbb{Q}[\sqrt[3]{2}, \zeta_3]$.

Vimos na definição 2.20 a definição de um polinômio separável. Podemos definir então uma *extensão separável*.

Definição 4.5. Seja $\mathbb{L} \mid \mathbb{K}$ uma extensão, ela será separável se todo elemento de $\mathbb{L}$ for raiz de um polinômio separável com coeficientes em $\mathbb{K}$.

Vale ressaltar ainda que, como vimos, por tratarmos de subcorpos de $\mathbb{C}$, todos os polinômios irredutíveis são separáveis.

Definição 4.6. Seja $\mathbb{L} \mid \mathbb{K}$ uma extensão, ela é dita *extensão galoisiana* se ela for normal e separável. Como trabalhamos com extensões que são subcorpos de $\mathbb{C}$, então elas serão sempre separáveis. Sendo assim uma extensão será galoisiana se, e somente se, for normal.

Seja $\mathbb{M}$ um subcorpo intermediário da extensão galoisiana $\mathbb{L} \mid \mathbb{K}$, pode-se afirmar que $\mathbb{L} \mid \mathbb{M}$ é galoisiana, porém $\mathbb{M} \mid \mathbb{K}$, não é necessariamente galoisiana. Usando o mesmo exemplo, seja $\mathbb{K} = \mathbb{Q}$, $\mathbb{M} = \mathbb{Q}[\sqrt[3]{2}]$ e $\mathbb{L} = \mathbb{Q}[\sqrt[3]{2}, \zeta_3]$, facilmente verificamos tal afirmação.

4.3 Automorfismos de Corpos

No capítulo 1, ao estudar grupos, vimos a definição de homomorfismos, e mais particularmente de automorfismos. Agora vejamos a definição para corpos, que ocorre de maneira similar.

Definição 4.7. Seja $\mathbb{K}$ um corpo, e σ uma bijeção, tal que $\sigma : \mathbb{K} \to \mathbb{K}$ e preserva a soma e o produto de modo que, $\forall a, b \in \mathbb{K}$:

$$\sigma(a + b) = \sigma(a) + \sigma(b)$$
$$\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$$

À essa bijeção σ denominamos *automorfismo*. E denotaremos por $\operatorname{Aut}\mathbb{K}$ o conjunto de todos os automorfismos de $\mathbb{K}$.

Proposição 4.8. *O conjunto dos automorfismos de um corpo* $\mathbb{L}$, $\operatorname{Aut}\mathbb{L}$ *é um grupo com a operação composição.*

Demonstração. Sabe-se que o corpo satisfaz todas as propriedades de grupo. Sendo assim, a prova segue análoga à da Proposição 1.29. □

Dada a extensão $\mathbb{L} \mid \mathbb{K}$, nos interessa o estudos dos automorfismos dessa extensão, ditos os automorfismos de $\mathbb{L}$, que preservam $\mathbb{K}$, denotaremos o conjunto desses automorfismos por $\mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$. Entendam por preservar, manter todos os elementos do corpo base, $\mathbb{K}$ inalterados.

Definição 4.9. O grupo de automorfismos de uma extensão é chamado de Grupo de Galois:

$$\mathrm{Aut}_{\mathbb{K}}\,\mathbb{L} := \{\sigma : \mathbb{L} \to \mathbb{L}; \sigma(k) = k, \forall k \in \mathbb{K}\}$$

Proposição 4.10. *Seja $\sigma \in \mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$, $f(x) \in \mathbb{K}[x]$ e α é raiz de $f(x)$, então $\sigma(\alpha)$ também é uma raiz de $f(x)$.*

Demonstração. Inicialmente, mostremos que $\sigma(f(x)) = f(\sigma(x))$.

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

Portanto,

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

Como $f(\alpha) = 0$ e todo automorfismo leva zero nele próprio:

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

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

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

Logo, o automorfismo leva uma raiz de $f(x)$ em outra raiz.

□

Proposição 4.11. *O grupo $\mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$, definido anteriormente é um subgrupo de $\mathrm{Aut}\,\mathbb{L}$.*

Demonstração. Da Proposição 4.8, sabemos que $\mathrm{Aut}\,\mathbb{L}$ é um grupo com a operação composição de funções. Usando a Proposição 1.4, devemos mostrar que dados $\sigma, \psi \in \mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$, teremos $\sigma \circ \psi \in \mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$ e $\sigma^{-1} \in \mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$, vejamos.

Seja $x \in \mathbb{K}$, da definição de automorfismo e da definição de $\mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$,

$$(\sigma \circ \psi)(x) = \sigma(\psi(x)) = \sigma(x) = x$$

Garantindo assim a primeira condição. Teremos também $\sigma^{-1} \in \mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$, pois

$$x = \sigma^{-1}\sigma(x) = \sigma^{-1}(x)$$

Concluímos assim, que $\mathrm{Aut}_{\mathbb{K}}\,\mathbb{L} \leq \mathrm{Aut}\,\mathbb{L}$.

□

O grupo $\mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$ também admite subgrupos. Dada a extensão $\mathbb{L} \mid \mathbb{K}$, e sendo $\mathbb{M}$ um corpo intermediário, ou seja $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$, temos que $\mathrm{Aut}_{\mathbb{M}}\,\mathbb{L} \leq \mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$, veremos mais detalhes na seção 4.4, quando faremos um estudo sobre a Correspondência de Galois.

Teorema 4.12. *Seja $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$, e $\mathbb{L} \mid \mathbb{K}$ uma extensão galoisiana. Se a extensão $\mathbb{M} \mid \mathbb{K}$ for galoisiana, então $\mathrm{Aut}_{\mathbb{M}}\,\mathbb{L} \trianglelefteq \mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$.*

Demonstração. De modo análogo ao que fizemos na proposição 4.11, teremos que $\mathrm{Aut}_{\mathbb{M}}\,\mathbb{L} \leq \mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$.

Agora, seja $H = \mathrm{Aut}_{\mathbb{M}}\,\mathbb{L}$ e $G = \mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$, devemos mostrar que $H \trianglelefteq G$.

Da Definição 2.15 temos que $H \trianglelefteq G$ se $gHg^{-1} = H,\ \forall g \in G$.

Seja $h \in H$ e $g \in G$, devemos ter,

$$ghg^{-1} \in H \text{ ou seja, } ghg^{-1}(x) \in \mathbb{M},\ \forall x \in \mathbb{M}$$

Seja $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ uma base da extensão $\mathbb{M} \mid \mathbb{K}$, então se $x \in \mathbb{M}$, temos que,

$$x = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n, \text{ com } a_1, a_2, \ldots, a_n \in \mathbb{K}$$

E fazendo $ghg^{-1}(x)$ teremos:

$$\begin{aligned} ghg^{-1}(x) &= ghg^{-1}(a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n) \\ &= a_1ghg^{-1}(\alpha_1) + a_2ghg^{-1}(\alpha_2) + \cdots + a_nghg^{-1}(\alpha_n) \end{aligned}$$

E de acordo com a Proposição 4.10, temos que, se $p(x) \in \mathbb{K}[x]$ é o polinômio minimal de α, o fato de $\mathbb{M} \mid \mathbb{K}$ ser uma extensão normal faz com que todas as raízes de $p(x) = 0$ estejam em $\mathbb{M}$. Como g é um automorfismo então $g(\alpha)$ será uma outra raiz de $p(x)$ e portanto está em M. Repetindo-se esse procedimento para os elementos $\alpha_1, \alpha_2, \ldots, \alpha_n$, concluímos que $g(x) \in M$ para todo $x \in M$. Analogamente, $g^{-1}(x) \in \mathbb{M}$. Por fim,

$$ghg^{-1}(x) = g(h(g^{-1}(x))) = gg^{-1}(x) = x \ \in \mathbb{M}$$

Como queríamos demonstrar.

□

Teorema 4.13. *Seja $\mathbb{L} \mid \mathbb{K}$ uma extensão finita. Então as seguintes condições são equivalentes:*

(a) $\mathbb{L} \mid \mathbb{K}$ *galoisiana;*

(b) $\mathbb{L} \mid \mathbb{K}$ *normal;*

(c) $[\mathbb{L} : \mathbb{K}] = |\operatorname{Aut}_{\mathbb{K}} \mathbb{L}|$.

Demonstração. $(a) \Longrightarrow (b)$: segue da Definição 4.6.

$(b) \Longrightarrow (c)$: Seja $p(x) \in \mathbb{K}[x]$ o polinômio minimal de α, tal que $\mathbb{L} = \mathbb{K}(\alpha)$, e seja ainda $\sigma \in \operatorname{Aut}_{\mathbb{K}} \mathbb{L}$. Como sabemos, $\sigma(\alpha) = \alpha'$, onde α' é também raiz de $p(x)$ e $\alpha' \in \mathbb{L}$. Logo $\mathbb{K}[\alpha'] \subset \mathbb{L}$ e $[\mathbb{K}[\alpha'] : \mathbb{K}] = [\mathbb{L} : \mathbb{K}] = \partial p(x)$ então $\mathbb{L} = \mathbb{K}[\alpha] = \mathbb{K}[\alpha']$. Como σ fica determinado com o quê faz com α, então $|\operatorname{Aut}_{\mathbb{K}} \mathbb{L}|$ é no máximo igual a quantidade de raízes de $p(x)$, que é no máximo $\partial p(x) = [\mathbb{L} : \mathbb{K}]$, logo $|\operatorname{Aut}_{\mathbb{K}} \mathbb{L}| \leq [\mathbb{L} : \mathbb{K}]$.

O leitor pode em [2], consultar a prova de que $[\mathbb{L} : \mathbb{K}] \leq |\operatorname{Aut}_{\mathbb{K}} \mathbb{L}|$, e então $[\mathbb{L} : \mathbb{K}] = |\operatorname{Aut}_{\mathbb{K}} \mathbb{L}|$.

$(c) \Longrightarrow (a)$ Supondo $[\mathbb{L} : \mathbb{K}] = |\operatorname{Aut}_{\mathbb{K}} \mathbb{L}|$, mostremos que $\mathbb{L} \mid \mathbb{K}$ é galoisiana.

Seja $p(x)$ o polinômio separável e minimal de α, e $\mathbb{L} = \mathbb{K}[\alpha]$. Seja ainda $\sigma \in \operatorname{Aut}_{\mathbb{K}} \mathbb{L}$, tem-se que $\sigma(\alpha) \in \mathbb{L}$ e é outra raiz de $p(x)$. Assim $|\operatorname{Aut}_{\mathbb{K}} \mathbb{L}|$ é menor ou igual ao número de raízes de $p(x)$. Agora, como $[\mathbb{L} : \mathbb{K}] = |\operatorname{Aut}_{\mathbb{K}} \mathbb{L}|$, teremos $|\operatorname{Aut}_{\mathbb{K}} \mathbb{L}| = \partial p(x)$ que é igual ao número de raízes de $p(x)$ em $\mathbb{L}$. Segue que $\mathbb{L}$ contém todas as raízes de $p(x)$, e portanto $\mathbb{L} = \operatorname{Gal}(p(x), \mathbb{K})$, e $\mathbb{L} \mid \mathbb{K}$ é galoisiana. □

Proposição 4.14. *Se $\mathbb{L} \mid \mathbb{K}$ é o corpo de decomposição de um polinômio de grau n em $\mathbb{K}$, então $\operatorname{Aut}_{\mathbb{K}} \mathbb{L}$ é isomorfo a um subgrupo de S_n (grupo das permutações de n elementos).*

Demonstração. Seja $\sigma \in \operatorname{Aut}_{\mathbb{K}} \mathbb{L}$, $p(x)$ o polinômio de grau n que se decompõe na extensão $\mathbb{L} \mid \mathbb{K}$, α uma raiz de $p(x)$ e ω o conjunto das n raízes de $p(x)$. Como sabemos, o automorfismo leva uma raiz de um polinômio em outra, assim, $\sigma(\alpha)$ é também uma raiz de $p(x)$, ou seja, os automorfismos permutam as raízes de $p(x)$. Como temos n raízes sendo permutadas, e diante do que já vimos sobre o grupo das permutações, podemos concluir que o conjunto dos automorfismos é um subconjunto do conjunto das permutações de n elementos, portanto $\operatorname{Aut}_{\mathbb{K}} \mathbb{L}$ é isomorfo à um subgrupo de S_n.

□

No intuito de ilustrar o que foi visto nessa seção, vejamos um exemplo:

Exemplo 4.15. Usando o exemplo que vinhamos tratando, determinemos o grupo de Galois da extensão $\operatorname{Gal}(x^3 - 2, \mathbb{Q})$.

Vimos no Exemplo 4.2 que o corpo de decomposição de $p(x) = x^3 - 2$ é $\mathbb{Q}[\sqrt[3]{2}, \zeta_3]$.

Da Lei da Torre, temos que:

$$\begin{aligned}[\mathbb{Q}[\sqrt[3]{2},\zeta_3]:\mathbb{Q}] &= [\mathbb{Q}[\sqrt[3]{2},\zeta_3]:\mathbb{Q}[\sqrt[3]{2}]]\cdot[\mathbb{Q}[\sqrt[3]{2}]:\mathbb{Q}] \\ &= 2\cdot 3 \\ &= 6\end{aligned}$$

E do item (c) do Teorema 4.13, temos que $|\operatorname{Aut}_{\mathbb{Q}}\mathbb{Q}[\sqrt[3]{2},\zeta_3]| = 6$.

