ADINA VERONICA REMOR

O MISTÉRIO POR TRÁS DA RESOLUÇÃO DE EQUAÇÕES POLINOMIAIS

TOLEDO

2021

ADINA VERONICA REMOR

O MISTÉRIO POR TRÁS DA RESOLUÇÃO DE EQUAÇÕES POLINOMIAIS

THE MYSTERY BEHIND SOLVING POLYNOMIAL EQUATIONS

Trabalho de Conclusão de Curso de graduação apresentado como requisito para obtenção do título de Licenciada em Matemática da Universidade Tecnológica Federal do Paraná (UTFPR).

Orientador: Wilian Francisco de Araújo

Coorientador: Robson Willians Vinciguerra

TOLEDO

2021

ADINA VERONICA REMOR

O MISTÉRIO POR TRÁS DA RESOLUÇÃO DE EQUAÇÕES POLINOMIAIS

Trabalho de Conclusão de Curso de graduação apresentado como requisito para obtenção do título de Licenciada em Matemática da Universidade Tecnológica Federal do Paraná (UTFPR).

Data de aprovação: 03 de agosto de 2021.

Wilian Francisco de Araújo
Doutorado
Universidade Tecnológica Federal do Paraná

Robson Willians Vinciguerra
Doutorado
Universidade Tecnológica Federal do Paraná

Leandro Antunes
Doutorado
Universidade Tecnológica Federal do Paraná

Larissa Hagedorn Vieira
Mestrado
Universidade Tecnológica Federal do Paraná

TOLEDO
2021

Este trabalho é dedicado à minha família, que são tudo para mim.

Agradecimentos

Em primeiro lugar, agradeço a Deus pelo dom da vida e por ser tão bom comigo.

Agradeço à minha família, em especial aos meus amados pais e meu amado irmão, por todo o apoio e amor incondicional. Por sempre me incentivarem e darem todas as condições necessárias para que eu pudesse ir em busca dos meus sonhos.

Agradeço a minha melhor amiga Andressa, por sempre me ouvir e me apoiar. Por todas as risadas, choros e loucuras partilhadas.

Agradeço ao meu amor Bruno, por todo o apoio, incentivo, por ser meu porto seguro. Por me compreender e tornar a minha vida mais feliz.

Agradeço aos meus amigos Anderson, Gustavo, Luana, Luiz e Rodrigo por todos os momentos de alegria e desespero partilhados ao longo do curso. A graduação não seria a mesma sem o nosso grupo do fundão.

Agradeço a todos os outros amigos que tive o privilégio de conviver ao longo destes anos de graduação, Jeferson, James, Daniele, Samara, Aline, Scheila, Sabrina, Judy, entre outros. Obrigada por tornarem esta caminhada mais leve.

Agradeço a todos os professores que fizeram parte da minha graduação, por todos os aprendizados adquiridos. Por todo o incentivo, por cada conselho e ajuda prestados, vocês merecem toda a minha admiração.

Em especial, agradeço aos meus professores orientadores Wilian e Robson, meus pais do coração. Obrigada por toda a paciência, confiança, exemplo e incentivo.

Por fim, agradeço ao CNPq pelo auxílio financeiro.

"Por vezes sentimos que aquilo que fazemos não é senão uma gota de água no mar. Mas o mar seria menor se lhe faltasse uma gota."
(Madre Teresa de Calcutá)

Resumo

Resolver equações polinomiais foi um problema que acompanhou inúmeros matemáticos ao longo dos séculos. Conforme a matemática ia se aprimorando, fórmulas para encontrar raízes de polinômios foram sendo elaboradas. Mas o grande mistério que atormentava a comunidade matemática até o século XIX, era que ninguém conseguia encontrar uma fórmula resolutiva para as equações polinomiais de grau 5, utilizando apenas as operações de adição, subtração, multiplicação, divisão, potenciação e radiciação (conhecidas como resolução por radicais). Vários matemáticos tentaram resolver este problema, sem sucesso, até que um jovem matemático, chamado Evariste Galois (1811-1832), desenvolveu uma teoria inovadora que solucionou este mistério. O objetivo deste trabalho é apresentar a teoria desenvolvida por Galois, mostrando porque não é possível encontrar uma fórmula resolutiva por radicais que forneça as raízes de polinômios de grau maior ou igual a 5. Também pretende-se apresentar vários exemplos que demonstram como esta teoria funciona. Por fim, serão apresentados métodos que permitem calcular o grupo de Galois de qualquer polinômio de grau menor ou igual a 5.

Palavras-chave: Teoria de Grupos. Extensões de Corpos. Teoria de Galois.

Abstract

Solving polynomial equations was a problem that followed countless mathematicians over the centuries. As mathematics improved, formulas for finding polynomial roots were developed. But the great mystery that plagued the mathematical community until the 19th century was that no one could find a solving formula for polynomial equations of degree 5 using only the operations of addition, subtraction, multiplication, division, exponentiation, together with the extraction of roots (known as solving by radicals). Several mathematicians tried to solve this problem, unsuccessfully, until a young mathematician named Evariste Galois (1811-1832) developed an innovative theory that solved this mystery. The objective of this work is to present the theory developed by Galois, showing why it is not possible to find a solving formula by radicals that provides the roots of polynomials of degree greater than or equal to 5. It is also intended to present several examples that demonstrate how this theory works. Finally, methods will be presented to calculate the Galois group of any polynomial of degree less than or equal to 5.

Keywords: Group theory. Field extensions. Galois theory.

Lista de ilustrações

Figura 1 – Evariste Galois (1811-1832) 19
Figura 2 – Polígonos regulares inscritos em uma circunferência 24
Figura 3 – Simetrias do quadrado 24
Figura 4 – Aplicando $R_1 R_{\frac{\pi}{2}}$ em $P_1P_2P_3P_4$ 25
Figura 5 – Aplicando $R_1 R_{\frac{\pi}{2}}$ e $R_{\frac{\pi}{2}} R_1$ em $P_1P_2P_3P_4$ 26
Figura 6 – O grupo de Galois de $x^4 - 2$ interpretado como simetrias do quadrado . . . 74
Figura 7 – Triângulo equilátero inscrito em uma circunferência unitária com centro na origem, formado pelas raízes cúbicas da unidade 85

Lista de tabelas

Tabela 1 – Tábua do grupo S_3 22
Tabela 2 – $\mathbb{Q}$-automorfismos de $\mathbb{Q}[i, \sqrt{5}]$ 70
Tabela 3 – $\mathbb{Q}$-automorfismos de $\mathbb{Q}[i, \xi]$ 74
Tabela 4 – $\mathbb{Q}$-automorfismos de $\mathbb{Q}[i, \sqrt{2}]$ 79
Tabela 5 – $\mathbb{Q}$-automorfismos de $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$ 81
Tabela 6 – $\mathbb{Q}$-automorfismos de $\mathbb{Q}[u]$, em que u é uma raiz 11-ésima primitiva da unidade 88
Tabela 7 – $\mathbb{Q}$-automorfismos de $\mathbb{Q}[\alpha, u]$ 90
Tabela 8 – $\mathbb{Q}$-automorfismos de $\mathbb{Q}[\alpha, u]$ 91
Tabela 9 – $\mathbb{Q}$-automorfismos de $\mathbb{Q}[\beta, u]$ 96
Tabela 10 – Critérios para calcular o grupo de Galois de um polinômio irredutível de grau 4111
Tabela 11 – Polinômios irredutíveis de grau 4 com diferentes grupos de Galois sobre $\mathbb{Q}$. 111
Tabela 12 – Exemplos de polinômios irredutíveis $f(x)$ de grau 5 e seus respectivos polinômios resolventes 112
Tabela 13 – Critérios para determinar o grupo de Galois de um polinômio irredutível de grau 5 113
Tabela 14 – Exemplos de polinômios irredutíveis $f(x)$ de grau 5 com diferentes grupos de Galois sobre $\mathbb{Q}$ 113

Lista de símbolos

G	denotará um grupo;
$o(G)$	denotará a ordem de um grupo;
$\mathbb{Z}_m$	denotará o grupo aditivo das classes de restos módulo m;
$charK$	denotará a característica do corpo K;
$H \leq G$	denotará que H é um subgrupo de G;
$H \lhd G$	denotará que H é um subgrupo normal de G;
S_n	denotará o grupo das permutações do conjunto $\{1, ..., n\}$;
A_n	denotará o grupo das permutações pares do conjunto $\{1, ..., n\}$;
D_n	denotará o grupo diedral de ordem $2n$;
$Ker(f)$	denotará o núcleo de um homomorfismo f;
$(G : H)$	denotará o índice de H em G;
$K[x]$	denotará o anel de polinômios sobre um corpo K na indeterminada x;
$K[x] \cdot f(x)$	denotará o ideal de $K[x]$ gerado pelo polinômio $f(x)$;
$\partial p(x)$	denotará o grau do polinômio $p(x)$;
$K(\alpha)$	denotará o menor corpo obtido de K adjuntando α;
$K[\alpha]$	denotará o conjunto $\{p(\alpha) \mid p(x) \in K[x]\}$;
$L : K$	denotará a extensão de corpos L de K;
$[L : K]$	denotará a dimensão da extensão $L : K$ vista como espaço vetorial;
$Gal(f, K)$	denotará o corpo de decomposição do polinômio $f(x) \in K[x]$;
$Aut_K L$	denotará o conjunto dos K-automorfismos de L;
$\Gamma(L : K)$	denotará o grupo de Galois da extensão $L : K$;
M^*	denotará o grupo formado por todos os M-automorfismos de L;
$H^\dagger$	denotará o corpo fixo de H;

$\mathcal{F}$	denotará o conjunto dos corpos intermediários;
$\mathcal{G}$	denotará o conjunto dos subgrupos do grupo de Galois;
$P(X)$	denotará o conjunto das permutações dos elementos do conjunto X;
α^g	denotará a ação de g em α;
Id ou e	denotará o elemento neutro do grupo;
Id	também poderá denotar a função identidade.

Sumário

1 INTRODUÇÃO 14

2 NOTA HISTÓRICA 17

3 PRÉ-REQUISITOS 21
3.1 Grupos 21
3.2 Anéis 27
3.3 Anel de polinômios 30

4 EXTENSÕES DE CORPOS 35
4.1 Extensões algébricas e transcendentes 39
4.2 Corpo de decomposição de um polinômio 44
4.3 Grau de uma extensão 48
4.4 Extensões galoisianas, normais e separáveis 57

5 TEORIA DE GALOIS 61
5.1 Adentrando à teoria de Galois 61
5.2 Automorfismos de corpos 63
5.2.1 Fecho normal 64
5.3 A correspondência de Galois 68
5.4 Exemplos 69
5.4.1 Exemplo 1 69
5.4.2 Exemplo 2 73
5.4.3 Exemplo 3 79
5.4.4 Exemplo 4 84
5.4.5 Exemplo 5 89
5.4.6 Exemplo 6 94

6 SOLUBILIDADE E CÁLCULO DO GRUPO DE GALOIS DE POLINÔMIOS 99
6.1 Solução por radicais 99
6.1.1 Grupos solúveis 99
6.1.2 Extensões radicais 101
6.2 Classificando os Grupos de Galois 105
6.2.1 Polinômios de grau 2 106
6.2.2 Polinômios de grau 3 108
6.2.3 Polinômios de grau 4 110

6.2.4 Polinômios de grau 5 111

7 CONSIDERAÇÕES FINAIS 115

REFERÊNCIAS 116

Índice 119

1 Introdução

Na matemática, qualquer problema que possa ser solucionado através dos números certamente pode ser tratado direta ou indiretamente, por meio de equações. Como interpretar equações? Equações estão relacionadas a maneira como equivalências entre associações de entes estão representadas. Assim, trata-se de uma igualdade estabelecida por meio uma relação entre fatos, conceitos e ideias. Elas podem ser encontradas nas mais variadas áreas, e o pensamento resolutivo constitui a base da matemática.

Assim, as equações, sejam elas algébricas, exponenciais, logarítmicas, trigonométricas, etc. são o alicerce da matemática, e a busca por suas resoluções sempre motivaram os matemáticos de todos os tempos. Neste trabalho estaremos interessados em um tipo especial de equação citado anteriormente: as equações algébricas. Elas são aquelas cujos coeficientes pertencem a um corpo K e as únicas operações realizadas são soma, subtração, multiplicação, divisão, potenciação e radiciação. A forma geral de uma equação algébrica é

$$a_0 + a_1x + a_2x^2 + ... + a_nx^n = 0 \tag{1.1}$$

em que $n \in \mathbb{Z}$ e $a_0, a_1, ..., a_n \in K$. O maior índice n tal que $a_n \neq 0$ é denominado o grau da referida equação.