Seja $x \in \mathbb{Q}[\sqrt[3]{2},\zeta_3]$, tal que,

$$x = a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2^2} + a_3\zeta_3 + a_4\sqrt[3]{2}\zeta_3 + a_5\sqrt[3]{2^2}\zeta_3$$

Com $a_i \in \mathbb{Q}$ e $i = 1,2,3,4,5$.

Seja ainda $\sigma \in \operatorname{Aut}_{\mathbb{Q}}\mathbb{Q}[\sqrt[3]{2},\zeta_3]$, tal que $\sigma(a) = a,\ \forall a \in \mathbb{Q}$. Fazendo $\sigma(x)$ teremos:

$$\begin{aligned}\sigma(x) &= \sigma(a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2^2} + a_3\zeta_3 + a_4\sqrt[3]{2}\zeta_3 + a_5\sqrt[3]{2^2}\zeta_3) \\ &= \sigma(a_0) + \sigma(a_1\sqrt[3]{2}) + \sigma(a_2\sqrt[3]{2^2}) + \sigma(a_3\zeta_3) + \sigma(a_4\sqrt[3]{2}\zeta_3) + \sigma(a_5\sqrt[3]{2^2}\zeta_3) \\ &= a_0 + \sigma(a_1)\sigma(\sqrt[3]{2}) + \sigma(a_2)\sigma(\sqrt[3]{2^2}) + \sigma(a_3)\sigma(\zeta_3) + \sigma(a_4)\sigma(\sqrt[3]{2}\zeta_3) + \sigma(a_5)\sigma(\sqrt[3]{2^2}\zeta_3) \\ &= a_0 + a_1\sigma(\sqrt[3]{2}) + a_2\sigma(\sqrt[3]{2^2}) + a_3\sigma(\zeta_3) + a_4\sigma(\sqrt[3]{2}\zeta_3) + a_5\sigma(\sqrt[3]{2^2}\zeta_3) \\ &= a_0 + a_1\sigma(\sqrt[3]{2}) + a_2\sigma(\sqrt[3]{2})^2 + a_3\sigma(\zeta_3) + a_4\sigma(\sqrt[3]{2})\sigma(\zeta_3) + a_5\sigma(\sqrt[3]{2})^2\sigma(\zeta_3) \\ &= a_0 + a_1\sigma(\sqrt[3]{2}) + a_2(\sigma(\sqrt[3]{2}))^2 + a_3\sigma(\zeta_3) + a_4\sigma(\sqrt[3]{2})\sigma(\zeta_3) + a_5(\sigma(\sqrt[3]{2}))^2\sigma(\zeta_3)\end{aligned}$$

Como $\sqrt[3]{2}$ e ζ_3 não pertencem à $\mathbb{Q}$, notemos que os automorfismos são caracterizado pelo que eles fazem com $\sqrt[3]{2}$ e ζ_3. Sabemos que as raízes de $p(x) = x^3 - 2$ são $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta_3$, e $\sqrt[3]{2}\zeta_3^2$, e que as raízes 3-ésimas da unidade são ζ_3 e ζ_3^2. Dessa forma, podemos definir os automorfismos de $\operatorname{Aut}_{\mathbb{Q}}\mathbb{Q}[\sqrt[3]{2},\zeta_3]$, como sendo σ_{ij}, onde os índices i e j serão tais que o índice i caracteriza o que σ_{ij} faz com $\sqrt[3]{2}$ e o índice j, pelo que faz com ζ_3. Sendo que o índice i leva $\sqrt[3]{2}$ nas três raízes do polinômio, por isso $i = 1,2,3$ e o índice j leva ζ_3 nas raízes 3-ésimas primitivas da unidade, por isso $j = 1,2$. Vejamos a essa descrição na tabela abaixo:

σ_{ij}	$\sigma_{ij}(\sqrt[3]{2})$	$\sigma_{ij}(\zeta_3)$
$\sigma_{11} = e$	$\sqrt[3]{2}$	ζ_3
σ_{12}	$\sqrt[3]{2}$	ζ_3^2
σ_{21}	$\sqrt[3]{2}\zeta_3$	ζ_3
σ_{22}	$\sqrt[3]{2}\zeta_3$	ζ_3^2
σ_{31}	$\sqrt[3]{2}\zeta_3^2$	ζ_3
σ_{32}	$\sqrt[3]{2}\zeta_3^2$	ζ_3^2

Enfim, concluímos que $\operatorname{Aut}_{\mathbb{Q}}\mathbb{Q}[\sqrt[3]{2},\zeta_3] = \{e = \sigma_{11},\sigma_{12},\sigma_{21},\sigma_{22},\sigma_{31},\sigma_{32}\}$.

Vale ainda ressaltar, que comprova-se aqui a proposição 4.14, uma vez que nosso polinômio tem grau 3, e o grupo $\operatorname{Aut}_{\mathbb{Q}}\mathbb{Q}[\sqrt[3]{2},\zeta_3]$ que encontramos, é isomorfo a um subgrupo de S_3, precisamente ao próprio S_3.

4.4 Correspondência de Galois

A chamada *Correspondência de Galois*, estuda basicamente a relação entre uma extensão galoisiana e seus corpos intermediários, com seu grupo de Galois e seus subgrupos.

Antes de enunciarmos de fato o principal teorema, vale ressaltar que dada uma extensão galoisiana $\mathbb{L} \mid \mathbb{K}$, então $\mathbb{K}$ é o *corpo preservado* pelos automorfismos de $\mathbb{L}$ pertencentes ao grupo $\mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$.Vejamos agora o teorema que é fruto dos principais resultados da Teoria de Galois.

Teorema 4.16. *(Teorema Fundamental da Teoria de Galois)*

Seja $\mathbb{L} \mid \mathbb{K}$ uma extensão galoisiana, $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$ e Δ o conjunto de todos os corpos intermediários dessa extensão, ou seja, $\Delta := \{\mathbb{M} \mid \mathbb{K} \subset \mathbb{M} \subset \mathbb{L}\}$. Seja ainda Θ o conjunto dos subgrupos de $\mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$, ou seja, $\Theta := \{\mathrm{Aut}_{\mathbb{M}}\,\mathbb{L} \mid \mathbb{K} \subset \mathbb{M} \subset \mathbb{L}\}$. Por fim, considere a aplicação:

$$\begin{array}{rccc} \psi & : & \Delta & \to & \Theta \\ & & \mathbb{M} & \mapsto & \mathrm{Aut}_{\mathbb{M}}\,\mathbb{L} \end{array}.$$

Então:

i. *ψ é uma bijeção;*

ii. *Assim como temos que $[\mathbb{L} : \mathbb{K}] = |\,\mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}|$, temos também que $[\mathbb{L} : \mathbb{M}] = |\,\mathrm{Aut}_{\mathbb{M}}\,\mathbb{L}|$ e $[\mathbb{M} : \mathbb{K}] = \left|\dfrac{\mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}}{\mathrm{Aut}_{\mathbb{M}}\,\mathbb{L}}\right|$;*

iii. *Se $\mathbb{K} \subset \mathbb{M}_1 \subset \mathbb{M}_2 \subset \mathbb{L}$, então $\mathrm{Aut}_{\mathbb{K}}\,\mathbb{L} \geq \mathrm{Aut}_{\mathbb{M}_1}\,\mathbb{L} \geq \mathrm{Aut}_{\mathbb{M}_2}\,\mathbb{L}$;*

iv. *Como vimos, se $\mathbb{L} \mid \mathbb{K}$ é galoisiana, então $\mathbb{L} \mid \mathbb{M}$ é galoisiana, já $\mathbb{M} \mid \mathbb{K}$ é galoisiana se, e somente se, $\mathrm{Aut}_{\mathbb{M}}\,\mathbb{L} \trianglelefteq \mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$. Se for esse o caso, então $\mathrm{Aut}_{\mathbb{K}}\,\mathbb{M} \simeq \dfrac{\mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}}{\mathrm{Aut}_{\mathbb{M}}\,\mathbb{L}}$;*

Demonstração. *i.* Seja $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$, podemos associar $\mathbb{M}$ ao automorfismo $\mathrm{Aut}_{\mathbb{M}}\,\mathbb{L}$ que é um subgrupo de $\mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}$.

Seja $\mathbb{K} \subset \mathbb{M}_1, \mathbb{M}_2 \subset \mathbb{L}$. Suponha que $\mathrm{Aut}_{\mathbb{M}_1}\,\mathbb{L} = \mathrm{Aut}_{\mathbb{M}_2}\,\mathbb{L}$. Agora, seja $\sigma \in \mathrm{Aut}_{\mathbb{M}_1}\,\mathbb{L} = \mathrm{Aut}_{\mathbb{M}_2}\,\mathbb{L}$. Seja $\alpha \in \mathbb{M}_1$ então $\sigma(\alpha) = \alpha$, assim $\alpha \in \mathbb{M}_2$, pois $\sigma \in \mathrm{Aut}_{\mathbb{M}_2}\,\mathbb{L}$, e portanto $\mathbb{M}_1 \subset \mathbb{M}_2$. Analogamente, $\mathbb{M}_2 \subset \mathbb{M}_1$. Dessa forma, temos que $\mathbb{M}_1 = \mathbb{M}_2$, provando assim que ψ é injetiva.

Agora, seja $G \subset \Theta$, tome $\mathbb{M}' = \{\alpha \in \mathbb{L} | h(\alpha) = \alpha,\ \forall h \in G\}$. Temos que $\mathbb{K} \subset \mathbb{M}'$ pois $h(\alpha) = \alpha, \forall \alpha \in \mathbb{K}$ e $h \in G$. Se $\alpha, \beta \in \mathbb{M}'$ temos:

$$h(\alpha + \beta) = h(\alpha) + h(\beta) = \alpha + \beta$$

$$h(\alpha \cdot \beta) = h(\alpha) \cdot h(\beta) = \alpha \cdot \beta$$

Note que 0 e 1 estão em $\mathbb{M}'$ trivialmente. Temos ainda que o elemento simétrico e o elemento inverso pertencem a $\mathbb{M}'$, pois seja $\alpha \in \mathbb{M}'$, então:

$$h(-\alpha) + \alpha = h(-\alpha) + h(\alpha) = h(-\alpha + \alpha) = h(0) = 0.$$

Logo $h(-\alpha) = -\alpha$. Agora, seja $\alpha \in \mathbb{M}'$ com $\alpha \neq 0$, então:

$$h(\alpha^{-1}) \cdot \alpha = h(\alpha^{-1}) \cdot h(\alpha) = h(\alpha^{-1} \cdot \alpha) = h(1) = 1.$$

Logo $h(\alpha^{-1}) = \alpha^{-1}$.

Portanto $\mathbb{M}'$ é um corpo e temos $\mathbb{K} \subset \mathbb{M}' \subset \mathbb{L}$. Então $\exists \mathbb{M}'$ tal que $G = \operatorname{Aut}_{\mathbb{M}'} \mathbb{L}$, onde $\psi(\mathbb{M}') = \operatorname{Aut}_{\mathbb{M}'} \mathbb{L}$. Logo ψ é também sobrejetiva, e portanto bijetiva.

ii. Já demonstramos no item *c* da Proposição 4.13 que $[\mathbb{L} : \mathbb{K}] = |\operatorname{Aut}_{\mathbb{K}} \mathbb{L}|$, e de modo análogo teremos que $[\mathbb{L} : \mathbb{M}] = |\operatorname{Aut}_{\mathbb{M}} \mathbb{L}|$. Da Lei da Torre, vista na proposição 3.11:

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{M}][\mathbb{M} : \mathbb{K}] \Longrightarrow |\operatorname{Aut}_{\mathbb{K}} \mathbb{L}| = |\operatorname{Aut}_{\mathbb{M}} \mathbb{L}|[\mathbb{M} : \mathbb{K}] \Longrightarrow$$

$$[\mathbb{M} : \mathbb{K}] = \frac{|\operatorname{Aut}_{\mathbb{K}} \mathbb{L}|}{|\operatorname{Aut}_{\mathbb{M}} \mathbb{L}|}$$

Por fim, do Lema 1.23 e do Teorema 4.12, segue que,

$$[\mathbb{M} : \mathbb{K}] = \left| \frac{\operatorname{Aut}_{\mathbb{K}} \mathbb{L}}{\operatorname{Aut}_{\mathbb{M}} \mathbb{L}} \right|.$$

iii. Da cadeia $\mathbb{K} \subset \mathbb{M}_1 \subset \mathbb{M}_2 \subset \mathbb{L}$, e como, por hipótese temos que $\mathbb{L} \mid \mathbb{K}$ é galoisiana, como já sabemos, $\mathbb{L} \mid \mathbb{M}_1$ e $\mathbb{L} \mid \mathbb{M}_2$ também serão galoisianas.