De acordo com [GARBI, 2010], ao longo dos milênios várias descobertas envolvendo o grau dessas equações e a busca por suas resoluções foram alcançadas, porém o auge dos avanços nesse tema foi alcançado graças a um jovem chamado Evariste Galois. As pesquisas desenvolvidas por esse matemático mudaram todo o rumo da Álgebra, permitindo o surgimento de novas teorias: a teoria de grupos, que possuí aplicações nos mais variados campos e a teoria de Galois, uma das teorias mais lindas que existe e responsável por dar uma resposta satisfatória a um problema matemático que ficou em aberto por inúmeros séculos, a solubilidade de equações de grau maior ou igual a 5. De acordo com [FREIRE, 2009],

> Os trabalhos do matemático francês Evariste Galois exerceram enorme influência na Matemática do século XX, sendo uma das fontes do surgimento do conceito de Estrutura Matemática, que é central para essa disciplina atualmente. Essas observações apontam reflexos da originalidade, fertilidade e generalidade das ideias de Galois. Na verdade, é possível afirmar que a Teoria de Galois marca a transição histórica da Álgebra como estudo de polinômios para a chamada Álgebra Moderna, ou seja, o estudo de estruturas algébricas.

O tema escolhido para o desenvolvimento deste trabalho é álgebra abstrata, e o objeto de estudo é a teoria de Galois. Em especial, estaremos interessados em responder o

que é a teoria de Galois e como ela demonstra se determinado polinômio é solúvel por radicais, ou seja, se é possível encontrar uma fórmula que forneça as raízes desse polinômio utilizando apenas operações de adição, subtração, multiplicação, divisão, radiciação e potenciação.

Além disso, vamos apresentar diferentes exemplos que demonstram como a teoria de Galois funciona. Geralmente, livros clássicos de teoria de Galois exibem poucos exemplos e de forma bem resumida. Neste material, construímos uma gama de opções, apresentando todos os cálculos realizados.

Dessa forma, o objetivo geral deste trabalho é estudar a teoria de Galois e classificar se um polinômio é solúvel por radicais ou não, bem como apresentar exemplos do cálculo do grupo de Galois de alguns polinômios dados. Para isso, consultamos diversos materiais: trabalhos de conclusão de curso como [CRUZ, 2014], [FERNANDES, 2016], e [SOUZA, 2017], que possuíam uma linguagem mais acessível e introdutória; livros como [COELHO; LOURENCO, 2018], [DOMINGUES; IEZZI, 2003], [GARCIA A.; IEQUAIN, 2013] e [GONÇALVES, 2012] no qual definições, exemplos e resultados da teoria de grupos, teoria de anéis e extensões de corpos necessários para construir a teoria de Galois foram estudados; livros como [COX, 2004], [HOWIE, 2006], [MILNE, 2020], [MORANDI, 1996] e [STEWART I, 2015], que desenvolvem a teoria de Galois, sendo este trabalho baseado principalmente em [STEWART I, 2015].

Este trabalho está organizado em cinco capítulos. No primeiro capítulo, apresentamos um breve resumo histórico a respeito da investigação da resolução de equações algébricas. O segundo capítulo apresenta definições e resultados básicos da teoria de grupos, teoria de anéis e anéis de polinômios. No terceiro capítulo, discorremos a respeito das extensões de corpos, mostrando exemplos e resultados necessários para o quarto capítulo, que é o auge deste trabalho.

No quarto capítulo, está explicada a teoria de Galois, relacionando grupos finitos com as extensões de corpos. É neste capítulo que também são apresentados inúmeros exemplos de construções de grupos de Galois, desenvolvidos por autoria própria, ou baseados em [ANDRADE, 2013], [REZENDE, 2017] e [STEWART I, 2015]. Por fim, no último capítulo, mostramos porque nem todas as equações de grau maior ou igual a 5 são solúveis por radicais, e também classificamos todos os grupos de Galois de um polinômio irredutível com grau menor ou igual a 5. Como será visto, é possível computar o grupo de Galois apenas conhecendo o polinômio e algumas ferramentas auxiliares. Para o desenvolvimento deste capítulo, nos baseamos nos materiais [AWTREY; BEUERLE; KEENAN, 2017], [AWTREY; CESARSKI; JAKES, 2017], [BARAI, 2019], [BERGLUND, 2011], [CASTRO, 2007], [CONRAD, 2010b], [CONRAD, 2010a], [DUMMIT, 1991], [GUDKOV; LUR'E, 2017], [KAPPE; WARREN, 1989], [KAVANAGH, 2010], [LAVALLEE, 2008], [ROMERO, 2018] e [ROTH, 1971].

Espera-se que por meio deste trabalho, interessados em conhecer essa área tenham maior embasamento da teoria, visto que pretende-se apresentar mais exemplos e tornar a linguagem mais acessível, já que normalmente os livros apresentam uma notação mais carregada e de difícil compreensão. Assim, caro leitor, sinta-se convidado a embarcar nesta aventura que inicia-se agora, no qual primeiramente viajaremos ao longo da história da matemática. Após, faremos algumas paradas na teoria de grupos, anéis e extensões de corpos. Por fim, esperamos que você se divirta com a teoria de Galois, entendendo os exemplos e compreendendo como esta teoria resolve o problema que ficou em aberto por tantos séculos.

2 Nota histórica

As primeiras manifestações de equações matemáticas podem ser observadas em papiros mesopotâmicos e egípcios, envolvendo problemas geométricos como o cálculo de área e perímetro e a busca por medidas desconhecidas. De acordo com [GARBI, 2010], os matemáticos babilônicos do II milênio a.C. também já possuíam um grande conhecimento matemático, resolvendo equações do primeiro e segundo grau.

Na Europa, as primeiras manifestações de equações do segundo grau surgiram na escola pitagórica, com a famosa relação: $a^2 = b^2 + c^2$, em que a, b, e c representam os lados de um triângulo retângulo. A busca por ternas pitagóricas originou inúmeros estudos e influenciou grandes matemáticos ao longo dos séculos. Euclides, em seu livro *Os elementos* definiu algumas noções comuns que permitem a resolução de equações do primeiro grau.

No primeiro milênio da era cristã surgiram inúmeros matemáticos talentosos na Índia. Nesse contexto a fórmula geral para resolução de equações do segundo grau foi desenvolvida. Ela também é conhecida como fórmula de Bhaskara (embora não seja ele o autor).

No início do século XVI a disputa por encontrar as resoluções das equações algébricas continuou. Aqui, podemos destacar dois matemáticos muito importantes: Girolamo Cardano (1501-1576) e Nicolo Fontana (1501-1557), mais conhecido por Tartaglia, que travaram uma longa briga para encontrar a fórmula geral da equação cúbica. No final, Tartaglia conseguiu o feito, embora a fórmula de resolução tenha sido chamada de fórmula de Cardano.

Ainda nesse período da história, Ludovico Ferrari, discípulo de Cardano, conseguiu encontrar a fórmula geral para resolver equações do quarto grau. Agora, depois de avanços tão consideráveis, as perguntas que surgiram na comunidade matemática foram: equações de quinto grau também são solúveis por radicais? Ou seja, há um expressão matemática que utiliza apenas as seis operações básicas, que é escrita em torno dos coeficientes e que permite encontrar as raízes dessa equação?

Os maiores nomes das matemática, como Descartes, Fermat, Newton, Euler, Bernoulli, Laplace e Gauss viveram durante os séculos XVII, XVIII e XIX. Por meio das descobertas feitas anteriormente, tais matemáticos desenvolveram diversos avanços, como o surgimento dos números complexos, da geometria analítica, do cálculo e dos números irracionais. Perguntas como: “Por que a fórmula de Tartaglia só fornece uma solução? Não é natural pensar que uma equação do terceiro grau tenha mais de uma solução?”, “Como determinar todas as soluções de uma equação algébrica?”, “Como encontrar as soluções de uma equação do quinto grau?” contribuíram para esses avanços. Porém, a última questão ainda estava em aberto. Paolo Ruffini (1765-1822) tentou fazer uma demonstração para essa

última questão, porém não conseguiu realizá-la corretamente.

Niels Henrik Abel (1802-1829) desenvolveu avanços nesse tema. Antes mesmo de entrar na universidade, ele publicou um artigo contendo a fórmula geral de resolução das equações do quinto grau. Seus professores não conseguiram detectar qualquer falha no seu pensamento, e até mesmo o maior matemático do seu país, que deveria avaliar o artigo, não foi capaz de encontrar erros. Mas, por precaução, achou melhor solicitar que Abel escrevesse o artigo mais detalhadamente. Ao fazer isso, Abel notou que havia algo estranho. Percebendo seus erros, alguns anos depois ele conseguiu demonstrar que, a menos de casos particulares, uma equação do quinto grau não é solúvel por radicais. Por meio dos estudos que Abel realizou, e a sua demonstração que utilizava a álgebra da época, o norueguês representa o ápice da álgebra clássica.

Mas algumas dúvidas ainda pairavam no ar: se há casos particulares que podem ser solúveis por radicais, como podemos caracterizá-los? Qual é a relação entre as raízes dessas equações, quando existem?

Nesse mesmo período um jovem matemático surgiu com ideias brilhantes, que estavam além da compreensão das demais pessoas. Seu nome é Evariste Galois, e é conhecido como o pai da Álgebra Moderna. Ele foi responsável pelo surgimento de uma nova teoria (que posteriormente recebeu seu nome em sua homenagem), que, entre uma das suas aplicações foi demonstrar o porquê equações algébricas de quinto grau não são solúveis por radicais. Embora Abel já tivesse alcançado esse resultado, Galois criou uma teoria independente das ideias de Abel, e na teoria criada por Galois, o resultado de Abel se torna um caso particular. Assim, Abel marca o auge da Álgebra Clássica, enquanto Galois representa o início da Álgebra Moderna.

Porém, apesar de sua importância para a matemática, Évariste Galois não recebeu o devido reconhecimento que merecia. Sua vida foi marcada por fatos lamentáveis, tendo como resultado seu falecimento de maneira tão estúpida. Evariste Galois nasceu em Bourg-la-Reine na França em 25 de outubro de 1811, no seio de uma família culta e liberal, durante a primeira república de Napoleão Bonaparte. Seu avô paterno fora diretor de uma escola da Universidade Imperial e seus pais Nicholas-Gabriel Galois e Adelaide-Marie Demante haviam estudado filosofia, literatura clássica e religião, ou seja, as disciplinas consideradas importantes na época. Seu pai, foi nomeado prefeito da cidade em que moravam e até os 12 anos de idade, sua mãe foi sua professora e o ensinou grego e latim. Então, em 1823, ele foi matriculado no Liceu Louis-le-Grand, uma escola preparatória em Paris, onde também estudaram Victor Hugo e Robespierre.

Figura 1 – Evariste Galois (1811-1832)

Fonte: (Google, 2021)

No início de sua jornada no Liceu Louis-le-Grand, Galois se destacava e era muito elogiado pelos professores. Mas com o tempo, passou a interessar-se apenas pela matemática e teve uma grande queda no desempenho em disciplinas humanas.

Assim, em 1828, Galois se inscreveu para a École Polytechnique de Paris, antes de concluir o curso básico em matemática, mas ele foi rejeitado. Ele passou a ser orientado pelo professor Louis-Paul-Emile e publicou seu primeiro trabalho: *Demonstração de um teorema sobre frações contínuas periódicas*, ao mesmo tempo em que trabalhava em outro projeto mais importante: *Pesquisas sobre as equações algébricas de grau primo*. Este trabalho foi entregue a Cauchy, para tentar novamente uma vaga na École Polytechnique, mas novamente não conseguiu.

Poucos dias após ser reprovado pela segunda vez, seu pai se suicidou após ser vítima de boatos espalhados por um religioso com objetivos políticos conflitantes. Isto fez com que Galois se tornasse um rebelde político.

Em 1829, Evariste ingressou na École Normale Supérieure, onde publicou 3 artigos que faziam parte no trabalho entregue a Cauchy. Ele também entregou este trabalho para ser avaliado para o Grande Prêmio da Matemática, mas o relator Fourier morreu antes de lê-lo e o manuscrito se perdeu. Isso fez com que Galois se sentisse desprezado pelo meio científico.

Em 1830, houve uma revolução que derrubou o monarca Charles X, através de rebeliões e enfrentamentos das tropas do rei. Galois queria participar das batalhas, mas o diretor da escola onde estava não permitiu que os alunos participassem. Com o fim da rebelião e a manutenção da monarquia com o novo rei Louis Philippe, Galois escreveu para uma revista reclamando da posição do diretor em proibi-lo de participar das rebeliões, logo depois, também publicou um artigo atacando professores, examinadores e editores

afirmando que eram medíocres. Isso fez com que fosse expulso da instituição.

Ele então submeteu seu trabalho a Academia Simèon-Dennis Poisson, e passou a dedicar-se a política. Em um jantar de republicanos, Galois propôs um brinde ao rei fazendo um gesto com o punhal (sugerindo um assassinato), a notícia se espalhou e ele foi preso, mas em junho de 1831 foi solto. Durante as comemorações de um ano da revolução de 1830, Galois foi preso novamente a pedido do rei. Durante o período em que ficou preso, soube que seu trabalho não foi aceito pela academia e decidiu iniciar o trabalho *Duas Memórias de Análise Pura* e pediu que o enviasse para vários matemáticos renomados. Dois dias antes de seu aniversário de 20 anos, ele foi condenado a 6 meses de prisão.

Neste período, uma epidemia de cólera tomou conta de Paris, e os detentos foram transferidos para um hospital. No hospital, Galois conheceu Stéphanie Poterin du Motel, sobrinha de um médico, e apaixonou-se. Galois foi muito insistente e a moça que não estava interessada queixou-se com o colega de Galois, Duchâtelet. Os dois tiveram uma discussão, Galois ofendeu a moça e Duchâtelet o desafiou a um duelo.

Então, em 29 de maio de 1832, véspera do duelo, Galois passou a noite escrevendo cartas a seus companheiros republicanos e reescrevendo seu trabalho. Nas margens ele anotava detalhes para tornar sua escrita mais inteligível e em algumas demonstrações escrevia "eu não tenho tempo... eu não tenho tempo". Então ele foi para o duelo, pegou uma das pistolas (segundo as más línguas, apenas uma possuía munição) e caminhou até sua posição. Duchâtelet atirou e Galois caiu, mas não morreu ali, foi levado a um hospital, onde morreu na manhã de 31 de maio de 1832.

Como já citado anteriormente, Galois representa um marco na história da matemática. Graças a ele, a álgebra moderna surgiu. Suas contribuições nesse campos são incontáveis. Certamente Galois estava a frente de seu tempo, fazendo jus ao título de pai da álgebra moderna.

Neste trabalho, esperamos que você conheça um pouco melhor as ideias de Galois, podendo aprofundar-se nos pensamentos desse grande gênio que viveu há dois séculos atrás. Que você possa se divertir ao estudar essa teoria tão bonita, e que seja uma grande aventura para todos nós.

3 Pré-requisitos

Neste capítulo apresentaremos alguns resultados e definições básicos para o desenvolvimento deste trabalho. Falaremos a respeito de algumas estruturas, como grupos, anéis, anel dos polinômios, corpos e suas propriedades. As demonstrações serão omitidas, já que não caracterizam o foco de estudo neste momento, e podem ser encontradas nos livros [COELHO; LOURENCO, 2018], [DOMINGUES; IEZZI, 2003] e [GONÇALVES, 2012].

3.1 Grupos

Nessa seção, falaremos a respeito da estrutura algébrica grupo, bem como alguns resultados e definições que serão importantes no decorrer deste trabalho.

Definição 3.1. *Um sistema matemático constituído de um conjunto G, tal que $G \neq \varnothing$, e uma operação $(x, y) \mapsto x * y$ sobre G é chamado **grupo** se as seguintes condições são satisfeitas:*

i) Associatividade: $(a * b) * c = a * (b * c)$, quaisquer que sejam $a, b, c \in G$.

ii) Existência do elemento neutro: existe um elemento $e \in G$ tal que $a * e = e * a = a$, qualquer que seja $a \in G$.

iii) Existência do simétrico: para todo $a \in G$ existe um elemento $a' \in G$ tal que $a * a' = a' * a = e$.

Se um grupo $(G, *)$ satisfazer a propriedade comutativa, ou seja, $\forall\, a, b \in G$ temos $a * b = b * a$, então $(G, *)$ é chamado **grupo abeliano**. Temos também os grupos finitos, no caso em que o conjunto G é finito. Nesse caso, o número de elementos de G é chamado *ordem* do grupo, representado por $o(G)$, e a tábua da operação $*$ (que por meio de uma tabela representa como os elementos são operados) se denomina *tábua do grupo.*

Definição 3.2. *Um grupo $(G, *)$ é cíclico quando ele pode ser gerado por um elemento a, ou seja, $G = [a] = \{a^m \mid m \in \mathbb{Z}\}$ (o elemento a é operado com ele mesmo m vezes).*

Vamos apresentar alguns exemplos:

Exemplo 3.3. *Os conjuntos numéricos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são exemplos de grupos, com a operação adição. Além disso, os conjuntos $\mathbb{Q}^*$, $\mathbb{R}^*$ e $\mathbb{C}^*$ são grupos multiplicativos.*

Exemplo 3.4. *O conjunto das classes de restos módulo m, $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$, também é exemplo de grupo, munido com a operação soma, cuja ordem é m.*

Lembra-se quando comentamos que a ideia de Galois foi permutar as raízes? E através dessa ideia que ele desenvolveu sua teoria? Pois bem, o próximo exemplo falará a respeito das permutações, que são os elementos que dão base para a Teoria de Galois.

Exemplo 3.5. *Seja S um conjunto não vazio e seja $G = \{f : S \to S \mid f$ é bijetiva$\}$. G com a operação $\circ$ (composição de funções) é grupo, tendo a função identidade Id como elemento neutro. Esse grupo é chamado grupo das permutações do conjunto S. Se $S = \{1, 2, \ldots, n\}$ denotaremos esse grupo por S_n e temos que o número de elementos de S_n é exatamente $n!$. Para $n \geq 3$, S_n é um grupo não abeliano.*

Sejam $a_1, a_2, \ldots, a_r \in I_n$ inteiros distintos, com $I_n = \{1, 2, \ldots, n\}$, $n \geq 2$. Se $\sigma \in S_n$ é uma permutação tal que $\sigma(a_1) = a_2$, $\sigma(a_2) = \sigma^2(a_1) = a_3, \ldots, \sigma(a_{r-1}) = \sigma^{r-1}(a_1) = a_r$ e $\sigma(a_r) = \sigma^r(a_1) = a_1$ e $\sigma(x) = x$ para todo $x \in I_n - \{a_1, a_2, \ldots, a_r\}$ então se diz que σ é um *ciclo de comprimento* r (ou *r-ciclo*) e que $\{a_1, a_2, \ldots, a_r\}$ é o *conjunto suporte de* σ. Tal ciclo será denotado por $(a_1 a_2 \ \ldots \ a_r)$. Se $r = 2$, então σ é chamado *transposição.*

Por exemplo, vamos comentar a respeito do S_3. O grupo S_3 possui $3! = 6$ elementos, que são todas as possíveis permutações dos elementos $1, 2$ e 3. Seja $\sigma \in S_3$. Se $\sigma(1) = 2$, $\sigma(2) = \sigma^2(1) = 3$ e $\sigma(3) = \sigma^3(1) = 1$, então a permutação σ é um $3-$ciclo, representado por (123). Já a permutação $\theta \in S_3$, $\theta(1) = 2$, $\theta(2) = 1$ e $\theta(3) = 3$ pode ser representada pelo ciclo (12), que é uma transposição. Observe que a função identidade Id não permuta nenhum elemento, por isso $Id(1) = 1$, $Id(2) = 2$ e $Id(3) = 3$. Assim, podemos encontrar todos os elementos de S_3 utilizando a notação acima, que são $Id, (12), (13), (23), (123)$ e (132). Para ver o resultado das composições desses elementos, podemos construir a tábua do grupo, como pode ser observado na Tabela 1.

Observe que este grupo é não abeliano, já que $(123) \circ (23) = (12)$ e $(23) \circ (123) = (13)$.

Tabela 1 – Tábua do grupo S_3

$\circ$	Id	(12)	(13)	(23)	(123)	(132)
Id	Id	(12)	(13)	(23)	(123)	(132)
(12)	(12)	Id	(132)	(123)	(23)	(13)
(13)	(13)	(123)	Id	(132)	(12)	(23)
(23)	(23)	(132)	(123)	Id	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	Id
(132)	(132)	(23)	(12)	(13)	Id	(123)

Fonte: Os autores (2021)

Além disso, cada $\sigma \in S_n$ pode ser expressa como uma composição de transposições (Ver [DOMINGUES; IEZZI, 2003], p. 203). Por exemplo, a permutação (123) pode ser expressa por $(13)(12)$. Essa notação é mais conveniente, já que a partir dela definimos permutações pares e ímpares: se uma permutação é expressa por um número par de transposições, dizemos que essa permutação é par; caso contrário, dizemos que é ímpar. Assim, a permutação (123) é uma permutação par, já a permutação (12) é ímpar. Esta paridade está bem definida. Para maiores informações, consultar [DOMINGUES; IEZZI, 2003], p. 206.

Exemplo 3.6. *Sejam $(G, *)$ e (J, Δ) dois grupos. No conjunto $G \times J$ definimos a operação $(g_1, j_1) \cdot (g_2, j_2) = (g_1 * g_2, j_1 \Delta j_2)$, em que $g_1, g_2 \in G$, $j_1, j_2 \in J$. Com esta operação, $G \times J$ adquire estrutura de grupo, chamado produto direto de G com J.*

O elemento neutro do grupo acima é (e, u), em que e é o elemento neutro de G e u é o elemento neutro de J. Além disso, o inverso de um elemento $(g, j) \in G \times J$ é (g', j'). Por fim, $G \times J$ é um grupo abeliano se e somente se $(G, *)$ e (J, Δ) são grupos abelianos.

Por exemplo, considere $G = (\mathbb{Z}_2, +)$ e $J = (\mathbb{Z}_2, +)$. Os elementos de $G \times J = \mathbb{Z}_2 \times \mathbb{Z}_2$ são $(0,0), (1,0), (0,1)$ e $(1,1)$. O elemento neutro de $\mathbb{Z}_2 \times \mathbb{Z}_2$ é $(0,0)$, e pode-se perceber também que para todo $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ tem-se $(a, b)^2 = (a, b) + (a, b) = (0, 0) = e$.

Portanto $G = (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ é um grupo abeliano não cíclico.

Do mesmo modo que introduzimos o grupo $G \times J$ poderíamos introduzir o grupo $G_1 \times G_2 \times \ldots \times G_n$ chamado de *produto direto (externo)* dos grupos $G_1, \ldots, G_n$.

A fim de facilitar a linguagem, a partir de agora adotaremos a notação G para grupo, no lugar de $(G, *)$. Além disso, a operação $*$ será representada por $\cdot$ e o elemento simétrico de qualquer elemento x será representado por x^{-1}.

Sejam G um grupo e H um subconjunto não vazio de G. Dizemos que H é um **subgrupo** de G se, com a mesma operação de G, H também for um grupo.

Mas, caso queiramos descobrir se H é subgrupo de G, verificar todas as propriedades novamente em H pode ser laborioso. Assim, o seguinte teorema nos auxilia nesse aspecto:

Teorema 3.7. *Seja H um subconjunto não-vazio do grupo $(G, \cdot)$. Então H é subgrupo de G se e somente se $a \cdot b^{-1} \in H$.*

Demonstração. Ver [DOMINGUES; IEZZI, 2003], p. 154. □

Podemos citar alguns exemplos de subgrupos, como:

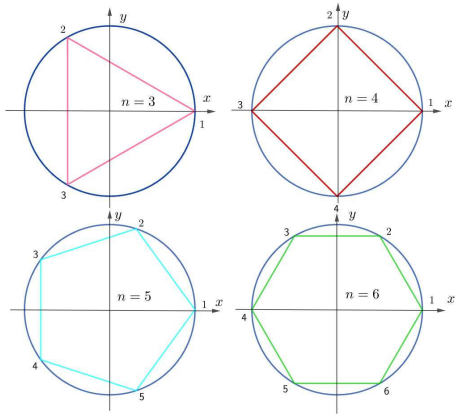
Exemplo 3.8. *O conjunto $m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\}$ é subgrupo de $(\mathbb{Z}, +)$, gerado por m.*

Exemplo 3.9. *O grupo alternado A_n formado por todas as permutações pares é subgrupo de S_n, cuja ordem é $\dfrac{n!}{2}$.*

Exemplo 3.10. *Vamos apresentar um outro grupo muito interessante, que contém exatamente $2n$ elementos e é subgrupo de S_n.*

Seja $1, 2, 3, \ldots, n$ o conjunto dos vértices de um polígono regular de n lados. Observe a figura a seguir, no qual construímos os polígonos regulares para $n = 3, 4, 5$ e 6.

Figura 2 – Polígonos regulares inscritos em uma circunferência



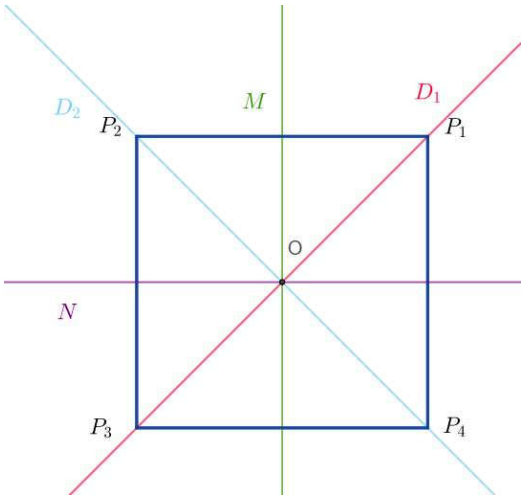
Fonte: Os autores (2021)

Seja $\theta \in S_n$ a permutação determinada pelo efeito de uma rotação de um ângulo de $\frac{2\pi}{n}\, rd$ no sentido anti-horário, isto é, $\theta = (123\ldots\ n-1\ n)$. Considere também $r \in S_n$ a permutação determinada pelo efeito de uma reflexão da figura em torno do eixo x, isto é, se n é par, r fixa os vértices 1 e $\frac{n+2}{2}$ e é representada por $(2\ n)(3\ n-1)\ldots(\frac{n}{2}\ \ \frac{n+4}{2})$. Se n é ímpar, r fixa apenas o vértice 1 e é representada por $(2\ n)(3\ n-1)\ldots(\frac{n+1}{2}\ \ \frac{n+3}{2})$.