Do Teorema 4.12, temos que, da extensão $\mathbb{L} \mid \mathbb{M}_1$, $\operatorname{Aut}_{\mathbb{K}} \mathbb{L} \trianglerighteq \operatorname{Aut}_{\mathbb{M}_1} \mathbb{L}$ e de $\mathbb{L} \mid \mathbb{M}_2$, $\operatorname{Aut}_{\mathbb{M}_1} \mathbb{L} \trianglerighteq \operatorname{Aut}_{\mathbb{M}_2} \mathbb{L}$. Portanto:

$$\operatorname{Aut}_{\mathbb{K}} \mathbb{L} \trianglerighteq \operatorname{Aut}_{\mathbb{M}_1} \mathbb{L} \trianglerighteq \operatorname{Aut}_{\mathbb{M}_2} \mathbb{L}.$$

Como usamos $\trianglerighteq$ para classificar subgrupos normais, que são simplesmente subgrupos, podemos reescrever essa sentença usando $\geq$:

$$\operatorname{Aut}_{\mathbb{K}} \mathbb{L} \geq \operatorname{Aut}_{\mathbb{M}_1} \mathbb{L} \geq \operatorname{Aut}_{\mathbb{M}_2} \mathbb{L}.$$

iv. Análogo ao que fizemos no item anterior, como $\mathbb{L} \mid \mathbb{K}$ é galoisiana, $\mathbb{L} \mid \mathbb{M}$ também é, logo, segue do Teorema 4.12 que,

$$\mathrm{Aut}_{\mathbb{M}}\,\mathbb{L} \trianglelefteq \mathrm{Aut}_{\mathbb{K}}\,\mathbb{L}.$$

Seja

$$\begin{array}{rccc} f: & \mathrm{Aut}_{\mathbb{K}}\mathbb{L} & \to & \mathrm{Aut}_{\mathbb{K}}\mathbb{M} \\ & \sigma & \mapsto & \sigma\mid_{\mathbb{M}} \end{array},$$

onde $\sigma\mid_{\mathbb{M}}$ são os automorfismos restritos aos elementos de $\mathbb{M}$.

Note que como $\mathbb{M} \mid \mathbb{K}$ é galoisiana então, dado $\alpha \in \mathbb{M}$, tal que α é raiz de um polinômio minimal em $\mathbb{M}[x]$, de acordo com a Proposição 4.10, $\sigma(\alpha) \in \mathbb{M}$, e portanto a função f está bem definida e facilmente verifica-se que f é um homomorfismo de grupos e que é sobrejetivo.

O núcleo de f, denotado por $\mathrm{Ker}(f)$, são todos os automorfismos $\sigma \in \mathrm{Aut}_{\mathbb{K}}\mathbb{L}$ tais que $\sigma\mid_{\mathbb{M}} = \mathrm{id}_{\mathbb{M}}$, ou seja, $\mathrm{Ker}(f) = \mathrm{Aut}_{\mathbb{M}}\mathbb{L}$. Como $\mathrm{Aut}_{\mathbb{M}}\mathbb{L} \trianglelefteq \mathrm{Aut}_{\mathbb{K}}\mathbb{L}$, então, pelo Teorema 4.12, temos bem definido o grupo $\dfrac{\mathrm{Aut}_{\mathbb{K}}\mathbb{L}}{\mathrm{Aut}_{\mathbb{M}}\mathbb{L}}$ e temos que a aplicação:

$$\begin{array}{rccc} \bar{f}: & \dfrac{\mathrm{Aut}_{\mathbb{K}}\mathbb{L}}{\mathrm{Aut}_{\mathbb{M}}\mathbb{L}} & \to & \mathrm{Aut}_{\mathbb{K}}\mathbb{M} \\ & \bar{\sigma} & \mapsto & \sigma\mid_{\mathbb{M}} \end{array}$$

E de acordo com o Teorema 1.28, $\bar{f}$ é um isomorfismo. Então concluímos que $\mathrm{Aut}_{\mathbb{K}}\mathbb{M} \simeq \dfrac{\mathrm{Aut}_{\mathbb{K}}\mathbb{L}}{\mathrm{Aut}_{\mathbb{M}}\mathbb{L}}$.

□

Continuando a trabalhar com o polinômio $p(x) = x^3 - 2$, vejamos num exemplo como acontece a relação estabelecida com a Correspondência de Galois.

Exemplo 4.17. Estabeleça a relação entre a extensão $\mathbb{Q}[\sqrt[3]{2}, \zeta_3] \mid \mathbb{Q}$ e seus subcorpos, com o grupo $\mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}[\sqrt[3]{2}, \zeta_3]$ e seus subgrupos.

Na seção 1.7.1, determinamos todos os subgrupos de S_3, a saber: $H_1 = \{e\}; H_2 = \{e, \alpha\beta\}; H_3 = \{e, \alpha\}; H_4 = \{e, \beta\alpha\}; H_5 = \{e, \beta, \beta^2\}$; e $H_6 = S_3$.

Enumeremos as três raízes de $p(x) = x^3 - 2$, a saber $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta_3$, $\sqrt[3]{2}\zeta_3^2$, respectivamente por 1, 2 e 3. Observamos o quê cada σ_{ij} faz com $\sqrt[3]{2}$ e ζ_3, através da tabela do exemplo 4.15:

$$\sigma_{11}: \begin{pmatrix} \sqrt[3]{2} & \sqrt[3]{2}\zeta_3 & \sqrt[3]{2}\zeta_3^2 \\ \downarrow & \downarrow & \downarrow \\ \sqrt[3]{2} & \sqrt[3]{2}\zeta_3 & \sqrt[3]{2}\zeta_3^2 \end{pmatrix} \Longrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$$

$$\sigma_{12}: \begin{pmatrix} \sqrt[3]{2} & \sqrt[3]{2}\zeta_3 & \sqrt[3]{2}\zeta_3^2 \\ \downarrow & \downarrow & \downarrow \\ \sqrt[3]{2} & \sqrt[3]{2}\zeta_3^2 & \sqrt[3]{2}\zeta_3 \end{pmatrix} \Longrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \alpha\beta$$

$$\sigma_{21}: \begin{pmatrix} \sqrt[3]{2} & \sqrt[3]{2}\zeta_3 & \sqrt[3]{2}\zeta_3^2 \\ \downarrow & \downarrow & \downarrow \\ \sqrt[3]{2}\zeta_3 & \sqrt[3]{2}\zeta_3^2 & \sqrt[3]{2} \end{pmatrix} \Longrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \beta$$

$$\sigma_{22}: \begin{pmatrix} \sqrt[3]{2} & \sqrt[3]{2}\zeta_3 & \sqrt[3]{2}\zeta_3^2 \\ \downarrow & \downarrow & \downarrow \\ \sqrt[3]{2}\zeta_3 & \sqrt[3]{2} & \sqrt[3]{2}\zeta_3^2 \end{pmatrix} \Longrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \alpha$$

$$\sigma_{31}: \begin{pmatrix} \sqrt[3]{2} & \sqrt[3]{2}\zeta_3 & \sqrt[3]{2}\zeta_3^2 \\ \downarrow & \downarrow & \downarrow \\ \sqrt[3]{2}\zeta_3^2 & \sqrt[3]{2} & \sqrt[3]{2}\zeta_3 \end{pmatrix} \Longrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \beta^2$$

$$\sigma_{32}: \begin{pmatrix} \sqrt[3]{2} & \sqrt[3]{2}\zeta_3 & \sqrt[3]{2}\zeta_3^2 \\ \downarrow & \downarrow & \downarrow \\ \sqrt[3]{2}\zeta_3^2 & \sqrt[3]{2}\zeta_3 & \sqrt[3]{2} \end{pmatrix} \Longrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \beta\alpha$$

Com isso podemos determinar os subgrupos de $\mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}[\sqrt[3]{2}, \zeta_3]$, através da relação de isomorfismo com os subgrupos de S_3. Chamemos de J_k os subgrupos de $\mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}[\sqrt[3]{2}, \zeta_3]$:

$$H_1 = \{e\} \simeq \{\sigma_{11}\} = J_1$$

$$H_2 = \{e, \alpha\beta\} \simeq \{\sigma_{11}, \sigma_{12}\} = J_2$$

$$H_3 = \{e, \alpha\} \simeq \{\sigma_{11}, \sigma_{22}\} = J_3$$

$$H_4 = \{e, \beta\alpha\} \simeq \{\sigma_{11}, \sigma_{32}\} = J_4$$

$$H_5 = \{e, \beta, \beta^2\} \simeq \{\sigma_{11}, \sigma_{22}, \sigma_{31}\} = J_5$$

$$H_6 = \{e, \alpha\beta, \alpha, \beta, \beta^2, \beta\alpha\} \simeq \{\sigma_{11}, \sigma_{12}, \sigma_{22}, \sigma_{21}, \sigma_{31}, \sigma_{32}\} = J_6$$

E agora, relacionemos cada subgrupo J_k de $\mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}[\sqrt[3]{2}, \zeta_3]$ à um subcorpo $\mathbb{M}_k$ de $\mathbb{Q}[\sqrt[3]{2}, \zeta_3] \mid \mathbb{Q}$:

$$J_1 \Longrightarrow \mathbb{M}_1 = \mathbb{Q}[\sqrt[3]{2}, \zeta_3]$$

$$J_2 \Longrightarrow \mathbb{M}_2 = \mathbb{Q}[\sqrt[3]{2}]$$

$$J_3 \Longrightarrow \mathbb{M}_3 = \mathbb{Q}[\sqrt[3]{2}\zeta_3^2]$$

$$J_4 \Longrightarrow \mathbb{M}_4 = \mathbb{Q}[\sqrt[3]{2}\zeta_3]$$

$$J_5 \Longrightarrow \mathbb{M}_5 = \mathbb{Q}[\zeta_3]$$

$$J_6 \Longrightarrow \mathbb{M}_6 = \mathbb{Q}$$

Assim, J_k é o grupo de automorfismos de $\mathbb{Q}[\sqrt[3]{2}, \zeta_3]$ que preserva $\mathbb{M}_k$, ou seja, $J_k = \mathrm{Aut}_{\mathbb{M}_k} \mathbb{Q}[\sqrt[3]{2}, \zeta_3]$.

A titulo de curiosidade, vejamos que em J_3 além da identidade, tem-se σ_{22}, e então $\sigma_{22}(\sqrt[3]{2}\zeta_3^2) = \sigma_{22}(\sqrt[3]{2})\sigma_{22}(\zeta_3^2) = \sqrt[3]{2}\zeta_3\zeta_3 = \sqrt[3]{2}\zeta_3^2$, então, de fato, σ_{22} preserva $\mathbb{Q}[\sqrt[3]{2}\zeta_3^2]$.

Por fim, sobre o grupo de Galois e extensões envolvendo raízes n-ésimas, vale destacar:

Proposição 4.18. *Tome $\mathbb{K}$ um subcorpo de $\mathbb{C}$ e $\zeta_n \in \mathbb{C}$ uma raiz n-ésima primitiva da unidade. Então a extensão $\mathbb{K}[\zeta_n] \mid \mathbb{K}$ é galoisiana e seu grupo de Galois é isomorfo a um subgrupo de $\mathbb{Z}_n^*$, sendo portanto abeliano.*

Demonstração. Ver demonstração em [5] ou [15]. □

Proposição 4.19. *Seja $\mathbb{K}$ um subcorpo de $\mathbb{C}$ que contém, uma raiz n-ésima primitiva da unidade. Dado $\alpha \in \mathbb{C}$ tal que $\alpha^n \in \mathbb{K}$, então a extensão $\mathbb{K}[\alpha] \mid \mathbb{K}$ é galoisiana e seu grupo de Galois é cíclico.*

Demonstração. Ver demonstração em [15]. □

Teorema 4.20. *Seja $\mathbb{L} \mid \mathbb{K}$ uma extensão de grau n. Se $\mathrm{Aut}_{\mathbb{K}} \mathbb{L}$ é um grupo cíclico, e se $\mathbb{L}$ contem uma raíz n-ésima primitiva da unidade, então $\exists a \in \mathbb{K}$ com $a \neq 0$ tal que $x^n - a$ seja irredutível em $\mathbb{K}[x]$ e $\mathbb{L} = \mathrm{Gal}(x^n - a, \mathbb{K})$. Além disso, $\forall \alpha \in \mathbb{L}$ tal que $\alpha^n = a$ temos $\mathbb{L} = \mathbb{K}[\alpha]$.*

Demonstração. Ver demonstração em [6]. □

Teorema 4.21. *Se ζ_n é uma raiz n-ésima primitiva da unidade. Então $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \phi(n)$. Consequentemente $\mathrm{Aut}_{\mathbb{Q}} \mathbb{Q}[\zeta_n] \simeq \mathbb{Z}_n^*$.*

Demonstração. Ver demonstração em [15]. □

Capítulo 5

Solubilidade por Radicais

Neste capítulo, definiremos *solubilidade por radicais*, de modo a mostrar quais tipo de equações polinomiais tem essa característica. E para tal, usaremos a Correspondência de Galois para transformar esse problema de encontrar soluções de uma equação, num problema de grupos.

Podemos dizer que $f(x) = 0$ é solúvel por radicais, se possuir uma raiz expressa por meio de radicais. Por exemplo: dada a equação $x^4 - 7x^2 + 10 = 0$, suas soluções serão $\{\sqrt{2},\ -\sqrt{2},\ \sqrt{5},\ -\sqrt{5}\}$.

5.1 Extensão Radical

Definição 5.1. Dizemos que $\mathbb{L} \mid \mathbb{K}$ é uma extensão radical se existirem corpos intermediários K_i, com $i = 1, 2, ..., t$, tais que,

$$\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 = \mathbb{K}_0[\alpha_1] \subset \mathbb{K}_2 = \mathbb{K}_1[\alpha_2] \subset \cdots \subset \mathbb{K}_{t-1} = \mathbb{K}_{t-2}[\alpha_{t-1}] \subset \mathbb{K}_t = \mathbb{K}_{t-1}[\alpha_t] = \mathbb{L},$$

onde para cada $i \in \{1, 2, \ldots, m\}$, existe $m_i \in \mathbb{Z}$ tal que $\alpha_i^{m_i} \in \mathbb{K}_{i-1}$.