Observe que $D_n = \langle \theta, r\rangle = \{e, r, \theta, \theta^2, \theta^3, \ldots, \theta^{n-1}, r\theta, r\theta^2, \ldots, r\theta^{n-1}\}$ é subgrupo de S_n, onde e é a identidade de S_n. Chamamos D_n de *grupo diedral de ordem* $2n$ ou *grupo de simetrias do polígono regular de* n *lados.*

Vamos apresentar mais detalhadamente o D_4, grupo das simetrias do quadrado, que é subgrupo do S_4. Assim, seja $P_1P_2P_3P_4$ um quadrado, D_1 e D_2 suas diagonais, M e N suas mediatrizes e O o ponto de intersecção dessas quatro retas, como a seguir:

Figura 3 – Simetrias do quadrado



Fonte: Os autores (2021)

As transformações espaciais que preservam o quadrado são:

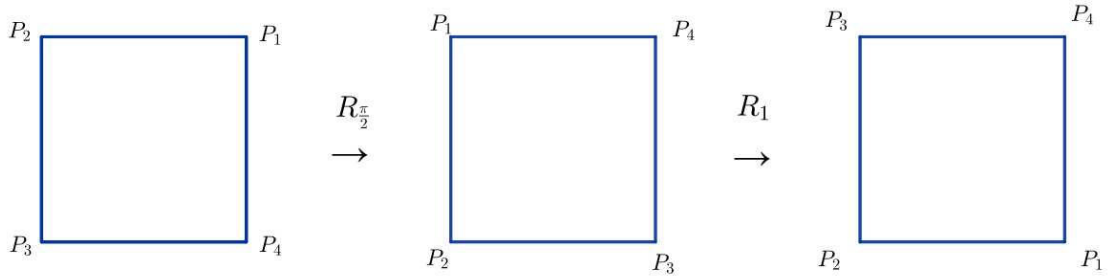
- $Id, R_{\frac{\pi}{2}}, R_{\pi}, R_{\frac{3\pi}{2}}$: são as rotações planas centradas em O, no sentido anti-horário, de ângulos $0, \frac{\pi}{2}, \pi$ e $\frac{3\pi}{2}$, respectivamente.
- R_1, R_2, R_M e R_N: são as rotações espaciais de ângulo π com eixos D_1, D_2, M e N, respectivamente.

Podemos identificar essas transformações como elementos de S_n. Por exemplo, a transformação $R_{\frac{\pi}{2}}$ leva P_1 em P_2, P_2 em P_3, P_3 em P_4 e P_4 em P_1. Essa transformação é isomorfa a permutação (1234). Seguindo esse raciocínio, escrevemos as demais transformações como permutações:

- $Id = Id$;
- $R_{\frac{\pi}{2}} \simeq (1234)$;
- $R_{\pi} \simeq (13)(24)$;
- $R_{\frac{3\pi}{2}} \simeq (1432)$;
- $R_1 \simeq (24)$;
- $R_2 \simeq (13)$;
- $R_M \simeq (12)(34)$;
- $R_N \simeq (14)(23)$;

Ao calcular $R_1 R_{\frac{\pi}{2}}$, em $P_1P_2P_3P_4$, obtemos $P_1 \to P_4$, $P_2 \to P_3$, $P_3 \to P_2$ e $P_4 \to P_1$, como é possível ver na Figura 4.

Figura 4 – Aplicando $R_1 R_{\frac{\pi}{2}}$ em $P_1P_2P_3P_4$



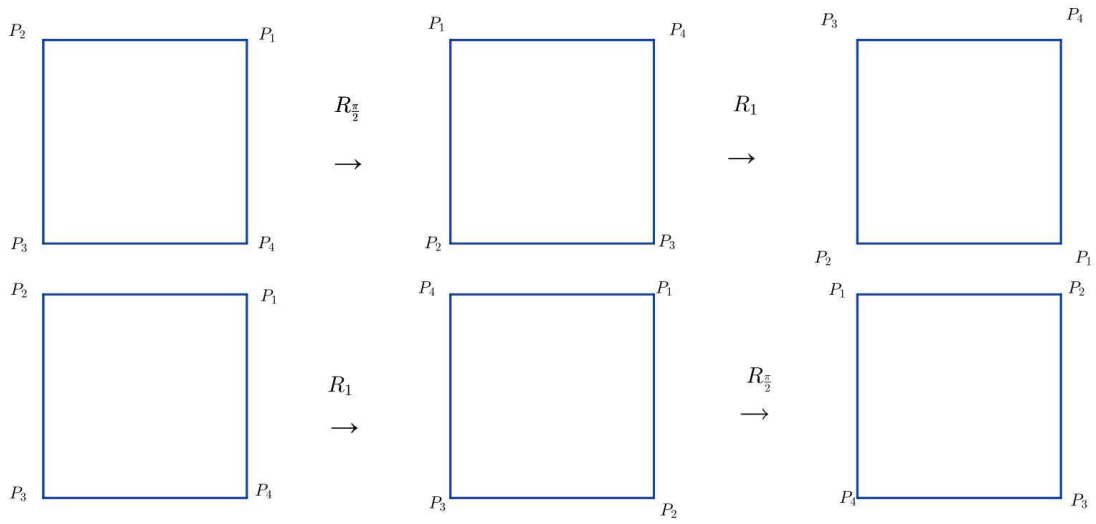
Fonte: Os autores (2021)

Observe que acima, ao aplicar $R_1 R_{\frac{\pi}{2}}$ em $P_1P_2P_3P_4$, nada mais fizemos que compor as permutações $(24)(1234) = (14)(23)$.

Note também que $R_{\frac{\pi}{2}}^4 = Id$, $R_1^2 = R_2^2 = R_M^2 = R_N^2 = Id$, $R_{\frac{\pi}{2}} R_1 = R_M$, $R_{\frac{\pi}{2}}^2 R_1 = R_2$ e $R_{\frac{\pi}{2}}^3 R_1 = R_N$. Portanto $D_4 = \langle R_{\frac{\pi}{2}}, R_1 \rangle$.

Além disso, D_4 é um grupo não abeliano, como podemos ver a seguir:

Figura 5 – Aplicando $R_1 R_{\frac{\pi}{2}}$ e $R_{\frac{\pi}{2}} R_1$ em $P_1P_2P_3P_4$



Fonte: Os autores (2021)

O exemplo anterior será relembrado a posteriori, quando construirmos os grupos de Galois. Mas agora, veremos que também é possível construir funções entre grupos que preservam as operações:

Definição 3.11. *Sejam $(G, *)$ e $(J, \triangle)$ grupos. Uma aplicação $f : G \to J$ é dita um* ***homomorfismo*** *de G em J se*

$$f(x * y) = f(x) \Delta f(y), \quad \forall\, x, y \in G.$$

Se f for uma aplicação bijetora, dizemos que o homomorfismo f é um ***isomorfismo****. Neste caso, $(G, *)$ e $(J, \triangle)$ são grupos isomorfos, e denotamos $G \simeq J$.*

Definição 3.12. *Sejam $f : G \to J$ um homomorfismo de grupos e u o elemento neutro de J. Definimos o* ***núcleo*** *de f, denotado por $Ker(f)$, como sendo o conjunto:*

$$Ker(f) = \{x \in G \mid f(x) = u\}.$$

Através de um grupo G podemos também construir um novo conjunto, que em alguns casos possui estrutura de grupo. Para isso, seja G um grupo e H um subgrupo de G. Definimos a relação $\sim$ definida sobre G por "$a \sim b \Leftrightarrow a^{-1}b \in H$", que é uma relação de equivalência. Assim, a classe de equivalência $\overline{a} = \{b \in G \mid a \sim b\}$ é igual ao conjunto $\{ah \mid h \in H\}$. Essa classe é chamada de classe lateral à direita de a, módulo H. Analogamente a classe de equivalência $Ha = \{ha \mid h \in H\}$ é chamada classe lateral à esquerda de a, módulo H.

Observe que em particular tem-se $H = eH = He$.

Definição 3.13. *Um subgrupo N de um grupo G é chamado* ***subgrupo normal*** *se $\forall\, g \in G$ se verifica a igualdade $gN = Ng$. Ou seja, a classe lateral à esquerda de g em N é igual a classe lateral à direita de g em N, $\forall g \in G$.*

Definição 3.14. *O conjunto quociente de G pela relação $\sim$, denotado por $\frac{G}{H}$ é o conjunto das classes laterais $aH (a \in G)$.*

Esse conjunto determina uma partição de G, pois:

- se $a \in G$, então $aH \neq \varnothing$;
- se $a, b \in G$, então $aH = bH$ ou $aH \cap bH = \varnothing$;
- a união de todas as classes laterais é igual a G.

Como $aH = bH$ ou $aH \neq bH$, vamos tomar $\frac{G}{H}$ como o conjunto de todas as classes laterais distintas. Assim, o número de elementos de $\frac{G}{H}$ é chamado de *índice* de H em G e é denotado por $(G : H)$.

Teorema 3.15. *Se G é grupo e H é um subgrupo normal de G, o conjunto $\frac{G}{H}$ munido com a operação $\cdot : \frac{G}{H} \times \frac{G}{H} \to \frac{G}{H}$ dada por $(aH) \cdot (bH) = (ab)H$ é denominado* ***grupo quociente****.*

Demonstração. Ver [GARCIA A.; IEQUAIN, 2013], p. 155. □

Teorema 3.16. *(Teorema de Lagrange) Seja H um subgrupo de um grupo finito G. Então $o(G) = o(H) \cdot (G : H)$ e portanto $o(H) \mid o(G)$.*

Demonstração. Ver [DOMINGUES; IEZZI, 2003], p. 189. □

Por fim terminaremos essa seção apresentando um teorema muito importante e que nos permite estabelecer algumas relações entre grupos, mesmo que de natureza distintas.

Teorema 3.17. *(Teorema do homomorfismo para grupos) Seja $f : G \to J$ um homomorfismo sobrejetor de grupos. Se $N = Ker(f)$, então $\frac{G}{N} \simeq J$.*

Demonstração. Ver [DOMINGUES; IEZZI, 2003], p. 197. □

3.2 Anéis

Nesta seção, falaremos a respeito da estrutura algébrica anel, assim como alguns resultados e definições importantes para o nosso trabalho.

Definição 3.18. *Um sistema matemático constituído de um conjunto não vazio A e um par de operações sobre A, respectivamente $(x, y) \mapsto x + y$ e $(x, y) \mapsto x \cdot y$ é chamado* ***anel*** *se as seguintes condições são satisfeitas:*

i) $(A, +)$ é grupo abeliano;

ii) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$;

iii) $x \cdot (y + z) = x \cdot y + x \cdot z$ *e* $(x + y) \cdot z = x \cdot z + y \cdot z$; $\forall\, x, y, z \in A$.

Utilizamos a notação $(A, +, \cdot)$ para representar um anel. Se além disso, um anel satisfazer a propriedade:

- $\exists\ 1 \in A$ tal que $\forall\, x \in A$ tem-se $x \cdot 1 = 1 \cdot x = x$, então $(A, +, \cdot)$ é chamado *anel com identidade.*
- Se $\forall\, x, y \in A$ tem-se $x \cdot y = y \cdot x$ então A é chamado *anel comutativo.*
- Se $\forall\, x, y \in A$ temos que $x \cdot y = 0$ implica que $x = 0$ ou $y = 0$ então A é um *anel sem divisores de zero.*

Se $(A, +, \cdot)$ é um anel comutativo com identidade e além disso não possui divisores de zero, então $(A, +, \cdot)$ é chamado **domínio de integridade.**

Se $(A, +, \cdot)$ é um domínio de integridade e além disso, $\forall\, x \in A$, $x \neq 0$, $\exists\ x^{-1} \in A$ tal que $x \cdot x^{-1} = x^{-1} \cdot x = 1$, dizemos que $(A, +, \cdot)$ é um **corpo.**

Exemplo 3.19. *Como já citado no Exemplo 3.4,* $\mathbb{Z}_n$ *também é um exemplo de anel comutativo com identidade.*

Exemplo 3.20. *O conjunto* $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ *é corpo com as operações usuais de* $\mathbb{R}$. *Além disso,* $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}]$, *basta considerar* $b = 0$.

Definição 3.21. *A* ***característica*** *de um domínio de integridade* D *é definida como sendo o menor inteiro positivo* m *tal que* $m \cdot 1 = 0$, *ou seja, a soma de* m *parcelas* 1 *é igual a* 0. *Esta propriedade ocorre para qualquer* $a \in D$, $a \neq 0$. *Caso tal inteiro não exista, dizemos que* A *tem característica 0. Notação:* $charD$.

Nos conjuntos numéricos, o único m que satisfaz $m \cdot a = 0$ $(a \neq 0)$ é $m = 0$, logo a característica dos domínios de integridade $\mathbb{Z}, \mathbb{Q}, \mathbb{Q}[\sqrt{2}], \mathbb{R}$ ou $\mathbb{C}$ é 0. Em especial, qualquer domínio de integridade contido em $\mathbb{C}$ tem característica 0. Já no Exemplo 3.19, quando n é primo, $\mathbb{Z}_n$ tem característica n (observe que se n não for primo, $\mathbb{Z}_n$ não possui estrutura de domínio de integridade e assim a definição não se aplica).

A partir de agora utilizaremos A para denotar um anel $(A, +, \cdot)$.

Definição 3.22. *Sejam* A *um anel e* B *um subconjunto não vazio de* A. *Dizemos que* B *é um* ***subanel*** *de* A *se:*

i) $x, y \in B \Rightarrow x + y \in B$;

ii) $x, y \in B \Rightarrow xy \in B$;

iii) $(B, +, \cdot)$ *é um anel.*

Caso um subanel B de um corpo K for também um corpo, dizemos que B é **subcorpo** de K. Caso queiramos mostrar que B é subcorpo, para não demonstrar todas as propriedades, basta mostrar que $B \neq \varnothing$, para todo $x, y \in B$ tem-se $x - y, xy \in B$ e $\forall\, x \neq 0 \in B$ tem-se $x^{-1} = \frac{1}{x} \in B$.

Além disso, podemos definir um outro subconjunto de um anel:

Definição 3.23. *Um subconjunto $I \neq \varnothing \subseteq A$ é um **ideal** de A se:*

i) $0 \in I$;

ii) $x, y \in I \Rightarrow x + y \in I$;

iii) $\forall\, a \in A$ *e* $\forall\, x \in I$ *tem-se* $ax \in I$ *e* $xa \in I$.

Exemplo 3.24. *O conjunto $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ é ideal de $\mathbb{Z}$.*

Definição 3.25. *Um ideal M de um anel A é dito **maximal** se $M \neq A$ e para todo ideal J tal que*

$$M \subseteq J \subseteq A \Rightarrow J = M \text{ ou } J = A.$$

Exemplo 3.26. *Se $p \in \mathbb{Z}$ é primo, então $p\mathbb{Z}$ é um ideal maximal de $\mathbb{Z}$.*

Definição 3.27. *Seja P um ideal em um anel comutativo A. Diz-se que P é um **ideal primo** se $P \neq A$ e se $ab \in P$ então $a \in P$ ou $b \in P$.*

Como na teoria de grupos, podemos construir funções entre anéis que preservam as operações:

Definição 3.28. *Sejam $(A, +, \cdot)$ e $(B, \oplus, \otimes)$ dois anéis. Uma aplicação $f : A \to B$ é um **homomorfismo de anéis** se:*

i) $f(x + y) = f(x) \oplus f(y),\ \forall\ x, y \in A$;

ii) $f(x \cdot y) = f(x) \otimes f(y),\ \forall\ x, y \in A$.

*Se f for injetora, então f é chamado de **monomorfismo**. Se f for bijetora, então dizemos que f é um **isomorfismo**, e denotamos $A \simeq B$.*

Além disso, os homomorfismos $f : A \to A$ serão chamados de **endomorfismos** e os isomorfismos $f : A \to A$ serão chamados de **automorfismos**.

Definição 3.29. *Seja $f : A \to B$ um homomorfismo de anéis. O **núcleo** de f é:*

$$Ker(f) = \{x \in A \mid f(x) = 0_B\}$$

Da mesma forma que na teoria de grupos, podemos construir conjuntos quocientes. Assim, considere um anel A e um ideal J de A. Definimos a relação de equivalência $x \sim y \Leftrightarrow x - y \in J$. Os elementos do conjunto quociente $A/\sim$ são classes de equivalência da forma $\overline{x} = \{a \in A \mid a \sim x\}$, mas ao denotar $x + J = \{x + j \mid j \in J\}$, obtemos $\overline{x} = x + J$.

No conjunto $\frac{A}{J}$, podemos definir duas operações adição e multiplicação, da seguinte forma:

$$+ : \frac{A}{J} \times \frac{A}{J} \to \frac{A}{J} \qquad \cdot : \frac{A}{J} \times \frac{A}{J} \to \frac{A}{J}$$
$$(x+J)+(y+J) \mapsto (x+y)+J \qquad (x+J)\cdot(y+J) \mapsto (x\cdot y)+J$$

Com as operações acima, $(\frac{A}{J}, +, \cdot)$ é um anel.

Teorema 3.30. *Sejam A um anel comutativo com identidade e J um ideal de A. Então:*

i) $\frac{A}{J}$ é um anel de integridade se e somente se J é um ideal primo.

ii) $\frac{A}{J}$ é corpo se e somente se J é um ideal maximal.

Demonstração. Ver [DOMINGUES; IEZZI, 2003], p. 266. □

Por fim, apresentamos o teorema do homomorfismo para anéis:

Teorema 3.31. *(Teorema do homomorfismo para anéis) Seja $f : A \to B$ um homomorfismo de anéis. Então*

$$\frac{A}{Ker(f)} \simeq Im(f).$$

Demonstração. Ver [DOMINGUES; IEZZI, 2003], p. 267. □

Exemplo 3.32. *Utilizando o teorema do homomorfismo, mostra-se que $\frac{\mathbb{Z}}{n\mathbb{Z}} \simeq \mathbb{Z}_n$.*

3.3 Anel de polinômios

Nesta seção apresentaremos o conjunto de polinômios em uma indeterminada. Esse conjunto é extremamente importante para nossos estudos, e é muito interessante, pois os elementos se comportam de uma maneira muito parecida com os elementos de $\mathbb{Z}$. Assim, apresentaremos definições e propriedades pertinentes a esse conjunto, que serão úteis no decorrer deste trabalho.

Definição 3.33. *Seja A um anel comutativo com identidade. O conjunto dos polinômios com coeficientes em A é definido por:*

$$A[x] = \{a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \mid a_i \in A \, e \, n \in \mathbb{N}\}$$

- Os elementos $a_i \in A$ são chamados *coeficientes*.
- x é a *indeterminada*.

Designaremos que os elementos de $A[x]$ são da forma $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n, n \geq 0$. Além disso, dizemos que dois polinômios $p(x) = a_o + a_1x + a_2x^2 + \ldots + a_nx^n$ e $q(x) = b_0 + b_1x + b_2x^2 \ldots + b_nx^n$ são *iguais* se e somente se $a_i = b_i$ em A, $\forall\, i \in \{1, \ldots, n\}$.

O polinômio identicamente nulo é $p(x) = 0 + 0x + 0x^2 + \ldots + 0x^n = 0$, ou seja, um polinômio $p(x) = a_0 + a_1x + \ldots + a_nx^n$ é identicamente nulo se e só se $a_i = 0$, $\forall\, i \in \{1, \ldots, n\}$.

Também podemos identificar os elementos de A em $A[x]$: basta construir um polinômio $p(x)$ de forma que $a_0 = a$ e $a_i = 0\, \forall\, i \geq 1$. Eles são conhecidos como *polinômios constantes*.

Agora, por meio da construção realizada, podemos construir duas operações de adição e multiplicação em $A[x]$. Para tal, considere $f(x) = a_o + a_1x + \ldots + a_nx^n$ e $g(x) = b_0 + b_1x + \ldots + b_mx^m$. Definimos:

$$+ : A[x] \times A[x] \to A[x] \qquad \cdot : A[x] \times A[x] \to A[x]$$
$$f(x) + g(x) \mapsto (a_0 + b_0) + (a_1 + b_1)x + \ldots \qquad f(x) \cdot g(x) \mapsto c_0 + c_1x + \ldots + c_kx^k + \ldots$$

onde $c_0 = a_0b_0$, $c_1 = a_0b_1 + a_1b_0$, $\ldots$, $c_k = \sum_{i=0}^{k} a_ib_{k-i}$, $k \in \mathbb{N}$.

O conjunto $A[x]$ com as operações definidas acima é um anel comutativo com identidade, chamado **anel dos polinômios sobre A na indeterminada x**.

Observe também que se D é domínio de integridade, $D[x]$ também será. Se K é um corpo, então $K[x]$ será apenas domínio de integridade, visto que nem todos os elementos possuem inverso para a multiplicação.

Definição 3.34. *Se um polinômio $p(x) = a_0 + a_1x + \ldots + a_nx^n$ é tal que $a_n \neq 0$ e $a_j = 0$, $\forall\, j \in \mathbb{N}, j > n$, dizemos que n é o **grau** do polinômio $p(x)$, e representamos por $\partial p(x) = n$ ou $\partial p = n$. Além disso, o elemento a_n é chamado de **coeficiente líder** de $p(x)$. Se $a_n = 1$ dizemos que $p(x)$ é um polinômio mônico.*

A função grau possui algumas propriedades interessantes:

Teorema 3.35. *Sejam D um domínio de integridade e $f(x), g(x) \in D[x]$. Então:*

a) $\partial(f + g) \leq max\{\partial f, \partial g\}$;

b) $\partial(f \cdot g) = \partial f + \partial g$.

Demonstração. Ver [GONÇALVES, 2012], p. 64. □

Podemos observar também que os polinômios com grau maior ou igual a 1 não possuem inverso. Dessa forma, os únicos elementos inversíveis de $A[x]$ são os elementos inversíveis em A.

Lembra-se quando havíamos comentado que o anel de polinômios é semelhante a $\mathbb{Z}$? De fato, se os coeficientes pertencerem a um corpo K, teremos resultados muitos semelhantes em ambos os conjuntos. O próximo teorema exemplifica essa questão.

Teorema 3.36. *(Algoritmo da divisão): Sejam $f(x), g(x) \in K[x]$ e $g(x) \neq 0$. Então existem únicos $q(x), r(x) \in K[x]$ tais que:*

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

onde $r(x) = 0$ ou $\partial r < \partial g$. Os polinômios $q(x)$ e $r(x)$ são chamados quociente e resto da divisão, respectivamente.

Demonstração. Ver [GONÇALVES, 2012], p. 67. □

Definição 3.37. *Sejam $f, g \in K[x]$, dizemos que f divide g e denotamos por $f \mid g$ se existir um polinômio $h \in K[x]$ tal que $g = fh$. Neste caso, dizemos que f é divisor de g ou que g é divisível por f.*

*i) Um elemento $a \in K$ é uma **raiz** ou um zero de f se $f(a) = 0$.*

ii) Dizemos que a é uma raiz de multiplicidade k se $(x-a)^k \mid f$ mas $(x-a)^{k+1} \nmid f$. Se $k = 1$, então a é uma raiz simples de f.

Corolário 3.38. *Sejam K um corpo e $a \in K$. Então a é uma raiz de f se e somente se $(x-a)$ divide f.*

O seguinte teorema nos apresenta o número máximo de raízes de um polinômio:

Teorema 3.39. *Seja K um corpo e seja $f(x) = a_0 + a_1x + \ldots + a_nx^n$ um polinômio não nulo em $K[x]$ de grau n. Então o número de raízes de f em K é no máximo n.*

Demonstração. Ver [GONÇALVES, 2012], p. 68. □

Outros resultados que apresentam uma semelhança do $K[x]$ com $\mathbb{Z}$ são:

Teorema 3.40. *Todo ideal de $K[x]$ é principal, ou seja, é gerado por um polinômio $p(x) \in K[x]$. Assim, se J é um ideal de $K[x]$, $J = K[x]p(x) = \{f(x)p(x) \mid f(x) \in K[x]\}$.*

Demonstração. Ver [GONÇALVES, 2012], p. 72. □

Agora, apresentaremos uma definição importante para nossos estudos, que nos acompanhará até o fim deste trabalho.

Definição 3.41. *Seja $f(x) \in K[x]$ tal que $\partial f \geq 1$. Dizemos que f é um **polinômio irredutível** sobre K se toda vez que $f(x) = g(x) \cdot h(x)$, $g(x), h(x) \in K[x]$ temos $g(x) = a$ constante em K ou $h(x) = b$ constante em K. Se $f(x)$ não for irredutível sobre K dizemos que $f(x)$ é redutível sobre K.*

Observe por exemplo que o polinômio $p(x) = x^2 + 1$ sobre $K = \mathbb{R}$ é irredutível. Porém, sobre $K = \mathbb{C}$, temos que $p(x)$ é redutível, visto que pode ser escrito como $p(x) = (x + i)(x - i)$.

Teorema 3.42. *(Teorema da fatoração única) Seja K um corpo. Então todo polinômio $f(x) \in K[x] - \{0\}$ pode ser escrito na forma $f(x) = u \cdot p_1(x) \cdot \ldots \cdot p_m(x)$, onde $u \in K - \{0\}$ e $p_1(x), \ldots, p_m(x) \in K[x]$ são polinômios irredutíveis sobre K (não necessariamente distintos). Mas ainda, essa expressão é única a menos da constante u e da ordem dos polinômios $p_1(x), \ldots, p_m(x)$.*

Demonstração. Ver [GONÇALVES, 2012], p. 80. □

Como veremos adiante, nem sempre é fácil afirmar se determinado polinômio é irredutível ou não. Portanto, o seguinte resultado nos auxilia nesse aspecto:

Teorema 3.43. *Seja K um corpo e $p(x) \in K[x]$. Então as seguintes condições são equivalentes:*

i) $p(x)$ *é irredutível sobre* K*;*

ii) $J = K(x) \cdot p(x)$ *é um ideal maximal em* $K[x]$*;*

iii) $\dfrac{K[x]}{J}$ *é um corpo, onde* $J = K[x] \cdot p(x)$*.*

Demonstração. Ver [GONÇALVES, 2012], p. 76. □

Porém utilizar o teorema acima nem sempre é fácil, e como determinar a irredutibilidade de polinômios também não é uma tarefa simples, vamos apresentar um critério que nos auxilia em determinadas situações:

Teorema 3.44. *(Critério de Eisenstein) Seja $f(x) = a_0 + a_1x + \ldots + a_nx^n$ um polinômio em $\mathbb{Z}[x]$. Suponhamos que exista um inteiro primo p tal que:*

i) $p \nmid a_n$*;*

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

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

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

Demonstração. Ver [GONÇALVES, 2012], p. 83. □

Considere, por exemplo, o polinômio $f(x) = x^4 + 10x^3 + 20x^2 + 30x + 22$. Basta tomar $p = 2$ e aplicar o Critério de Eisenstein, assim podemos concluir que $f(x)$ é irredutível sobre $\mathbb{Q}$ (observe que não podemos garantir nada em relação a $\mathbb{R}$).