Lema 5.2. *Seja $\mathbb{L} \mid \mathbb{K}$ uma extensão radical. Então $\exists \mathbb{M}$, com $\mathbb{L} \subset \mathbb{M}$, tal que $\mathbb{M} \mid \mathbb{K}$ é radical e galoisiana.*

Demonstração. Ver demonstração em [2]. □

Podemos agora, definir equação solúvel por radicais.

Definição 5.3. Seja $f(x)$ um polinômio sobre $\mathbb{K}$, subcorpo de $\mathbb{C}$, e seja $\mathbb{L} = \mathrm{Gal}(f, \mathbb{K})$ seu corpo de decomposição. Dizemos que $f(x) = 0$ é solúvel por radicais se existe um corpo $\mathbb{M}$, tal que $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$, com $\mathbb{M} \mid \mathbb{K}$ seja radical.

Notemos que $\mathbb{L} \mid \mathbb{K}$ não precisa ser uma extensão radical. Ilustremos com um exemplo.

Exemplo 5.4. Suponhamos que uma das soluções de $f(x) = 0$ seja:

$$x = \sqrt{2} + \sqrt[5]{8 + \sqrt[3]{5}}$$

Fazendo $\alpha = \sqrt{2},\ \beta = \sqrt[3]{5}$ e $\gamma = \sqrt[5]{8+\beta}$, uma extensão $\mathbb{L} \mid \mathbb{Q}$ que contenha x pode ser obtida da seguinte maneira:

$$\mathbb{Q} \subset \mathbb{Q}[\alpha] \subset \mathbb{Q}[\alpha;\beta] \subset \mathbb{Q}[\alpha;\beta;\gamma] = \mathbb{L}$$

E notemos que $\alpha^2 \in \mathbb{Q}$, $\beta^3 \in \mathbb{Q}[\alpha]$ e $\gamma^5 \in \mathbb{Q}[\alpha;\beta]$, portanto $\mathbb{L} \mid \mathbb{Q}$ é uma extensão radical.

Vejamos o principal teorema desse capítulo:

Teorema 5.5. *Seja $f(x) \in \mathbb{K}[x]$, um polinômio não-constante, com $\mathbb{K} \subset \mathbb{C}$, e seja $\mathbb{L} = \mathrm{Gal}(f, \mathbb{K})$. Então $f(x) = 0$ é solúvel por radicais se, e somente se, o grupo de Galois da extensão $\mathbb{L} \mid \mathbb{K}$, $\mathrm{Aut}_{\mathbb{K}} \mathbb{L}$, é um grupo solúvel.*

Demonstração. ($\Longrightarrow$) Suponhamos que $f(x) = 0$ seja solúvel por radicais, e $\mathbb{L} \mid \mathbb{K}$ seja seu corpo de decomposição. Da definição 5.3, $\exists \mathbb{M}$ com $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$, tal que $\mathbb{M} \mid \mathbb{K}$ é radical, e então:

$$\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 = \mathbb{K}_0[\alpha_1] \subset \cdots \subset \mathbb{K}_t = \mathbb{K}_{t-1}[\alpha_t] = \mathbb{M}$$

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

Tome $n = \mathrm{mmc}(m_1, m_2, \ldots, m_t)$, e seja $\zeta_n \in \mathbb{C}$ uma raiz n-ésima primitiva da unidade. Fazendo $\mathbb{M}' = \mathbb{M}[\zeta_n]$, onde $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M} \subset \mathbb{M}'$, temos que $\mathbb{M}' = \mathbb{K}[\alpha_1, \alpha_2 \ldots, \alpha_t, \zeta_n]$, que é equivalente a $\mathbb{M}' = \mathbb{K}[\zeta_n, \alpha_1, \alpha_2 \ldots, \alpha_t]$, e $\mathbb{M}'[\zeta_n] \mid \mathbb{K}$ é uma extensão radical, uma vez que $\zeta_n^n = 1 \in \mathbb{K}$, de acordo com a definição 5.1.

Temos então a seguinte cadeia:

$$\mathbb{M}_0 = \mathbb{K} \subset \mathbb{M}_1 = \mathbb{M}_0[\zeta_n] \subset \mathbb{M}_2 = \mathbb{M}_1[\alpha_1] \subset \cdots \subset \mathbb{M}_{t+1} = \mathbb{M}_t[\alpha_t] = \mathbb{M}'$$

Onde para cada $i \in \{1, 2, \ldots, t\}$, temos que $\alpha_i^{m_i} \in \mathbb{M}_{i-1}$.

Notemos que tanto $\mathbb{L} \mid \mathbb{K}$ quanto $\mathbb{M}' \mid \mathbb{K}$ são extensões galoisianas.

Seja $G_i = \mathrm{Aut}_{\mathbb{M}_i} \mathbb{M}'$, com $i \in \{0, 1, \ldots, t+1\}$, do item $iv.$ do Teorema 4.16 obtemos a seguinte subsérie normal:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_{t+1} = \{e\}$$

Ainda no item $iv.$, do Teorema 4.16, segue que,

$$\frac{G_{i-1}}{G_i} = \frac{\mathrm{Aut}_{\mathbb{M}_{i-1}} \mathbb{M}'}{\mathrm{Aut}_{\mathbb{M}_i} \mathbb{M}'} \simeq \mathrm{Aut}_{\mathbb{M}_{i-1}} \mathbb{M}_i$$

Analisando $\mathrm{Aut}_{\mathbb{M}_{i-1}}\mathbb{M}_i$, temos que, para $i=1$, $\mathrm{Aut}_{\mathbb{M}_0}\mathbb{M}_1 = \mathrm{Aut}_{\mathbb{K}}\mathbb{K}[\zeta_n]$, que de acordo com a Proposição 4.18, é abeliano.

Para $n \geq 2$, segue da Proposição 4.19, que $\mathrm{Aut}_{\mathbb{M}_{i-1}}\mathbb{M}_i$ cíclico, logo abeliano.

Portanto $G = \mathrm{Aut}_{\mathbb{K}}\mathbb{M}'$ é solúvel. Novamente do item $iv.$ do Teorema 4.16 temos que,

$$\mathrm{Aut}_{\mathbb{K}}\mathbb{L} \simeq \frac{\mathrm{Aut}_{\mathbb{K}}\mathbb{M}'}{\mathrm{Aut}_{\mathbb{L}}\mathbb{M}'}$$

E portanto, do item $ii.$ da proposição 1.47 segue que $\mathrm{Aut}_{\mathbb{K}}\mathbb{L}$ é solúvel.

($\Longleftarrow$) Agora suponha que $\mathrm{Aut}_{\mathbb{K}}\mathbb{L}$ seja um grupo solúvel. Denotemos $m = [\mathbb{L}:\mathbb{K}]$ e tomemos $n = \mathrm{mmc}(2,3,\ldots,m)$. Seja ζ_n uma raiz n-ésima primitiva da unidade então temos $\mathbb{L}[\zeta_n]$ é uma extensão finita de $\mathbb{L}$. Como o polinômio minimal de ζ_n sobre $\mathbb{K}$ é separável, então seu polinômio minimal sobre $\mathbb{L}$ também é separável, logo $\mathbb{L}[\zeta_n]:\mathbb{L}$ é uma extensão separável e é claro que $\mathbb{L}[\zeta_n]$ contém todas as raízes deste polinômio. Portanto $\mathbb{L}[\zeta_n]:\mathbb{L}$ é, também, normal, e portanto galoisiana. Agora, considere a aplicação:

$$\begin{array}{rccc} \psi: & \mathrm{Aut}_{\mathbb{K}[\zeta_n]}\mathbb{L}[\zeta_n] & \to & \mathrm{Aut}_{(\mathbb{K}[\zeta_n]\cap\mathbb{L})}\mathbb{L} \\ & \sigma & \mapsto & \sigma\mid_{\mathbb{L}} \end{array}$$

Como $\mathbb{L} \mid \mathbb{K}$ é galoisiana então $\mathbb{L} \mid (\mathbb{K}[\zeta_n]\cap\mathbb{L})$ também é galoisiana pois $\mathbb{K} \subset (\mathbb{K}[\zeta_n]\cap\mathbb{L}) \subset \mathbb{L}$ e $\mathbb{K}[\zeta_n]\cap\mathbb{L}$ é um corpo, então a aplicação ψ está bem definida e é um homomorfismo. Se $\psi(\sigma) = \mathrm{id}_{\mathbb{L}}$ então $\sigma \in \mathrm{Aut}_{\mathbb{L}}\mathbb{L}[\zeta_n]$ mas como $\sigma \in \mathrm{Aut}_{\mathbb{K}[\zeta_n]}\mathbb{L}[\zeta_n]$ então $\sigma(\zeta_n) = \zeta_n$ logo $\sigma = \mathrm{id}_{\mathbb{L}[\zeta_n]}$, portanto ψ é injetiva. Na verdade, ψ é sobrejetiva. De fato, seja $G' = \psi(\mathrm{Aut}_{\mathbb{K}[\zeta_n]}\mathbb{L}[\zeta_n])$ e $\mathbb{K}'$ o corpo associado à G' pela Correspondência de Galois. Note que, pela definição de $\mathbb{K}'$ temos que $(\mathbb{K}[\zeta_n]\cap\mathbb{L}) \subset \mathbb{K}'$. Para todo $\sigma \in G'$ e todo $\alpha \in \mathbb{K}'$ temos $\sigma(\alpha) = \alpha$. Então, para todo $\eta \in \mathrm{Aut}_{\mathbb{K}[\zeta_n]}\mathbb{L}[\zeta_n]$ temos $\eta(\alpha) = \eta\mid_{\mathbb{L}}(\alpha) = \alpha$. Então $\alpha \in (\mathbb{K}[\zeta_n]\cap\mathbb{L})$. Portanto $\mathbb{K}' \subset (\mathbb{K}[\zeta_n]\cap\mathbb{L})$. Isso mostra que $\mathrm{Aut}_{\mathbb{K}[\zeta_n]}\mathbb{L}[\zeta_n]$ é isomorfo a $\mathrm{Aut}_{(\mathbb{K}[\zeta_n]\cap\mathbb{L})}\mathbb{L}$ que é subgrupo de $\mathrm{Aut}_{\mathbb{K}}\mathbb{L}$. Denotemos $G = \mathrm{Aut}_{\mathbb{K}[\zeta_n]}\mathbb{L}[\zeta_n]$. Como $\mathrm{Aut}_{\mathbb{K}}\mathbb{L}$ é solúvel então G é solúvel, então garantimos a existência da subsérie normal:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_t = \{e\} \tag{5.1}$$

onde $\dfrac{G_{i-1}}{G_i}$ é abeliano para todo $i \in \{1,\ldots,t\}$.

Como G é finito, a Proposição 1.26 permite que consideremos $\dfrac{G_{i-1}}{G_i}$ cíclico, para todo $i \in \{1,\ldots,t\}$. Basta que façamos um refinamento apropriado da subsérie normal (5.1), se necessário.

De acordo com o Teorema 4.16, podemos associar a cada subgrupo dessa série um corpo intermediário da extensão $\mathbb{L}[\zeta_n] \mid \mathbb{K}[\zeta_n]$:

$$\mathbb{K}[\zeta_n] = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \cdots \subset \mathbb{L}_t = \mathbb{L}[\zeta_n]$$

De modo que $G_i = \mathrm{Aut}_{\mathbb{L}_i}\mathbb{L}[\zeta_n]$, para todo $i \in \{0,1,\ldots,t\}$.

Visto que:

$$\frac{G_{i-1}}{G_i} = \frac{\mathrm{Aut}_{\mathbb{L}_{i-1}} \mathbb{L}[\zeta_n]}{\mathrm{Aut}_{\mathbb{L}_i} \mathbb{L}[\zeta_n]} \simeq \mathrm{Aut}_{\mathbb{L}_{i-1}} \mathbb{L}_i$$

Concluímos que $\mathrm{Aut}_{\mathbb{L}_{i-1}} \mathbb{L}_i$ é cíclico para todo $i \in \{1, \ldots, t\}$.