Teorema 3.45. *(Irredutibilidade mod p) Sejam* $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$ *e* $p \in \mathbb{Z}$ *primo tal que* $p \nmid a_n$. *Defina* $\overline{f}(x) = \overline{a_0} + \overline{a_1}x + \ldots + \overline{a_n}x^n \in \mathbb{Z}_p[x]$. *Se* $\overline{f}(x)$ *é irredutível sobre* $\mathbb{Z}_p[x]$ *então* $f(x)$ *é irredutível sobre* $\mathbb{Q}$.

Seja $f(x) = x^3 + 6x^2 + 5x + 25 \in \mathbb{R}[x]$. Se $p = 2$, teremos $\overline{f}(x) = \overline{1}x^3 + \overline{1}x + \overline{1} \in \mathbb{Z}_2[x]$. Agora, basta verificar se $\overline{f}(x)$ possui raízes em $\mathbb{Z}_2$. Temos $\overline{f}(0) = \overline{1}$ e $\overline{f}(1) = \overline{1}$. Portanto, como $\overline{f}$ é irredutível em $\mathbb{Z}_2[x]$ segue que $f(x)$ é irredutível sobre $\mathbb{Q}$.

4 Extensões de corpos

Durante o ensino fundamental e médio, normalmente conhecemos apenas alguns conjuntos numéricos, como $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$. Durante a graduação, ao estudar as estruturas algébricas, nos deparamos com outros exemplos, como os corpos finitos. Mas, você sabia que existem muitos outros conjuntos "perdidos" por aí? Eles são muito especiais, pois têm estrutura de corpo. Neste capítulo apresentaremos tais conjuntos, revelando um novo mundo de exemplos que esteve escondido até agora.

Definição 4.1. *Uma* ***extensão de corpos*** *é um monomorfismo $i : K \to L$ onde K e L são corpos. Dizemos que K é o corpo menor e L é o corpo maior.*

Podemos representar extensões de corpos utilizando diagramas. Assim, o diagrama referente a definição acima pode ser representado por:

$$\begin{array}{c} L \\ {\scriptstyle i}\big| \\ K \end{array}$$

De uma forma mais simples, dizemos que $L \supseteq K$ é uma *extensão de K* se L e K possuem estrutura de corpo. Vamos apresentar alguns exemplos:

Exemplo 4.2. *Considere $K = \mathbb{R}$ e $L = \mathbb{C}$. Como $\mathbb{C} \supseteq \mathbb{R}$ segue que $\mathbb{C}$ é uma extensão de corpos de $\mathbb{R}$.*

Exemplo 4.3. *Sabemos que $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ é uma extensão de corpos de $\mathbb{Q}$, visto que podemos "enxergar" $\mathbb{Q}$ submerso em $\mathbb{Q}[\sqrt{2}]$, basta construir o monomorfismo $i : \mathbb{Q} \to \mathbb{Q}[\sqrt{2}]$ tal que $i(a) = a$ (consideramos a função inclusão).*

No decorrer deste trabalho identificaremos K como a imagem $i(K) \subseteq L$, já que a função $i : K \to i(K)$ é um isomorfismo. Neste caso, dizemos que L é uma extensão de K e denotaremos $L : K$.

Dado um subconjunto de $\mathbb{C}$, podemos construir extensões de corpos, como apresentamos na seguinte definição:

Definição 4.4. *Seja X um subconjunto de $\mathbb{C}$. Então o subcorpo de $\mathbb{C}$ gerado por X é a intersecção de todos os subcorpos de $\mathbb{C}$ que contém X. Em outras palavras é o menor subcorpo de $\mathbb{C}$ que contém X.*

Como consequência da definição acima, podemos exibir o seguinte resultado:

Proposição 4.5. *Todo subcorpo K de $\mathbb{C}$ contém $\mathbb{Q}$.*

Demonstração. Como K é subcorpo de $\mathbb{C}$, sabemos que K é fechado para a soma e multiplicação, e além disso, K possui estrutura de corpo. Então já sabemos que $0, 1 \in K$, o que garante que $K \neq \varnothing$. Além disso, como K possui uma operação de adição e é fechado para ela, sabemos que $1 + 1 + \ldots + 1 = n \in K$, $\forall\, n > 0$. E como todo elemento possui inverso, $-n \in K$. Dessa forma obtemos $\mathbb{Z} \subseteq K$. Mas K também possui uma operação de multiplicação, portanto $p \cdot q \in K$, $\forall\, p, q \in K$. Além disso, como K possui estrutura de corpo, $\forall\, p \in K, p \neq 0$, $\exists\, p^{-1} \in K$ tal que $p \cdot p^{-1} = p^{-1} \cdot p = 1$. E como essa operação é fechada podemos concluir que $p \cdot q^{-1} \in K$. Portanto $K \supseteq \mathbb{Q}$, como queríamos. □

Definição 4.6. *Se $L : K$ é uma extensão de corpos e Y é um subconjunto qualquer de L, o subcorpo de $\mathbb{C}$ gerado por $K \cup Y$ é representado por $K(Y)$ e é dito ser obtido de K adjuntando Y.*

A partir dessa definição utilizaremos a notação $K(\alpha)$ para representar o corpo K adjuntado por α, e se $Y = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ denotaremos $K(Y)$ por $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Exemplo 4.7. *Se $X = \varnothing$, então $\mathbb{Q}(X) = \mathbb{Q}$. De fato, pela Proposição 4.5, sabemos que $\mathbb{Q}(X) \supseteq \mathbb{Q}$. Porém como $X = \varnothing$, o menor subcorpo de $\mathbb{C}$ que contém X é o próprio $\mathbb{Q}$. Portanto $\mathbb{Q}(X) = \mathbb{Q}$.*

Uma observação importante que merece destaque é que se $\alpha_1 \in K(\alpha)$, então $K(\alpha, \alpha_1) = K(\alpha)(\alpha_1) = K(\alpha)$. Em outras palavras, adjuntar um elemento que já pertence a extensão, não altera a extensão.

Exemplo 4.8. *O conjunto $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ é o subcorpo de $\mathbb{C}$ obtido de $\mathbb{Q}$ adjuntando $\sqrt{2}$. Em especial, $\mathbb{Q}[\sqrt{2}] \simeq \mathbb{Q}(\sqrt{2})$, visto que $\mathbb{Q}[\sqrt{2}]$ possui estrutura de corpo, como comentado no Exemplo 3.20.*

Demonstração. Seja $(L_\lambda)_{\lambda \in \Delta}$ a família de subcorpos L_λ tais que cada L_λ contém $\mathbb{Q} \cup \{\sqrt{2}\}$. Vamos mostrar que $\mathbb{Q}[\sqrt{2}]$ é igual a intersecção $\bigcap\limits_{\lambda \in \Delta} L_\lambda$.

Como $\sqrt{2} \in L_\lambda\ \forall\, \lambda \in \Delta$ podemos concluir que $\sqrt{2} \in \bigcap\limits_{\lambda \in \Delta} L_\lambda$. Além disso, como $\mathbb{Q} \subseteq L_\lambda\ \forall\ \lambda \in \Delta$, podemos concluir que $\mathbb{Q} \subseteq \bigcap\limits_{\lambda \in \Delta} L_\lambda$ e portanto $1 \in \bigcap\limits_{\lambda \in \Delta} L_\lambda$. Como $\bigcap\limits_{\lambda \in \Delta} L_\lambda \supseteq \{1, \sqrt{2}\}$, segue que todos os elementos da forma $a \cdot 1 + b\sqrt{2}, a, b \in \mathbb{Q}$ estão em $\bigcap\limits_{\lambda \in \Delta} L_\lambda$, já que são gerados por 1 e $\sqrt{2}$. Dessa forma $\mathbb{Q}[\sqrt{2}] \subseteq \bigcap\limits_{\lambda \in \Delta} L_\lambda$.

Por outro lado, como $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}]$ e $\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, temos $\mathbb{Q}[\sqrt{2}] \supseteq \mathbb{Q} \cup \{\sqrt{2}\}$, portanto $\mathbb{Q}[\sqrt{2}]$ pertence a família $(L_\lambda)_{\lambda \in \Delta}$. E como $\bigcap\limits_{\lambda \in \Delta} L_\lambda \subseteq L_\lambda\ \forall\ \lambda \in \Delta$, podemos concluir que $\bigcap\limits_{\lambda \in \Delta} L_\lambda \subseteq \mathbb{Q}[\sqrt{2}]$.

Portanto como $\mathbb{Q}[\sqrt{2}] \subseteq \bigcap\limits_{\lambda \in \Delta} L_\lambda$ e $\bigcap\limits_{\lambda \in \Delta} L_\lambda \subseteq \mathbb{Q}[\sqrt{2}]$ segue que $\bigcap\limits_{\lambda \in \Delta} L_\lambda = \mathbb{Q}[\sqrt{2}]$. □

Exemplo 4.9. *$L = \mathbb{Q}[i, \sqrt{5}]$ é o subcorpo gerado por $\mathbb{Q} \cup \{i, \sqrt{5}\}$.*

Demonstração. Novamente, pela Proposição 4.5, sabemos que $L = \mathbb{Q}(i, \sqrt{5}) \supseteq \mathbb{Q}$. Além do mais, $i, \sqrt{5} \in L$. Mas como L possui estrutura de corpo, é fechado para a multiplicação, assim $i\sqrt{5} \in L$ também. Portanto, podemos deduzir que os elementos de L são da forma $\alpha = a + bi + c\sqrt{5} + di\sqrt{5}$, $a, b, c, d \in \mathbb{Q}$. Agora, resta verificar se L é um subcorpo de $\mathbb{C}$. Dados $\alpha_1 = a + bi + c\sqrt{5} + di\sqrt{5}$ e $\alpha_2 = a' + b'i + c'\sqrt{5} + d'i\sqrt{5} \in L$, temos: $\alpha_1 + \alpha_2 = (a+a') + (b+b')i + (c+c')\sqrt{5} + (d+d')i\sqrt{5} \in L$. E $\alpha_1 \cdot \alpha_2 = (aa' - bb' + 5cc' - 5dd') + (ab' + ba' + 5cd' + 5dc')i + (ac' - bd' + ca' - bd')\sqrt{5} + (ad' + bc' + cb' + da')i\sqrt{5} \in L$. Agora, resta verificar se $\forall\, \alpha \neq 0 \in L$, $\exists\, \alpha^{-1} \in L$ tal que $\alpha \cdot \alpha^{-1} = \alpha^{-1} \cdot \alpha = 1$. Assim, vamos escrever $\alpha = a + bi + c\sqrt{5} + di\sqrt{5}$ da seguinte forma: $\alpha = x + y\sqrt{5}$, em que $x = a + bi$ e $y = c + di$. Vamos considerar M o subconjunto de L que contém todos os elementos da forma $p + qi$, portanto $x, y \in M$. Agora, considere $\beta = a + bi - c\sqrt{5} - di\sqrt{5} = x - y\sqrt{5} \in L$. Então $\alpha \cdot \beta = (x + y\sqrt{5})(x - y\sqrt{5}) = x^2 - 5y^2 = z$, em que $z \in M$. Como $\alpha \neq 0$. segue que $\beta \neq 0$ e, portanto, $z \neq 0$. Assim $\alpha \cdot \beta = z \Rightarrow (\alpha \cdot \beta)^{-1} = z^{-1} \Rightarrow \beta^{-1} \cdot \alpha^{-1} = z^{-1} \Rightarrow \alpha^{-1} = \beta \cdot z^{-1}$. Como $z \in M$, $z = u + vi$, $u, v \in \mathbb{Q}$. Agora, considere $w = u - vi \in M$. Assim $zw = (u + vi)(u - vi) = u^2 + v^2 \in \mathbb{Q}$ e teremos: $z^{-1} = \dfrac{u - vi}{u^2 + v^2} \in M$. Como $M \subseteq L$, segue que $z^{-1} \in L$, portanto $\alpha^{-1} = \beta \cdot z^{-1} \in L$. Logo L é um subcorpo de $\mathbb{C}$ que é gerado por $\mathbb{Q} \cup \{i, \sqrt{5}\}$. □

Exemplo 4.10. *O conjunto $\mathbb{Q}[\sqrt[3]{2}, u]$ é o subcorpo de $\mathbb{C}$ gerado por $\mathbb{Q} \cup \{\sqrt[3]{2}, u\}$, em que $u = \dfrac{-1}{2} + \dfrac{\sqrt{3}}{2}i$ (a raiz cúbica da unidade).*

Daremos um enfoque maior neste exemplo no decorrer deste capítulo. Agora, vamos a uma definição importante.

Definição 4.11. *Uma extensão de corpos $L : K$ é uma **extensão simples** se existe $\alpha \in L$ tal que $L = K(\alpha)$.*

Por meio do Exemplo 4.8 vemos que a extensão $\mathbb{Q}[\sqrt{2}]$ é simples. Além disso, temos alguns outros exemplos:

Exemplo 4.12. *$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$ é uma extensão simples, já que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.*

Demonstração. Como $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ é subcorpo de $\mathbb{C}$, é fechado para a operação, desta forma $\sqrt{2} + \sqrt{3} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, o que nos fornece $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Assim, resta mostrar que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$, ou equivalentemente, $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Como $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, e $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ é fechado para a operação multiplicação, temos que $(\sqrt{2} + \sqrt{3})^2 = 2 + 2\sqrt{2} \cdot \sqrt{3} + 3 = 5 + 2\sqrt{6} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, o que implica que $\sqrt{6} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Mas $\sqrt{6} \cdot (\sqrt{2} + \sqrt{3}) \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ implica que $2\sqrt{3} + 3\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Assim, $(2\sqrt{3} + 3\sqrt{2}) - 2(\sqrt{2} + \sqrt{3}) \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, donde segue que $\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. E $-(2\sqrt{3} + 3\sqrt{2}) + 3(\sqrt{2} + \sqrt{3}) \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, logo $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Como $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ e $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ é o menor corpo que contém $\mathbb{Q} \cup \{\sqrt{2}, \sqrt{3}\}$ então $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Assim concluímos que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. □

Exemplo 4.13. *A extensão $L = \mathbb{Q}(i, \sqrt{5})$ apresentada no Exemplo 4.9 também é uma extensão simples, obtida por meio de $\mathbb{Q} \cup \{i + \sqrt{5}\}$.*

Demonstração. A demonstração é análoga a anterior. □

Exemplo 4.14. *A extensão $\mathbb{R} : \mathbb{Q}$ não é uma extensão simples.*

Por enquanto vamos apenas apresentar esse exemplo. No decorrer deste trabalho, após apresentar outros conceitos que facilitarão a compreensão da afirmação acima, comentaremos mais a respeito.

Definição 4.15. *Um **isomorfismo** entre duas extensões de corpos $i : K \to K'$, $j : L \to L'$ é um par (λ, μ) de isomorfismos $\lambda : K \to L$, $\mu : K' \to L'$ tal que, $\forall\, k \in K$ tem-se $j(\lambda(k)) = \mu(i(k))$.*

Equivalentemente, dizemos que o diagrama abaixo comuta.

$$\begin{array}{ccc} K & \xrightarrow{\ i\ } & K' \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\mu} \\ L & \xrightarrow[\ j\ ]{} & L' \end{array}$$

Exemplo 4.16. *As extensões $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{3})$ não são isomorfas (considerando isomorfismo entre extensões de corpos).*

Primeiro, observe que qualquer isomorfismo entre duas extensões de corpos (em característica 0) fixa $\mathbb{Q}$, visto que 1 é mapeado em 1 e $\mathbb{Q}$ está contido em qualquer subcorpo de $\mathbb{C}$.

Agora, suponha que existe um isomorfismo $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$. Assim, existem $a, b \in \mathbb{Q}$ tais que $\phi(\sqrt{2}) = a + b\sqrt{3}$. Como ϕ é homomorfismo, temos:

$$\begin{aligned} 2 &= \phi(2) \\ &= \phi((\sqrt{2})^2) \\ &= (\phi(\sqrt{2}))^2 \\ &= (a + b\sqrt{3})^2 \\ &= a^2 + 3b^2 + 2ab\sqrt{3} \end{aligned}$$

Logo:

$$\begin{cases} 2 = a^2 + 3b^2 \\ 2ab = 0 \end{cases}$$

Se $a = 0$, então $b = \pm\sqrt{\dfrac{2}{3}} \notin \mathbb{Q}$. Se $b = 0$ então $a = \pm\sqrt{2} \notin \mathbb{Q}$. Contradição em ambos os casos. Portanto as extensões $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{3})$ não são isomorfas, considerando isomorfismo entre extensões de corpos.

Definição 4.17. *Seja $L : K$ uma extensão finita. Se M é um subcorpo de L que contém K, ou seja, $K \subseteq M \subseteq L$, então M é chamado **corpo intermediário** de $L : K$.*

4.1 Extensões algébricas e transcendentes

Nesta seção introduziremos uma nova forma de estudar extensões de corpos: podemos associar às extensões o conjunto de polinômios, que estão intimamente ligados aos elementos dessa extensão. A partir desse ponto as coisas começam a ficar mais divertidas, e esse é só o começo.

Definição 4.18. *Seja K um subcorpo de $\mathbb{C}$ e seja $\alpha \in \mathbb{C}$. Dizemos que α é **algébrico** sobre K se existe um polinômio $f(x) \in K[x]$ não nulo tal que $f(\alpha) = 0$. Caso não exista nenhum polinômio que satisfaz tais condições, dizemos que α é **transcendente** sobre K.*

Como exemplo considere $\alpha = \sqrt[3]{2}$, que é algébrico sobre $\mathbb{Q}$, visto que é raiz do polinômio $x^3 - 2$. Ao escolher $\alpha = \pi$ sobre $\mathbb{Q}$, não encontramos um polinômio com coeficientes em $\mathbb{Q}$ no qual π seja raiz. Por esse motivo, π é transcendente sobre $\mathbb{Q}$. Porém, se considerarmos $\mathbb{Q}(\pi)$, π é um elemento algébrico sobre $\mathbb{Q}(\pi)$, já que é raiz do polinômio $x - \pi$. Observe que nesse exemplo $\pi \in \mathbb{Q}(\pi)$. Assim, podemos fazer a seguinte observação:

Observação 4.19. *Se $\alpha \in K$, então α é algébrico sobre K, pois é raiz do polinômio $f(x) = x - \alpha \in K[x]$.*

Definição 4.20. *Se para todo $\alpha \in L \supseteq K$, α é algébrico sobre K, então a extensão $L : K$ diz-se uma **extensão algébrica**.*

Além disso, se α é algébrico sobre K, dizemos que $K(\alpha)$ é uma *extensão algébrica simples*. Caso α seja transcendente, dizemos que $K(\alpha)$ é uma *extensão transcendente simples*.

Podemos nos questionar agora em relação a existência de polinômios cujo α seja raiz. O próximo teorema nos auxilia a compreender melhor essa questão:

Teorema 4.21. *Seja $\alpha \in L$ algébrico sobre K. Então existe um único polinômio mônico não nulo de menor grau sobre $K[x]$ tal que α é raiz.*

Demonstração. Seja α um elemento algébrico sobre K, assim existe $f(x) \in K[x]$ tal que $f(\alpha) = 0$. Queremos mostrar que existe um único polinômio mônico de menor grau $m(x) \in K[x]$ tal que $m(\alpha) = 0$.

Se $f(x)$ for mônico, a existência de um polinômio mônico cujo α é raiz já está garantida. Se $f(x)$ não for mônico, seja a_n seu coeficiente líder. Assim, considere o polinômio $g(x) = \dfrac{f(x)}{a_n}$. Dessa forma $g(x)$ é mônico e como $f(\alpha) = 0$ segue que $g(\alpha) = 0$.

Agora, vamos mostrar que existe um polinômio mônico de menor grau. Seja Z o conjunto de todos os polinômios mônicos tais que α é raiz. Como já vimos, $Z \neq \varnothing$. Assim, pelo Princípio da Boa Ordem (aplicado aos graus dos polinômios em Z, que são números naturais), existe $m(x) \in K[x]$ um polinômio mônico de menor grau tal que α é raiz. Agora, vamos mostrar que ele é único. Suponha que exista $h(x)$ mônico tal que $h(\alpha) = 0$ e $\partial h = \partial m$. Mas assim teríamos $h(\alpha) - m(\alpha) = 0 \Rightarrow (h - m)(\alpha) = 0$, e se $h \neq m$ obtemos $h - m$ polinômio mônico com grau menor que $m(x)$ tal que α é raiz. Absurdo. Portanto $h(x) = m(x)$. □

Definição 4.22. *Seja $\alpha \in L$ algébrico sobre K. O **polinômio minimal** de α sobre K é o polinômio mônico de menor grau tal que α é raiz. Tal polinômio será denotado por $m_\alpha(x)$.*

Como exemplo temos $m_{\sqrt{2}}(x) = x^2 - 2$. De fato, $m_{\sqrt{2}}(\sqrt{2}) = (\sqrt{2})^2 - 2 = 0$ e seu coeficiente líder é 1, logo $m_{\sqrt{2}}(x)$ é mônico. Além disso, $m_{\sqrt{2}}(x)$ é o polinômio de menor grau que satisfaz tais propriedades. De fato, os únicos polinômios de grau menor que $m_{\sqrt{2}}(x)$ são da forma $f(x) = x + r$, em que $r \in \mathbb{Q}$. Mas neste caso, para que $\sqrt{2}$ seja raiz de $f(x)$, teríamos $r = -\sqrt{2} \in \mathbb{Q}$. Absurdo.

Outro exemplo interessante é analisar o polinômio minimal de $\alpha = i$ sobre uma extensão qualquer $K(i) : K$ (desde que $i \notin K$). Como i é raiz de $m(x) = x^2 + 1$ e $m(x)$ é mônico, basta verificar que este é o polinômio mônico de menor grau tal que i é raiz.

Vejamos que os polinômios de grau menor são da forma $f(x) = x+a$ ou são polinômios constantes. Observe que se $f(i) = 0$ então $a = -i \in K$. Absurdo. E se $f(x) = c \neq 0 \in K[x]$ é um polinômio constante, temos $f(i) = c \neq 0$. Logo em ambos os casos i não é raiz de $f(x)$, dessa forma $m(x)$ é o polinômio minimal de i em relação a $K(i) : K$.

Portanto temos que $m(x)$ é o polinômio minimal da extensão $\mathbb{Q}(i) : \mathbb{Q}$, $\mathbb{R}(i) : \mathbb{R}$ ou $\mathbb{Q}(\sqrt{5}, i) : \mathbb{Q}(\sqrt{5})$, por exemplo. Observe que extensões diferentes podem ter o mesmo polinômio minimal associado.

Teorema 4.23. *Se α é algébrico sobre K, então o polinômio minimal de α sobre K é irredutível sobre K. Ele divide todo polinômio que tem α como raiz.*

Demonstração. Suponha por absurdo que $m_\alpha(x)$ é redutível, assim existem $f(x), g(x) \in K[x]$ tais que $m_\alpha(x) = f(x) \cdot g(x)$, com $\partial f < \partial m_\alpha$ e $\partial g < \partial m_\alpha$. Como $m_\alpha(\alpha) = 0$, temos $f(\alpha) \cdot g(\alpha) = 0$. Mas $f(\alpha), g(\alpha) \in L$ e L é corpo, logo $f(\alpha) = 0$ ou $g(\alpha) = 0$. Se $f(\alpha) = 0$, $f(x)$ é um polinômio com grau menor que m_α cujo α é raiz, o que contraria a minimalidade do grau de m_α. Se $g(\alpha) = 0$, o raciocínio é análogo. Portanto $m_\alpha(x)$ é irredutível.

Agora, seja $p(x) \in K[x]$ um polinômio tal que $p(\alpha) = 0$. Pelo algoritmo da divisão, sabemos que existe $q(x), r(x) \in K[x]$ tais que $p(x) = q(x) \cdot m_\alpha(x) + r(x)$, com $\partial r < \partial m_\alpha$ ou $r(x) = 0$. Assim, $p(\alpha) = q(\alpha) \cdot m_\alpha(\alpha) + r(\alpha)$ implica que $0 = q(\alpha) \cdot 0 + r(\alpha)$, o que nos dá $r(\alpha) = 0$. Como $m_\alpha(x)$ é o polinômio de menor grau tal que α é raiz, concluímos que $r(x) = 0$ e portanto $m_\alpha(x) \mid p(x)$. □

Corolário 4.24. *O conjunto $I = \{p(x) \in K[x] \mid p(\alpha) = 0\}$ é um ideal de $K[x]$, gerado por $m_\alpha(x)$.*

Anteriormente, havíamos definido $K(\alpha)$ como o menor corpo obtido de K adjuntando α. Mas podemos definir o conjunto $K[\alpha]$, utilizando colchetes, cujos elementos serão vistos como imagens de polinômios, como pode ser observado na definição abaixo.

Definição 4.25. *Sejam $L : K$ uma extensão de corpos e $\alpha \in L$. Definimos $K[\alpha] := \{f(\alpha) \mid f(x) \in K[x]\}$.*

Com essa notação, $K[\alpha]$ é um subanel de $\mathbb{C}$, que terá a estrutura de corpo quando α for algébrico sobre K. Ou seja, se α é algébrico sobre K, temos $K[\alpha] = K(\alpha)$.