Seja $m_i = [\mathbb{L}_i : \mathbb{L}_{i-1}]$. Temos que $m_i \mid ([\mathbb{L}[\zeta_n] : \mathbb{K}[\zeta_n]]) = |G'|$. Como $G' \subset \mathrm{Aut}_{\mathbb{K}} \mathbb{L}$ então $m_i \mid (|\mathrm{Aut}_{\mathbb{K}} \mathbb{L}|) = [\mathbb{L} : \mathbb{K}]$, então $m_i \mid n$. Portanto $(\zeta_n)^{\frac{n}{m_i}}$ é uma raiz primitiva m_i-ésima da unidade e pertence a $\mathbb{L}_i$. Então pelo Teorema 4.20, existem $\alpha_i \in \mathbb{L}_i$ tais que $\mathbb{L}_i = \mathbb{L}_{i-1}[\alpha_i]$ e $\alpha_i^{m_i} \in \mathbb{L}_{i-1}$, para todo $i \in \{1, \ldots, t\}$, e tem-se:

$$\mathbb{K} \subset \mathbb{K}[\zeta_n] = \mathbb{L}_0 \subset \mathbb{L}_0[\alpha_1] = \mathbb{L}_1 \subset \mathbb{L}_1[\alpha_2] = \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_{t-1}[\alpha_t] = \mathbb{L}_t = \mathbb{L}[\zeta_n]$$

Portanto, $\mathbb{L}[\zeta_n] \mid \mathbb{K}$ é uma extensão radical e $\mathbb{L} \subset \mathbb{L}[\zeta_n]$, e de acordo com a Definição 5.3, temos que $f(x) = 0$ é solúvel por radicais, concluindo assim nossa demonstração. □

Diante deste teorema e da proposição 4.14, podemos fazer a seguinte generalização:

Seja $f(x)$ um polinômio não constante em $\mathbb{K}[x]$, cujo $\partial f(x) = m$, $m = 2, 3, 4$. Seja ainda $\mathbb{L} \mid \mathbb{K}$ o corpo de decomposição de $f(x)$, sabemos que $\mathrm{Aut}_{\mathbb{K}} \mathbb{L}$ é isomorfo à S_m, e para os valores de m aqui citados, temos que $f(x)$ é solúvel por radicais (como mostrado na seção 1.8). Vale ressaltar que para um S_n, com $n \geq 5$, apesar de este ser insolúvel, nada impede que ele possua subgrupos solúveis. Veremos na próxima seção como essa informação levaram matemáticos a criarem fórmulas de resoluções de equações polinomiais de graus m com $m = 2, 3, 4$.

De modo a exemplificar o teorema acima, observemos a seguinte equação polinomial: $x^n - a = 0$. Facilmente podemos notar e afirmar que trata-se de uma equação solúvel por radicais, uma vez que diante do que já vimos em capítulos anteriores, suas n soluções serão: $\{\sqrt[n]{a}, \sqrt[n]{a}\zeta_n, \sqrt[n]{a}\zeta_n^2, ..., \sqrt[n]{a}\zeta_n^{n-1}\}$, com $\zeta_n = \cos\frac{2k\pi}{n} + i\,\mathrm{sen}\,\frac{2k\pi}{n}, k = 1, 2, ..., n$.

Na proposição 5.12, da seção 5.3 o leitor pode verificar um exemplo de uma equação cujo grupo grupo de automorfismos do corpo de decomposição, ou seja, o grupo de Galois é um grupo solúvel.

5.2 Equações de grau ≤ 4

Nesta seção discorreremos sobre o processo de construção das fórmulas de resolução de equações de grau ≤ 4, inclusive salientando que tais fórmulas só foram possíveis de serem descritas justamente pelo fato de tais equações serem solúveis por meio de radicais.

O leitor interessado pode encontrar em [14] detalhes da história por trás de todo o desenvolvimento dessas fórmulas.

5.2.1 Solubilidade de equações de grau ≤ 4

A resolução de equações polinomiais é um problema muito antigo na história da matemática. Por volta de 1800 a.C., os babilônicos já utilizavam métodos de resolução

de equações quadráticas, enquanto os egípcios só conheciam métodos para resolução de equações lineares. Os gregos usavam a geometria pra resolver equações quadráticas e algumas cúbicas. Os árabes são responsáveis pelo método de resolução das equações quadráticas. Já as resoluções das equações cúbicas e quárticas são devidas principalmente aos matemáticos Tartaglia, Cardano e Ferrari.

Durante todo nosso trabalho, tratamos naturalmente das equações polinomiais, porém, não as definimos formalmente, façamos agora.

Definição 5.6. Chamamos de Equação Polinomial em uma única variável, toda equação do tipo $p(x) = 0$, onde $p(x)$ é um polinômio. E seu conjunto solução é formado pelas raízes de $p(x)$.

No capítulo anterior, definimos o que são equações solúveis por meio de radicais, usando a correspondência de Galois e transformando esse problema num problema de grupos.

Diante disso, e do estudo que fizemos sobre grupos no capítulo 1, vale ressaltar:

Proposição 5.7. *Seja $f(x) \in \mathbb{K}[x]$, um polinômio não constante, com $\mathbb{K} \subset \mathbb{C}$, e $\partial f(x) \leq 4$, então $f(x)$ é solúvel por radicais.*

Demonstração. Vimos no Teorema 5.5 que uma equação polinomial será solúvel por radicais, se seu grupo de Galois for solúvel. Vimos também na Proposição 4.14 que o grupo de Galois de uma extensão galoisiana é isomorfo à um subgrupo de S_n, que, de acordo com o item (i) da Proposição 1.49 e (i) da Proposição 1.47 , será sempre solúvel para $n \leq 4$ e seus subgrupos são também solúveis. Assim, como toda equação de grau n é tem seu grupo de Galois isomorfo à subgrupo de S_n, então para $n \leq 4$ teremos sempre que o grupo de Galois será sempre solúvel para $n \leq 4$ e portanto toda equação de grau ≤ 4 será solúvel por radicais. □

Como resultado desta proposição, podemos afirmar que é sempre possível achar as soluções destas equações, e a forma como fazemos é justamento manipulando os coeficientes da equação polinomial.

Obviamente a solução de uma equação polinomial de grau 1 ou equação linear é trivial. Seja $a, b \in \mathbb{C}$, com $a \neq 0$, uma equação linear é toda equação do tipo $ax + b = 0$ e sua solução é dada por $x = \dfrac{-b}{a}$. Claramente vemos que é uma solução obtida por meio de radicais.

Para as equações de graus $2, 3$ e 4, daremos uma atenção maior, mostrando inicialmente as deduções de suas tradicionais fórmulas, e mostrando, implicitamente, que suas soluções pertencem a extensão radical.

5.2.2 Equação Quadrática

Seja $a, b, c \in \mathbb{C}$, com $a \neq 0$, uma equação quadrática ou de grau 2 é toda equação do tipo $ax^2 + bx + c = 0$ e sua solução é obtida da seguinte maneira:

i. Inicialmente, podemos dividir toda a equação por a, de modo à torná-la mônica:

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

ii. Agora subtraindo de ambos os lados $\frac{c}{a}$ e somando $\frac{b^2}{4a^2}$ na intenção de completar um trinômio quadrado perfeito:

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

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

Podemos reescrever:

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

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

iii. Fazendo $\Delta = b^2 - 4ac$:

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

iv. Seja δ tal que $\delta^2 = \Delta$:

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

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

$$x + \frac{b}{2a} = \pm\frac{\delta}{2a}$$

$$x = -\frac{b}{2a} \pm \frac{\delta}{2a}$$

Quando Δ é um número real não-negativo, então $\delta = \sqrt{\Delta}$, já se Δ é um número real negativo, então $\delta = i\sqrt{-\Delta}$. Quando Δ não e um número real, podemos determinar δ análogo ao que vimos na seção 3.5.

Por se tratar de um tipo de equação, velha conhecida nossa, não mostraremos aqui um exemplo.

5.2.3 Equação Cúbica

Seja $a, b, c, d \in \mathbb{C}$, com $a \neq 0$, uma equação cúbica ou de grau 3 é toda equação do tipo $ax^3 + bx^2 + cx + d = 0$ e sua solução é obtida da seguinte maneira:

i. Inicialmente, podemos dividir toda equação por a, de modo à torná-la mônica:

$$x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a} = 0$$

ii. Fazendo $B = \frac{b}{a}$, $C = \frac{c}{a}$ e $D = \frac{d}{a}$:

$$x^3 + Bx^2 + Cx + D = 0$$

iii. Agora, façamos a seguinte mudança de variável, $x = y - \frac{B}{3}$:

$$\left(y - \frac{B}{3}\right)^3 + B\left(y - \frac{B}{3}\right)^2 + C\left(y - \frac{B}{3}\right) + D = 0$$

$$y^3 - By^2 + \frac{B^2y}{3} - \frac{B^3}{27} + By^2 - \frac{2B^2y}{3} + \frac{B^3}{9} + Cy - \frac{BC}{3} + D = 0$$

$$y^3 + \left(C - \frac{B^2}{3}\right)y + \frac{2B^3}{27} - \frac{BC}{3} + D = 0$$

iv. Fazendo $C - \frac{B^2}{3} = p$ e $\frac{2B^3}{27} - \frac{BC}{3} + D = q$:

$$y^3 + py + q = 0$$

Todo esse procedimento foi para transformar essa equação cúbica completa, numa que não possua o temos y^2. Vejamos agora como resolvê-la, com $p, q \neq 0$:

i. Escrevendo a solução y como $y = \alpha + \beta$:

$$\begin{aligned} y^3 &= (\alpha+\beta)^3 \\ &= \alpha^3+3\alpha^2\beta+3\alpha\beta^2+\beta^3 \\ &= 3\alpha\beta\underbrace{(\alpha+\beta)}_{y}+\alpha^3+\beta^3 \\ &= \underbrace{3\alpha\beta}_{-p}y+\underbrace{\alpha^3+\beta^3}_{-q} \end{aligned}$$

Temos então que:

$$\begin{cases} 3\alpha\beta = -p \\ \alpha^3+\beta^3 = -q \end{cases}$$

Notemos que $3\alpha\beta = -p$:

$$3\alpha\beta = -p \Longrightarrow$$

$$\alpha\beta = \frac{-p}{3} \Longrightarrow$$

$$(\alpha\beta)^3 = \left(-\frac{p}{3}\right)^3 \Longrightarrow$$

$$\alpha^3\beta^3 = -\left(\frac{p}{3}\right)^3$$

E então:

$$\begin{cases} \alpha^3+\beta^3 = -q \\ \alpha^3\beta^3 = -\left(\frac{p}{3}\right)^3 \end{cases}$$

Notemos que se trata de uma soma e produto de α^3 e β^3, que caracteriza as soluções da equação do segundo grau:

$$z^2+qz-\left(\frac{p}{3}\right)^3 = 0$$

$$z^2+qz = \left(\frac{p}{3}\right)^3$$

Vamos então resolvê-la, de acordo com o que vimos na seção anterior, adicionando em ambos os lados $\left(\frac{q}{2}\right)^2$:

$$z^2 + \left(\frac{q}{2}\right)^2 + qz = \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2$$

Denotamos $\Delta = \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2$. Δ é chamado de discriminante da equação do 3º grau, então:

$$\left(z + \frac{q}{2}\right)^2 = \Delta$$

Seja $\delta \in \mathbb{C}$ tal que $\delta^2 = \Delta$:

$$\left(z + \frac{q}{2}\right)^2 = \delta^2$$

$$z + \frac{q}{2} = \pm\delta$$

Assim teremos que,

$$\alpha^3 = -\frac{q}{2} + \delta \text{ e } \beta^3 = -\frac{q}{2} - \delta$$

Notemos que se $\Delta = 0$, teremos $\alpha^3 = \beta^3$.

Seja $\alpha \in \mathbb{C}$, tal que $\alpha^3 = -\frac{q}{2} + \delta$, de acordo com o que vimos na seção 3.5, existem três números que elevados ao cubo resultam em $-\frac{q}{2} + \delta$. Denotaremos ainda por α uma dessas soluções, então as soluções serão:

$$\begin{cases} \alpha_1 &= \alpha \\ \alpha_2 &= \alpha\zeta_3 \\ \alpha_3 &= \alpha\zeta_3^2 \end{cases},$$

onde $\zeta_3 = \dfrac{-1 + i\sqrt{3}}{2}$ e $\zeta_3^2 = \dfrac{-1 - i\sqrt{3}}{2}$ são duas raízes cúbicas da unidade. Vale ressaltar que $\dfrac{1}{\zeta_3} = \zeta_3^2$ bem como $\dfrac{1}{\zeta_3^2} = \zeta_3$.

Determinemos agora β_1, β_2 e β_3, que são as soluções de $\beta^3 = -\frac{q}{2} - \delta$, lembrando que $3\alpha\beta = -p$, tem-se:

$$\beta = \frac{-p}{3\alpha}.$$

Por conveniência, denotaremos β_1 apenas por β. Portanto,

$$\begin{cases} \beta_1 &= \dfrac{-p}{3\alpha_1} = \dfrac{-p}{3\alpha} = \beta \\ \beta_2 &= \dfrac{-p}{3\alpha_2} = \dfrac{-p}{3\alpha\zeta_3} = \dfrac{-p}{3\alpha}\zeta_3^2 = \beta\zeta_3^2 \\ \beta_3 &= \dfrac{-p}{3\alpha_3} = \dfrac{-p}{3\alpha\zeta_3^2} = \dfrac{-p}{3\alpha}\zeta_3 = \beta\zeta_3 \end{cases}$$

Então, como tínhamos $y = \alpha + \beta$, as soluções de $y^3 + py + q = 0$ serão:

$$\begin{cases} y_1 &= \alpha_1 + \beta_1 \\ y_2 &= \alpha_2 + \beta_2 \\ y_3 &= \alpha_3 + \beta_3 \end{cases}$$

$$\begin{cases} y_1 &= \alpha + \beta \\ y_2 &= \alpha\zeta_3 + \beta\zeta_3^2 \\ y_3 &= \alpha\zeta_3^2 + \beta\zeta_3 \end{cases}$$

Notemos que se $p, q \in \mathbb{R}$ então $\Delta \in \mathbb{R}$. Se $\Delta \geq 0$, então podemos tomar $\delta = \sqrt{\Delta}$ e então podemos tomar:

$$\alpha = \sqrt[3]{-\frac{q}{2} + \sqrt{\Delta}} \text{ e } \beta = \sqrt[3]{-\frac{q}{2} - \sqrt{\Delta}}$$

Pois,

$$\begin{aligned} \alpha\beta &= \sqrt[3]{\left(-\frac{q}{2} + \sqrt{\Delta}\right)\left(-\frac{q}{2} - \sqrt{\Delta}\right)} \\ &= \sqrt[3]{\left(-\frac{q}{2}\right)^2 - \left(\sqrt{\Delta}\right)^2} \\ &= \sqrt[3]{\left(\frac{q}{2}\right)^2 - \Delta} \\ &= \sqrt[3]{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3 - \left(\frac{q}{2}\right)} \\ &= \sqrt[3]{-\left(\frac{p}{3}\right)^3} \\ &= -\frac{p}{3} \end{aligned}$$

E então a solução será:

$$\begin{cases} y_1 &= \left(\sqrt[3]{-\dfrac{q}{2} + \sqrt{\Delta}}\right) + \left(\sqrt[3]{-\dfrac{q}{2} - \sqrt{\Delta}}\right) \\ y_2 &= \left(\sqrt[3]{-\dfrac{q}{2} + \sqrt{\Delta}}\right)\zeta_3 + \left(\sqrt[3]{-\dfrac{q}{2} - \sqrt{\Delta}}\right)\zeta_3^2 \\ y_3 &= \left(\sqrt[3]{-\dfrac{q}{2} + \sqrt{\Delta}}\right)\zeta_3^2 + \left(\sqrt[3]{-\dfrac{q}{2} - \sqrt{\Delta}}\right)\zeta_3 \end{cases}$$

ii. No caso analisado acima, temos que se $\Delta \geq 0$, $\alpha, \beta \in \mathbb{R}$, consequentemente $\alpha+\beta \in \mathbb{R}$ e:

$$\begin{aligned} \overline{y_2} &= \overline{\alpha\zeta_3 + \beta\zeta_3^2} \\ &= \alpha\overline{\zeta_3} + \beta\overline{\zeta_3^2} \\ &= \alpha\zeta_3^2 + \beta\zeta_3 \\ &= y_3 \end{aligned}$$

Daí, se $\Delta > 0$, teremos então uma raiz real e duas complexas conjugadas, note que y_2 e y_3 são conjugadas.

Já se $\Delta = 0$, tem-se $\alpha = \beta$ e lembrando que a soma de um número complexo com seu conjugado é o dobro de sua parte real, teremos:

$$\begin{cases} y_1 &= 2\alpha \\ y_2 &= \alpha(\zeta_3 + \zeta_3^2) = \alpha \cdot (-1) = -\alpha \\ y_3 &= \alpha(\zeta_3^2 + \zeta_3) = -\alpha \end{cases}$$

Logo, temos três raízes reais, sendo que uma delas é dupla, a saber $y_2 = y_3$, ou teremos uma raiz tripla, no caso em que $q = 0$, pois teríamos $\alpha = 0$, e portanto $y = 0$ é uma raiz tripla.

Por fim, se $\Delta < 0$, teremos:

$$\alpha^3 = -\frac{q}{2} + i\sqrt{-\Delta} \text{ e } \beta^3 = -\frac{q}{2} - i\sqrt{-\Delta}$$

Note que aqui podemos usar a raiz quadrada, pois $-\Delta > 0$. Note ainda que $\beta^3 = \overline{\alpha^3}$. Seja α uma das raízes de $\alpha^3 = -\frac{q}{2} + i\sqrt{-\Delta}$, podemos tomar $\beta = \overline{\alpha}$, pois:

$$\begin{aligned} (\alpha\beta)^3 &= \alpha^3\beta^3 = \left(\alpha^3 = -\frac{q}{2} + i\sqrt{-\Delta}\right)\left(\beta^3 = -\frac{q}{2} - i\sqrt{-\Delta}\right) \\ &= \left(\frac{q}{2}\right)^2 - \Delta \\ &= \left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3 - \left(\frac{q}{2}\right)^2 \\ &= -\left(\frac{p}{3}\right)^3 \end{aligned}$$

E como $\alpha\beta = \alpha\overline{\alpha} = |\alpha|^2 \in \mathbb{R}$, segue que $\alpha\beta = -\frac{p}{3}$. E então:

$$\begin{cases} y_1 &= \alpha + \overline{\alpha} = 2 \cdot \mathrm{Re}(\alpha) \\ y_2 &= \alpha\zeta_3 + \overline{\alpha}\zeta_3^2 = 2 \cdot \mathrm{Re}(\alpha\zeta_3) \\ y_3 &= \alpha\zeta_3^2 + \overline{\alpha}\zeta_3 = 2 \cdot \mathrm{Re}(\alpha\zeta_3^2) \end{cases}$$

Note que $\overline{\alpha}\zeta_3^2 = \overline{\alpha\zeta_3}$ e $\overline{\alpha}\zeta_3 = \overline{\alpha\zeta_3^2}$.

Portanto, se $\Delta < 0$, teremos três raízes reais.

iii. Voltando à variável x, tínhamos $x = y - \dfrac{B}{3}$, e então:

$$\begin{cases} x_1 &= y_1 - \dfrac{B}{3} = \alpha + \beta - \dfrac{B}{3} \\ x_2 &= y_2 - \dfrac{B}{3} = \alpha\zeta_3 + \beta\zeta_3^2 - \dfrac{B}{3} \\ x_3 &= y_3 - \dfrac{B}{3} = \alpha\zeta_3^2 + \beta\zeta_3 - \dfrac{B}{3} \end{cases}$$

Por fim, como $B = \dfrac{b}{a} \Longrightarrow \dfrac{A}{3} = \dfrac{b}{3a}$, as soluções de $ax^3 + bx^2 + cx + d = 0$ serão:

$$\begin{cases} x_1 &= \alpha + \beta - \dfrac{b}{3a} \\ x_2 &= \alpha\zeta_3 + \beta\zeta_3^2 - \dfrac{b}{3a} \\ x_3 &= \alpha\zeta_3^2 + \beta\zeta_3 - \dfrac{b}{3a} \end{cases}$$

Com,

$$p = C - \frac{B^2}{3} \Longrightarrow p = \frac{c}{a} - \frac{b^2}{3a^2},$$

$$q = \frac{2B^3}{27} + \frac{BC}{3} + C \Longrightarrow q = \frac{2b^3}{27a^3} + \frac{bc}{3a^2} + \frac{d}{a},$$

$$\zeta_3 = \frac{-1 + i\sqrt{3}}{2}$$

e

$$\zeta_3^2 = \frac{-1 - i\sqrt{3}}{2}$$

Vejamos um exemplo da resolução de uma equação cúbica. No entanto veremos aqui um exemplo que já está na forma $y^3 + py + q = 0$, de modo a abreviar nossos cálculos.

Exemplo 5.8. Determinemos as soluções de $x^3 - 6x - 9 = 0$.

Como dissemos, a equação cúbica já está na forma $y^3 + py + q = 0$. Por isso, podemos iniciar a resolução, encontrando o valor de Δ:

$$\Delta = \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2$$

$$\Delta = \left(\frac{-6}{3}\right)^3 + \left(\frac{-9}{2}\right)^2$$

$$\Delta = \frac{49}{4}$$

Agora, determinando os valores de α e β, como $\Delta \geq 0$, segue que $\sqrt{\Delta} = \frac{7}{2}$:

$$\alpha = \sqrt[3]{\frac{9}{2} + \frac{7}{2}} \text{ e } \beta = \sqrt[3]{\frac{9}{2} - \frac{7}{2}}$$

$$\alpha = \sqrt[3]{8} \text{ e } \beta = \sqrt[3]{1}$$

$$\alpha = 2 \text{ e } \beta = 1$$

Logo:

$$\begin{cases} \alpha_1 &= 2 \\ \alpha_2 &= 2\zeta_3 \\ \alpha_3 &= 2\zeta_3^2 \end{cases}$$

e

$$\begin{cases} \beta_1 &= 1 \\ \beta_2 &= \zeta_3 \\ \beta_3 &= \zeta_3^2 \end{cases}$$

Assim, as soluções serão:

$$\begin{cases} x_1 &= 2+1 \\ x_2 &= 2\zeta_3 + 1\zeta_3^2 \\ x_3 &= 2\zeta_3^2 + 1\zeta_3 \end{cases}$$

$$\begin{cases} x_1 &= 3 \\ x_2 &= -1 + i\sqrt{3} + \dfrac{-1 - i\sqrt{3}}{2} \\ x_3 &= -1 - i\sqrt{3} + \dfrac{-1 + i\sqrt{3}}{2} \end{cases}$$

$$\begin{cases} x_1 &= 3 \\ x_2 &= \dfrac{-3 + i\sqrt{3}}{2} \\ x_3 &= \dfrac{-3 - i\sqrt{3}}{2} \end{cases}$$

5.2.4 Equação Quártica

Seja $a, b, c, d, e \in \mathbb{C}$, com $a \neq 0$, uma equação quártica ou de grau 4 é toda equação do tipo $ax^4 + bx^3 + cx^2 + dx + e = 0$ e sua solução é obtida da seguinte maneira:

i. Inicialmente, podemos dividir toda equação por a, de modo à torná-la mônica:

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

Fazendo $B = \frac{b}{a}$, $C = \frac{c}{a}$, $D = \frac{d}{a}$ e $E = \frac{e}{a}$:

$$x^4 + Bx^3 + Cx^2 + Dx + E = 0$$

ii. Agora, fazendo a mudança de variável $x = y - \frac{B}{4}$, e procedendo com os cálculos, que aqui omitiremos, teremos:

$$y^4 + \left(C - \frac{3}{8}B^2\right)y^2 + \left(\frac{1}{8}B^3 - \frac{1}{2}BC + D\right)y + \left(-\frac{3}{256}B^4 + \frac{1}{16}B^2C - \frac{1}{4}BD + E\right) = 0$$

$$y^4 + py^2 + qy + r = 0$$

Onde

$$\begin{cases} p &= C - \frac{3}{8}B^2 \\ q &= \frac{1}{8}B^3 - \frac{1}{2}BC + D \\ r &= -\frac{3}{256}B^4 + \frac{1}{16}B^2C - \frac{1}{4}BD + E \end{cases}$$

iii. Reescrevendo $y^4 + py^2 + qy + r = 0$:

$$y^4 + py^2 + r = -qy$$

E adicionando $(m-p)\,y^2 + n$ em ambos os lados, e organizando:

$$\underbrace{y^4 + my^2 + (r+n)}_{(i)} = \underbrace{(m-p)\,y^2 - qy + n}_{(ii)}$$

Precisamos descobrir quais valores de m e n para que as expressões (i) e (ii) sejam trinômios quadrados perfeitos, para isso seus discriminantes devem ser nulos.

$$\begin{cases} m^2 - 4 \cdot 1 \cdot (r+n) = 0 \\ (-q)^2 - 4 \cdot (m-p) \cdot n = 0 \end{cases}$$

$$\begin{cases} m^2 - 4r - 4n = 0 \\ q^2 - 4n(m-p) = 0 \end{cases}$$

$$\begin{cases} m^2 = 4r + 4n \\ q^2 = 4n(m - p) \end{cases}$$

iv. Substituindo o valor de $4n$ da primeira equação na segunda:

$$(m^2 - 4r)(m - p) = q^2 \Longrightarrow$$

$$m^3 - pm^2 - 4rm + 4rp - q^2 = 0$$

Que é uma equação do terceiro grau na variável m. Sua resolução é feita como aprendemos na seção anterior. Agora escolhendo uma das três raízes, que, por simplicidade, denotaremos por m. De $m^2 = 4r+4n$, teremos $n = \dfrac{m^2 - r}{4}$, e substituindo em $y^4 + my^2 + (r + n) = (m - p)\, y^2 - qy + n$:

$$y^4 + my^2 + r + \frac{m^2 - 4r}{4} = (m - p)y^2 - qy + \frac{m^2 - 4r}{4}$$

$$y^4 + my^2 + \frac{m^2}{4} = (m - p)y^2 - qy + \frac{m^2 - 4r}{4}$$

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

Fazendo $\alpha = \dfrac{m}{2}$, $\beta = \sqrt{m - p}$ e $\gamma = -\dfrac{q}{2\beta}$:

$$(y^2 + \alpha)^2 = (\beta y + \gamma)^2$$

Cujas raízes são as raízes das seguintes equações quadráticas:

$$\begin{cases} y^2 + \alpha = \beta y + \gamma \\ y^2 + \alpha = -\beta y - \gamma \end{cases} \Longrightarrow$$

$$\begin{cases} y^2 - \beta y + \alpha - \gamma = 0 \\ y^2 + \beta y + \alpha + \gamma = 0 \end{cases}$$

v. Enfim, encontrar as soluções de uma equação do quarto grau consiste trabalhar com equações quadráticas e cúbicas.

Vejamos um exemplo da resolução de uma equação quártica. No entanto veremos aqui um exemplo que já está na forma $y^4+py^2+qy+r = 0$, de modo a abreviar nossos cálculos.

Exemplo 5.9. Determinemos as soluções de $x^4 - 15x^2 + 10x + 24 = 0$.

Como dissemos, a equação quártica já está na forma $y^4 + py^2 + qy + r = 0$. Daí temos que $p = -15$, $q = 10$ e $r = 24$. Agora faremos os procedimentos a partir do passo 3:

$$x^4 - 15x^2 + 10x + 24 = 0 \Longrightarrow x^4 - 15x^2 + 24 = -10x$$

Somando $(m - p)x^2 + n$:

$$x^4 + mx^2 + 24 + n = (m + 15)x^2 - 10x + n$$

Calculando o discriminante de cada trinômio de ambos os lados da equação e os igualando a zero teremos:

$$m^2 - 4n - 96 = 0 \Longrightarrow n = \frac{m^2 - 96}{4} \ (i)$$

e

$$100 - 4n(m + 15) = 0 \ (ii)$$

Substituindo (i) em (ii):

$$\begin{aligned} (m^2 - 96)(m + 15) &= 100 \\ m^3 + 15m^2 - 96m - 1540 &= 0 \end{aligned}$$

Para resolver tal equação cúbica, basta utilizar o que aprendemos na seção anterior, porém, omitiremos aqui os cálculos, e diremos apenas que uma de suas soluções é $m = 10$, que facilmente pode-se conferir. Com tal valor de m, temos que:

$$\alpha = \frac{m}{2} \Longrightarrow \alpha = 5,$$

$$\beta = \sqrt{m - p} \Longrightarrow \beta = 5$$

e

$$\gamma = \frac{-q}{2\beta} \Longrightarrow \gamma = -1$$

Assim:

$$(x^2 + \alpha)^2 = (x + \gamma)^2 \Longrightarrow$$

$$(x^2 + 5)^2 = (5x - 1)^2 \Longrightarrow$$

$$x^2 - 5x + 6 = 0 \ e \ x^2 + 5x + 4 = 0$$

Resolvendo ambas as equações, chegamos à conclusão de que as soluções de $x^4 - 15x^2 + 10x + 24 = 0$ serão: $x_1 = -4$, $x_2 = -1$, $x_3 = 2$ e $x_4 = 3$.

Vistas aqui as chamadas fórmulas de resolução das equações polinomiais de graus ≤ 4, nunca é demais salientar que tais fórmulas só foram possíveis de ser construídas ao longo do tempo, justamente pelo fato de que as suas soluções podem ser expressas por meio de radicais. E quanto às equações polinomiais de graus ≥ 5? Veremos na próxima seção.

5.3 Equações de Grau ≥ 5

Na seção anterior, vimos que não só é possível determinar fórmulas que generalizem as resoluções das equações de graus ≤ 4, como mostramos o desenvolvimento das mesmas. Agora mostraremos que não existe uma fórmula para resolução de equações de graus ≥ 5, e principalmente o motivo de não existir.

5.3.1 Por que não existem fórmulas?

A existência de uma fórmula só é possível se puder ser generalizada para toda e qualquer equação de determinado grau. Por exemplo, só existe fórmula pra equação cúbica, porque absolutamente toda equação polinomial de grau 3 tem sua solução expressa por radicais, pelo que garante a proposição 5.7.

Quando pensamos em equações de graus ≥ 5, nos perguntamos, "Suas soluções são expressas por meio de radicais?"A resposta mais coerente é que às vezes sim e às vezes não.

Sabemos que S_n é insolúvel para $n \geq 5$, mas nada impede que este tenha um subgrupo solúvel. Imaginemos então uma equação de grau 5, cujo grupo de Galois é isomorfo à um subgrupo solúvel de S_5, assim sua solução será sim expressão por meio de radicais. Porém, se o grupo de Galois for isomorfo ao próprio S_5, que é insolúvel, então essa equação não tem suas soluções expressas por meio de radicais.

Diante dessa falta de generalidade para equações de grau 5, podemos afirmar que nem toda equação de grau 5 é solúvel por meio de radicais, e portanto é impossível criar uma fórmula para resolvê-las. Obviamente podemos usar a mesma linha de raciocínio para equações de grau > 5.

A título de curiosidade, podemos citar a equação $x^5 - 5x^4 - 10x^3 - 10x^2 - 5x - 1 = 0$, que é um exemplo de uma equação que possui solução expressa por meio de radicais, uma de suas soluções é $x = 1 + \sqrt[5]{2} + \sqrt[5]{4} + \sqrt[5]{8} + \sqrt[5]{16}$. Porém como mencionado, nem sempre isso acontece.

5.3.2 Uma equação quíntica insolúvel

O simples fato de existir uma única equação de grau 5 que não possua solução expressa por meio de radicais, já garante sua não generalização e portanto sua impossibilidade de fórmulas para resolução, o mesmo vale para as demais de graus > 5.

Teoricamente já explicamos que para que uma equação de grau 5 seja insolúvel, basta que seu grupo de Galois seja insolúvel, inclusive exemplificamos o caso em que este é isomorfo ao S_5, portanto insolúvel. Veremos agora um exemplo prático de uma equação de grau 5 insolúvel por meio de radicais, justificando esse fato com base na teoria que desenvolvemos ao longo desse trabalho.

Vejamos agora um exemplo prático de uma equação de grau 5 insolúvel.

Proposição 5.10. *A equação $2x^5 - 10x + 5 = 0$ não é solúvel por meio de radicais.*

Demonstração. Sendo $f(x) = 2x^5 - 10x + 5$ o polinômio da equação em questão, chamemos de $\mathbb{L} = \text{Gal}(f, \mathbb{Q})$, o corpo de decomposição de $f(x)$ e de G seu grupo de Galois.

Pelo critério de Eisenstein, temos que $f(x)$ é irredutível, pois, para o primo, $p = 5$, tem-se que $p \nmid a_5 = 2$, $p \mid a_4 = 0, a_3 = 0, a_2 = 0, a_1 = -10, a_0 = 5$ e $p^2 = 25 \nmid a_0 = 5$. E seja α uma das raízes de $f(x)$, temos pela Lei da Torre, vista na proposição 3.11 que: $[\mathbb{L} : \mathbb{Q}] = [L : \mathbb{Q}[\alpha]][\mathbb{Q}[\alpha] : \mathbb{Q}]$, onde $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 5$, logo $[\mathbb{L} : \mathbb{Q}]$ é múltiplo de 5. E como pela correspondência de Galois $[\mathbb{L} : \mathbb{Q}] = |G|$, então $|G|$ é múltiplo da 5, ou em outras palavras 5 divide $|G|$.

Do teorema 1.17, o Teorema de Cauchy, temos que o grupo G possui um elemento de ordem 5. E como se sabe, no grupo S_5, o único elemento de ordem 5 de S_5 é o 5-ciclo, logo, sabemos que G possui um elemento 5-ciclo.

Fazendo uma breve análise das raízes de $f(x)$, já sabemos que $f(x)$ é irredutível e temos ainda que sua primeira derivada é $f'(x) = 10x^4 - 10$. Facilmente observamos que $f(x)$ e $f'(x)$ são coprimos, logo $f(x)$ é separável e então só possui raízes simples.

Fazendo $f'(x) = 10(x-1)(x+1)(x^2+1)$ observamos que $f'(x) > 0$ sempre que $x < -1$ ou $x > 1$, e $f'(x) < 0$ sempre que $-1 < x < 1$. Ou seja, $f(x)$ é crescente em $(-\infty, -1]$ e $[1, +\infty)$, e decrescente em $[-1, 1]$.

Agora, fazendo $f(-2) = -39$, $f(-1) = 13$, $f(1) = -4$ e $f(2) = 49$, constatamos a existência de uma raiz entre -2 e -1, outra entre -1 e 1 e uma terceira entre 1 e 2. Como $f(x)$ é separável, sabemos que as outras duas raízes só podem ser complexas, e são complexo-conjugadas.

Diante dessa informação, podemos imaginar que existe um automorfismo, $\gamma \in G$ que fixa as três raízes reais de $f(x)$ e permuta as outras duas complexas, a saber, a conjugação complexa restrita a $\mathbb{L}$. Esse automorfismo corresponde a uma transposição (um 2-ciclo) de S_5.

Como G possui um elemento 5-ciclo e uma transposição, ou seja, possui os elementos (12) e (12345), da proposição 1.39, temos que o G é o próprio S_5, que como sabemos da seção 1.8, é insolúvel, portanto G é insolúvel e do teorema 5.5, podemos concluir que $2x^5 - 10x + 5 = 0$ não é solúvel por meio de radicais.

□

Numa forma de generalizar, tem-se a seguinte proposição:

Proposição 5.11. *Seja $f(x) \in \mathbb{Q}[x]$, um polinômio não constante, cujo $\partial f(x) = 5$ e com exatamente três raízes reais, então seu grupo de Galois é isomorfo ao S_5 e $f(x)$ é insolúvel por meio de radicais.*

Demonstração. A demonstração é análoga à da proposição anterior. Note que já se tem a garantia de três raízes reais e duas complexas, e então, a identificação de um $5-ciclo$ e uma transposição é feita de modo similar à proposição anterior, tornando trivial sua conclusão. □

5.3.3 Um exemplo contraditório

Já falamos aqui mesmo neste capítulo, que não podemos afirmar que não existe equações de grau ≥ 5 solúvel por meio de radicais. O que ocorre é que não existindo uma única, já garantimos que não podemos chegar numa fórmula resolutiva. Mostramos inclusive, uma equação de grau 5 e uma de suas soluções expressas por meio de radicais.

No intuito de mostrar uma equação solúvel por meio de radicais de grau ≥ 5, mostrando que seu grupo de Galois é de fato solúvel, apresentaremos um exemplo com análise completa.

Proposição 5.12. *A equação $x^{30} - 2 = 0$ é solúvel por meio de radicais, pois seu grupo de Galois é solúvel.*

Demonstração. De acordo com o que já estudamos até aqui, além de podermos afirmar que essa equação é solúvel por meio de radicais, podemos exibir suas soluções, a saber, $\{\sqrt[30]{2};\ \sqrt[30]{2}\zeta_{30};\ \sqrt[30]{2}\zeta_{30}^2;\ \sqrt[30]{2}\zeta_{30}^3;\ldots;\ \sqrt[30]{2}\zeta_{30}^{29}\}$. Mostremos então que de fato seu grupo de Galois é solúvel.

Seja $p(x) = x^{30} - 2$, chamemos de $\mathbb{L} = \mathrm{Gal}(x^{30} - 2, \mathbb{Q})$ seu corpo de decomposição e de G seu grupo de automorfismos. Note que $[\mathbb{Q}[\sqrt[30]{2}] : \mathbb{Q}] = 30$, pois a base de $\mathbb{Q}[\sqrt[30]{2}]$ é $\{1, \sqrt[30]{2}, \sqrt[30]{2^2}, \sqrt[30]{2^3}, \ldots, \sqrt[30]{2^{29}}\}$, e $[\mathbb{Q}[\sqrt[30]{2}, \zeta_{30}] : \mathbb{Q}[\sqrt[30]{2}]] = \phi(30) = 8$, de acordo com o teorema 3.24. Temos então que $\mathbb{L} = \mathrm{Gal}(x^{30} - 2, \mathbb{Q}) = \mathbb{Q}[\sqrt[30]{2}, \zeta_{30}]$ e

$$\begin{aligned}
[\mathbb{L} : \mathbb{Q}] &= [\mathbb{Q}[\sqrt[30]{2}, \zeta_{30}] : \mathbb{Q}] \\
&= [\mathbb{Q}[\sqrt[30]{2}, \zeta_{30}] : \mathbb{Q}[\sqrt[30]{2}]] \cdot [\mathbb{Q}[\sqrt[30]{2}] : \mathbb{Q}] \\
&= 8 \cdot 30 \\
&= 240
\end{aligned}$$

Da correspondência de Galois, temos que $[\mathbb{L} : \mathbb{Q}] = |G| = 240$, portanto temos um total de 240 automorfismos. Vale lembrar que $G \leq S_{30}$.

Agora nos resta montar uma subsérie normal, que garanta a solubilidade de G.

Seja $x \in \mathbb{L}$, temos que:

$$x = a_1 \cdot 1, a_2 \cdot \sqrt[30]{2} + a_{30} \cdot \sqrt[30]{2^{29}} + a_{31} \cdot \zeta_{30} + a_{32} \cdot \sqrt[30]{2}\zeta_{30}^2 + \cdots + a_{240} \cdot \sqrt[30]{2^{29}}\zeta_{30}^{29}$$

Similar ao no Exemplo 4.15, os automorfismos de $\mathbb{L}$ que preservam $\mathbb{Q}$ são tais que, em resumo, modificam $\sqrt[30]{2}$ e/ou ζ_{30}, podendo preservar ambos, o caso do automorfismo identidade.

Denotaremos por α_i, $i \in \{0, 1, 2, \ldots, 29\}$, os automorfismos que preservam ζ_{30} e levam $\sqrt[30]{2}$ em $\sqrt[30]{2}\zeta_{30}^i$, ou seja, os $\alpha_i's$ permutam as raízes de $p(x)$.

Denotaremos ainda γ_j, $j \in \{1, 7, 11, 13, 17, 19, 23, 29\}$,os automorfismos que preservam $\sqrt[30]{2}$ e levam ζ_{30} em ζ_{30}^j.

Dessa forma, cada α_i é um automorfismo da extensão $\mathbb{L} \mid \mathbb{Q}[\zeta_{30}]$ e os γ_j da extensão $\mathbb{L} \mid \mathbb{Q}[\sqrt[30]{2}]$. Às essas extensões associemos os grupos que chamaremos de $H = \mathrm{Aut}_{\mathbb{Q}[\zeta_{30}]}\,\mathbb{L}$ e $J = \mathrm{Aut}_{\mathbb{Q}[\sqrt[30]{2}]}\,\mathbb{L}$.

Notemos que $\mathrm{Aut}_{\mathbb{Q}}\,\mathbb{L} = G = \{\gamma_j\alpha_i\}$ ou $G = \{\alpha_i\gamma_j\}$, isso é possível, pois $\gamma_a\alpha_b = \alpha_{ab}\gamma_a$, verifiquemos:

$$\gamma_a\alpha_b(\sqrt[30]{2}) = \gamma_a(\sqrt[30]{2}\zeta_{30}^b) = \sqrt[30]{2}(\zeta_{30}^b)^a = \sqrt[30]{2}\zeta_{30}^{ab} = \alpha_{ab}(\sqrt[30]{2}) = \alpha_{ab}\gamma_a(\sqrt[30]{2})$$

e

$$\gamma_a\alpha_b(\zeta_{30}) = \gamma_a(\zeta_{30}) = \zeta_{30}^a = \alpha_{ab}(\zeta_{30}^a) = \alpha_{ab}\gamma_a(\zeta_{30})$$

Assim, temos que $H, J \leq G$, e mais $H =< \alpha_1 >$, pois $H = \{\alpha_1^0, \alpha_1^1, \alpha_1^2, \ldots, \alpha_1^{30}\} = \{\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{29}\}$, portanto H é cíclico, consequentemente, abeliano, não podemos afirmar o mesmo de J.

Com essa informação, podemos montar uma subsérie normal $\{e\} \trianglelefteq H \trianglelefteq G$ desde que tenhamos $H \trianglelefteq G$, já que obviamente $\{e\} \trianglelefteq H$. Então verifiquemos se $H \trianglelefteq G$.

Para que tenhamos $H \trianglelefteq G$, devemos ter $gHg^{-1} = H$, $\forall g \in G$.

Provemos inicialmente que $gHg^{-1} \subset H$. Seja $g = \gamma_j\alpha_i \in G$, verifiquemos que $\gamma_j\alpha_i H(\gamma_j\alpha_i)^{-1} \in H \Longrightarrow \gamma_j\alpha_i H\alpha_i^{-1}\gamma_j^{-1} \in H$

Notemos que certamente $\alpha_i H\alpha_i^{-1} \in H$, e fazendo $\alpha_i H\alpha_i^{-1} = \alpha_i$, façamos $\sigma = \gamma_j\alpha_i\gamma_j^{-1}$, devemos verificar agora que $\sigma \in H$.

$$\sigma(\zeta_{30}) = \gamma_j\alpha_i\gamma_j^{-1}(\zeta_{30})$$

Notemos que γ_j^{-1} altera ζ_{30}, α_i mantém inalterado, e γ_j desfaz o que γ_j^{-1} fez com ζ_{30}, logo,

$$\sigma(\zeta_{30}) = \zeta_{30} = \alpha_m(\zeta_{30}), \text{com } m \in \{0, 1, 2, \ldots, 29\}$$

e

$$\sigma(\sqrt[30]{2}) = \gamma_j\alpha_i\gamma_j^{-1}(\sqrt[30]{2}) = \gamma_j\alpha_i(\sqrt[30]{2}) = \gamma_j(\sqrt[30]{2}\zeta_{30}^i) = \sqrt[30]{2}\zeta_{30}^{ij} = \sqrt[30]{2}\zeta_{30}^n = \alpha_n(\sqrt[30]{2})$$

Logo σ é equivalente à um $\alpha_i \in H$, portanto $\sigma \in H$ e então $\gamma_j\alpha_i H\alpha_i^{-1}\gamma_j^{-1} \in H$.

Para termos $H \in \gamma_j\alpha_i H\alpha_i^{-1}\gamma_j^{-1}$, como $g = \gamma_j\alpha_i$, devemos ter $H \in gHg^{-1}$, e facilmente confirmamos fazendo $g = e$.

Enfim temos que $gHg^{-1} = H$, e portanto $H \trianglelefteq G$.

Voltando à nossa subsérie normal, $\{e\} \trianglelefteq H \trianglelefteq G$, podemos confirmá-la de fato. E então para garantirmos que G seja solúvel, resta mostrar que $\dfrac{G}{H}$ é abeliano, uma vez que já temos que $\dfrac{H}{\{e\}} = H$ que já sabemos que é abeliano.

Temos que:

$$\frac{G}{H} = \{\gamma_1\alpha_0 H, \gamma_1\alpha_1 H, \gamma_1\alpha_2 H, \ldots, \gamma_1\alpha_{29} H, \gamma_7\alpha_0 H, \ldots, \gamma_{29}\alpha_{29} H\}$$

Que podemos reescrever como:

$$\frac{G}{H} = \{\gamma_1 H, \gamma_7 H, \gamma_{11} H, \ldots, \gamma_{29} H\}$$

Seja $x, y \in G$, com $x = \gamma_a\alpha_b \in \gamma_i H$ para algum $i = \{1, 7, \ldots, 29\}$ e $y = \gamma_c\alpha_d \in \gamma_j H$ para algum $j = \{1, 7, \ldots, 29\}$. Podemos dizer que x é representante da classe $\bar{x}$ e y de $\bar{y}$.

Por definição, $\bar{x} = \bar{y}$ se $x \cdot y^{-1} \in H$. Calculemos $x \cdot y^{-1}$:

$$x \cdot y^{-1} = (\gamma_a\alpha_b)(\gamma_c\alpha_d)^{-1} = \gamma_a\alpha_b\alpha_d^{-1}\gamma_c^{-1}$$

Sabemos que $\alpha_b\alpha_d^{-1} \in H$, façamos $\alpha_b\alpha_d^{-1} = \alpha_e$:

$$x \cdot y^{-1} = \gamma_a\alpha_e\gamma_c^{-1}$$

Da relação que já temos, $\gamma_k\alpha_l = \alpha_{kl}\gamma_k$:

$$x \cdot y^{-1} = \alpha_{ae}\gamma_a\gamma_c^{-1}$$

E para que $\alpha_{ae}\gamma_a\gamma_c^{-1} \in H$, temos que $\gamma_a\gamma_c^{-1} = e$, ou seja $\gamma_a = \gamma_c$.

Portanto, duas classes de $\dfrac{G}{H}$ são iguais, sempre que $\gamma_a = \gamma_c$.

Como queremos saber se $\dfrac{G}{H}$ é abeliano, devemos ter $\overline{xy} = \overline{yx}$, e sabemos que isso acontece se $xy \cdot (yx)^{-1} \in H$, calculemos $xy \cdot (yx)^{-1}$:

$$xy \cdot (yx)^{-1} = (\gamma_a\alpha_b\gamma_c\alpha_d)(\gamma_c\alpha_d\gamma_a\alpha_b) = \gamma_a\alpha_b\gamma_c\alpha_d\alpha_b^{-1}\gamma_a^{-1}\alpha_d^{-1}\gamma_c^{-1}$$

Fazendo $\gamma_a = \gamma_c$:

$$xy \cdot (yx)^{-1} = \gamma_a\alpha_b\gamma_a\alpha_d\alpha_b^{-1}\gamma_a^{-1}\alpha_d^{-1}\gamma_a^{-1}$$

Sabemos que $\alpha_d\alpha_b^{-1} \in H$, façamos $\alpha_d\alpha_b^{-1} = \alpha_e$:

$$\begin{aligned} xy\cdot(yx)^{-1} &= \gamma_a\alpha_b\underbrace{\gamma_a\alpha_e}_{\alpha_{ae}\gamma_a}\gamma_a^{-1}\alpha_d^{-1}\gamma_a^{-1} \\ &= \gamma_a\alpha_b\alpha_{ae}\underbrace{\gamma_a\gamma_a^{-1}}_{e}\alpha_d^{-1}\gamma_a^{-1} \\ &= \gamma_a\underbrace{\alpha_b\alpha_{ae}\alpha_d^{-1}}_{=\alpha_f\in H}\gamma_a^{-1} \\ &= \underbrace{\gamma_a\alpha_f}_{\alpha_{af}\gamma_a}\gamma_a^{-1} \\ &= \alpha_{af}\underbrace{\gamma_a\gamma_a^{-1}}_{e} \\ &= \alpha_{af}\in H \end{aligned}$$

Portanto $\overline{xy} = \overline{yx}$ e então $\dfrac{G}{H}$ é abeliano, e então G é solúvel, como queríamos demonstrar.

□

Visto tal demonstração, podemos generalizar:

Exemplo 5.13. Dada a equação $x^n - a = 0$, com n ímpar ou n par e a positivo, solúvel por meio de radicais e com corpo de decomposição $\mathbb{Q}[\sqrt[n]{a}, \zeta_n]$, temos que seu grupo de Galois é G abeliano, logo solúvel.

Notemos que o conjunto solução de tal equação é: $\{\sqrt[n]{a}, \sqrt[n]{a}\zeta_n, \sqrt[n]{a}\zeta_n^2, \ldots, \sqrt[n]{a}\zeta_n^{n-1}\}$. E sejam $\tau, \sigma \in G$, sabemos que eles levam uma raiz, n'outra, então $\tau(\sqrt[n]{a}) = \sqrt[n]{a}\zeta_n^i$, para algum $i \in \{0, 1, 2, \ldots, n-1\}$ e $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}\zeta_n^j$ para algum $j \in \{0, 1, 2, \ldots, n-1\}$. Vejamos:

$$(\sigma\circ\tau)(\sqrt[n]{a}) = \sigma(\sqrt[n]{a}\zeta_n^i) = \sqrt[n]{a}\zeta_n^j\zeta_n^i = \sqrt[n]{a}\zeta_n^{j+i}$$

e

$$(\tau\circ\sigma)(\sqrt[n]{a}) = \tau(\sqrt[n]{a}\zeta_n^j) = \sqrt[n]{a}\zeta_n^i\zeta_n^j = \sqrt[n]{a}\zeta_n^{i+j} = \sqrt[n]{a}\zeta_n^{j+i}$$

Assim temos que $\sigma\circ\tau = \tau\circ\sigma$, logo G é abeliano, e portanto solúvel, como queríamos demonstrar.

Findamos aqui nossos esforços em mostrar quando uma equação é solúvel por radicais, e o porque de não existirem fórmulas para resolver equações de grau ≥ 5. Vale ressaltar que aqui fizemos um estudo introdutório, uma vez que toda a teoria aqui exibida é bem mais ampla, no entanto, mostramos o essencial para nosso propósito.

Para contato com o autor:
ananery_js@hotmail.com

Referências Bibliográficas

[1] GARCIA, Arnaldo; LEQUAIN, Yves. **Elementos de Álgebra**. Rio de Janeiro: IMPA, 2002. (Projeto Euclides).

[2] GONÇALVES, Adilson. **Introdução à Álgebra**.Rio de Janeiro: IMPA, 2006. (Projeto Euclides).

[3] DOMINGUES; Hygino H.;IEZZI, Gelson. **Álgebra Moderna**.São Paulo: Atual, 2003.

[4] Herstein, I. N.**Algebra Moderna: Grupos, Anillos, Campos e Teoría de Galois**. México: Editorial Trillas México, 1980.

[5] Chamizo, L. F. **¡Qué bonita es la teoría de Galois!**. Notas de curso:2004-2005.

[6] Endler, Otto. **Teoria dos Corpos**. IMPA:2012 (Publicações Matemáticas).

[7] Stewart, I. **Galois Theory**, 3 ed. Chapman & Hall/CRC mathematics.

[8] Juan, Víctor de; Valero, Pedro. **Teoría de Galois**. Apuntes UAM: 2016.

[9] Iezzi, Gelson; e outros. **Fundamentos de Matemática Elementar: Volume 6**, São Paulo: Atual, 1977.

[10] Rezende, Josiane de Carvalho. **Um Estudo sobre as Raízes da Unidade e suas Aplicações em Matemática**. Dissertação (mestrado)- Universidade Estadual Paulista: Instituto de Geociências e Ciências Exatas, Rio Claro: 2017.

[11] Fernandes, Leandro dos Santos. **Polinômios, Corpos de Decomposição e uma Introdução à Teoria de Galois**. Trabalho de Conclusão de Curso (especialização) - Universidade Federal de Minas Gerais: Instituto de Ciências Exatas, Belo Horizonte, 2016.

[12] Santos, Kaique Ribeiro Prates. **Teoria Elementar de Galois**. Trabalho de conclusão de Curso (graduação) - Universidade Estadual do Sudoeste da Bahia: Departamento de Ciências Exatas e Tecnológica, Vitória da Conquista-BA, 2016.

[13] Filho, Renato de Melo. **Números Construtíveis, os Três Problemas Gregos Clássicos e o Fabuloso Teorema de Gauss sobre Construtibilidade de Polígonos Regulares**.Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Campina Grande, Campina Grande:2016.

[14] Santos, Sérgio Ricardo dos. **As Equações Polinomiais do 3º e 4º Graus**. Dissertação (mestrado)- Universidade Federal de Sergipe, São Cristóvão: 2013.

[15] Medeiros, Nivaldo. **Teoria de Galois - Notas de Curso**, 2016.

[16] Madeira, Helen Soares. **Introdução a Teoria de Galois: Uma Perspectiva Histórica**. Universidade Católica de Brasília.

[17] Ribeiro, Denise Benino Dourado. **O Uso da História das Equações nos Processos de Ensino e de Aprendizagem de Matemática na Educação Básica**. Dissertação (mestrado - Universidade Anhanguera de São Paulo: Programa de Pós Graduação em Educação Matemática, São Paulo, 2015.