Além disso, interpretar $K[\alpha]$ dessa forma é muito interessante, pois permite relacionar a teoria de anéis de polinômios com extensões de corpos, como pode ser observado no próximo teorema:

Teorema 4.26. *Se $\alpha \in L \supseteq K$ e se $\phi : K[x] \to L$ é definida por $\phi(f(x)) = f(\alpha)$, então ϕ é um homomorfismo tal que:*

i) $Im(\phi) = K[\alpha]$, $K \subseteq K[\alpha] \subseteq L$;

ii) α *é transcendente sobre* K *se e somente se* $Ker(\phi) = \{0\}$, *em que* $0 \in K[x]$ *é o polinômio identicamente nulo.*

iii) Se α *é algébrico sobre* K *então* $Ker(\phi) = K[x] \cdot m_\alpha(x)$ *é um ideal maximal de* $K[x]$;

iv) $\dfrac{K[x]}{Ker(\phi)} \simeq K[\alpha]$.

Demonstração. i) Seja $a \in Im(\phi)$, assim $a = f(\alpha)$ para algum $f(x) \in K[x]$. Mas como $K[\alpha] = \{f(\alpha) \mid f(x) \in K[x]\}$ segue que $f(\alpha) = a \in K[\alpha]$. Agora, seja $a \in K[\alpha]$, assim $a = f(\alpha)$ para algum $f(x) \in K[x]$. Porém $f(\alpha) = \phi(f(x))$, logo $a = f(\alpha) = \phi(f(x)) \in Im(\phi)$. Portanto concluímos que $Im(\phi) = K[\alpha]$. Observe que $K[\alpha] \supseteq K$ visto que $c(\alpha) = c$ para todo polinômio constante $c \in K[x]$. Além disso, $K[\alpha] = Im(\phi) \subseteq L$.

ii) Se α é transcendente sobre K, não existe polinômio $f(x) \in K[x] - \{0\}$ tal que $f(\alpha) = 0$. Logo $f(\alpha) = 0$ implica que $f(x) = 0$, assim $Ker(\phi) = \{f(x) \in K[x] \mid f(\alpha) = 0\} = \{f(x) \mid f(x) = 0\} = \{0\}$. Reciprocamente, Se $Ker(\phi) = \{0\}$ segue que $f(\alpha) = 0$ somente quando $f(x) = 0$, então $f(\alpha) \neq 0 \, \forall \, f(x) \in K[x] - \{0\}$, portanto α é transcendente sobre K.

iii) Sejam α algébrico sobre K e $m_\alpha(x)$ o polinômio minimal de α. Seja $f(x) \in K[x] - \{0\}$ tal que $f(\alpha) = 0$, logo $f(x) \in Ker(\phi)$. Vamos mostrar que $m_\alpha(x) \mid f(x)$. Como $\partial m_\alpha < \partial f$, pelo algoritmo da divisão existem $q(x), r(x) \in K[x]$ tais que $f(x) = q(x) \cdot m_\alpha(x) + r(x)$, com $\partial r < \partial m_\alpha$ ou $r(x) = 0$. Assim $f(\alpha) = q(\alpha) \cdot m_\alpha(\alpha) + r(\alpha) \Rightarrow 0 = q(\alpha) \cdot 0 + r(\alpha) \Rightarrow r(\alpha) = 0$. Mas $m_\alpha(x)$ é o polinômio de menor grau tal que α é raiz, assim concluímos que $r(x) = 0$ e dessa forma $m_\alpha(x) \mid f(x)$. Portanto $f(x) = q(x) \cdot m_\alpha(x) \in K[x] \cdot m_\alpha(x)$. Por outro lado, seja $f(x) \in K[x] \cdot m_\alpha(x)$, assim existe $q(x) \in K[x]$ tal que $f(x) = q(x) \cdot m_\alpha(x)$. Como $m_\alpha(\alpha) = 0$, temos $f(\alpha) = q(\alpha) \cdot m_\alpha(\alpha) = q(\alpha) \cdot 0 = 0 \Rightarrow f(x) \in Ker(\phi)$.

Agora, afirmamos que $Ker(\phi) = K[x] \cdot m_\alpha(x)$ é um ideal maximal de $K[x]$. De fato, como $m_\alpha(x)$, é irredutível, segue pelo Teorema 3.43 que $Ker(\phi) = K[x] \cdot m_\alpha(x)$ é ideal maximal.

iv) Como pelo item *i)* sabemos que $Im(\phi) = K[\alpha]$, segue pelo Teorema 3.31 que $\dfrac{K[x]}{Ker(\phi)} \simeq K[\alpha]$.

□

Como dito anteriormente, $K[\alpha]$ é um conjunto muito especial. Após estudarmos o teorema acima, podemos apresentar o próximo teorema que nos diz a respeito da estrutura de $K[\alpha]$:

Corolário 4.27. *Seja $\alpha \in L \supseteq K$. Se α é algébrico sobre K então $K[\alpha]$ é um subcorpo de L que contém K. Neste caso, $K[\alpha] = K(\alpha)$. Se α é transcendente sobre K então $K[\alpha]$ é um subdomínio de L isomorfo ao domínio $K[x]$ dos polinômios em uma indeterminada x.*

Demonstração. Segue do Teorema 4.26. □

Observe que por meio dos resultados anteriores podemos classificar as extensões simples: se α é algébrico sobre K, então $K[\alpha]$ é isomorfo a $\dfrac{K[x]}{K[x] \cdot m_\alpha(x)}$. Se α é transcendente sobre K então $K[\alpha]$ é isomorfo a $K[x]$.

Agora, vamos apresentar algumas aplicações:

Exemplo 4.28. *Tome $\alpha = \sqrt{2}$ sobre $\mathbb{Q}$. Sabemos, pela Definição 4.25 que $\mathbb{Q}[\sqrt{2}] = \{p(\sqrt{2}) \mid p(x) \in \mathbb{Q}[x]\}$.*

Mas, pelo Teorema 4.26 sabemos também que $\dfrac{\mathbb{Q}[x]}{\mathbb{Q}[x] \cdot m_{\sqrt{2}}(x)} \simeq \mathbb{Q}[\sqrt{2}]$. Além disso, já calculamos $m_{\sqrt{2}}(x) = x^2 - 2$. Logo se $I = \mathbb{Q}[x] \cdot (x^2 - 2)$, então $\dfrac{\mathbb{Q}[x]}{I} = \{f(x) + I \mid f(x) \in \mathbb{Q}[x]\} \simeq \{a + bx \mid a, b \in \mathbb{Q}\}$, assim $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, como já sabíamos pelo Exemplo 4.8.

Exemplo 4.29. *Os elementos da extensão $\mathbb{Q}[\pi]$ são da forma $a_0 + a_1\pi + a_2\pi^2 + a_3\pi^3 + \ldots$.*

De fato, como $\mathbb{Q}[\pi] \simeq \mathbb{Q}[x]$ e $\mathbb{Q}[x] = \{a_0 + a_1x + a_2x^2 + + \ldots \mid a_i \in \mathbb{Q} \ \forall \ i = 0, 1, \ldots\}$ então $\mathbb{Q}[\pi] = \{a_0 + a_1\pi + a_2\pi^2 + a_3\pi^3 + \ldots \mid a_0, a_1, a_2, a_3, \ldots \in \mathbb{Q}\}$.

Exemplo 4.30. *Considere agora $\mathbb{Q}[\sqrt[3]{2}]$. Como podemos descrever os elementos dessa extensão?*

Primeiramente, o polinômio minimal $m_{\sqrt[3]{2}}(x)$ associado a $\alpha = \sqrt[3]{2}$ é $x^3 - 2$. Dessa forma, $\mathbb{Q}[\sqrt[3]{2}] \simeq \dfrac{\mathbb{Q}[x]}{\mathbb{Q}[x] \cdot (x^3 - 2)} = \{a + bx + cx^2 \mid a, b, c \in \mathbb{Q}\}$. Portanto $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$.

Corolário 4.31. *Se α e β são raízes de um mesmo polinômio irredutível sobre K, então $K[\alpha]$ e $K[\beta]$ são corpos isomorfos, e o isomorfismo de corpos maiores pode ser entendido como uma função de α em β (e como a identidade sobre K).*

Demonstração. Sejam $\alpha, \beta \in L \supseteq K$ e $m(x) \in K[x]$ irredutível sobre K. Considere ainda que $m(\alpha) = m(\beta) = 0$. Sabemos pelo Teorema 4.26 que, se α e β são algébricos sobre K, então $Ker(\phi) = K[x] \cdot m(x)$ é um ideal maximal, o que implica pelo item iv) que $K[\alpha] \simeq \dfrac{K[x]}{Ker(\phi)} \simeq K[\beta]$. Poderíamos também demonstrar este corolário de outra forma: basta construir um homomorfismo $\tau : K[\alpha] \to K[\beta]$ de forma que $\tau(\alpha) = \beta$ e $\tau_{|_K} = Id$ e verificar que τ é um isomorfismo. □

O resultado acima nos garante que as extensões $\mathbb{R}[i]$ e $\mathbb{R}[-i]$ são isomorfas, visto que i e $-i$ são raízes do polinômio $m(x) = x^2 + 1$, irredutível sobre $\mathbb{R}$. Além disso, podemos generalizar esse exemplo por meio do corolário apresentado. Assim, se α é uma raiz complexa de um polinômio irredutível $f(x) \in K[x]$, sabemos que $\overline{\alpha}$ também será, e portanto $K[\alpha] \simeq K[\overline{\alpha}]$.

Proposição 4.32. *Sejam $L \supseteq K$ e $\alpha \in L$ algébrico sobre K. Se o grau do polinômio $m_\alpha(x)$ é n, então:*

i) Para todo $f(x) \in K[x]$, $f(\alpha)$ pode ser expresso de modo único na forma $f(\alpha) = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$, onde $a_i \in K$, $i = 0, \ldots, n-1$.

ii) $K[\alpha] = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mid a_i \in K\}$ é um subcorpo de L que contém K.

iii) Se $K = \mathbb{Z}_p$ então $K[\alpha]$ é um corpo contendo exatamente p^n elementos.

Demonstração. i) Sejam $\alpha \in L$ algébrico sobre K e $m_\alpha(x)$ o polinômio minimal de α sobre K de grau n. Seja $f(x) \in K[x]$ um polinômio qualquer. Pelo algoritmo da divisão, sabemos que existem $q(x), r(x) \in K[x]$ tais que

$$\begin{aligned} f(x) = q(x) \cdot m_\alpha(x) + r(x) \quad &\Rightarrow \quad f(\alpha) = q(\alpha) \cdot m_\alpha(\alpha) + r(\alpha) \\ &\Rightarrow \quad f(\alpha) = q(\alpha) \cdot 0 + r(\alpha) \\ &\Rightarrow \quad f(\alpha) = r(\alpha) \end{aligned}$$

no qual $r(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$, onde $a_i \in K, i = 1, \ldots, n-1$. Como $r(x) = 0$ ou $1 \leq \partial r < \partial m_\alpha$ segue que $f(\alpha) = r(\alpha) = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$.

Para mostrar a unicidade, suponha que existam $b_0, b_1, \ldots, b_{n-1} \in K$ tais que $f(\alpha) = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$. Assim, ao considerarmos o polinômio $q(x) \in K[x]$ dado por $q(x) = (a_0 - b_0) + (a_1 - b_1)x + \ldots + (a_{n-1} - b_{n-1})x^{n-1}$ temos $q(\alpha) = 0$ já que $0 = f(\alpha) - f(\alpha) = (a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}) - (b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}) = (a_0 - b_0) + (a_1 - b_1)\alpha + \ldots + (a_{n-1} - b_{n-1})\alpha^{n-1} = q(\alpha)$. Além disso $\partial q = n - 1 < n = \partial m_\alpha$. Por definição, $m_\alpha(x)$ é o polinômio de menor grau cujo α é raiz, assim só podemos ter $q(x) = 0$, donde segue $a_i = b_i \ \forall\, i = 1, \ldots, n-1$.

ii) O item *ii*) segue do Corolário 4.27.

iii) Sejam $\alpha \in L \supseteq K$ e $m_\alpha(x) \in K[x]$. Pelo Item *i*) sabemos que $\forall\, f(x) \in K[x]$ temos $f(\alpha) = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$. Como $a_i \in K = \mathbb{Z}_p \forall\, i \in \{0, \ldots, n-1\}$, há p possibilidades de escolha para cada um dos termos a_i. Pelo princípio da contagem há $p \cdot \ldots \cdot p = p^n$ formas diferentes de escrever $f(\alpha)$, portanto $\mathbb{Z}_p[\alpha]$ contém exatamente p^n elementos.

□

O próximo lema apresenta uma caracterização para isomorfismo entre extensões algébricas simples.

Lema 4.33. *Suponha que K e L sejam subcorpos de $\mathbb{C}$ e que $\iota : K \to L$ é um isomorfismo. Sejam $K[\alpha], L[\beta]$ extensões algébricas simples de K e L, respectivamente, de forma que*

α tenha polinômio minimal $m_\alpha(x)$ sobre K e β tenha polinômio minimal $m_\beta(x)$ sobre L. Além disso, suponha que $m_\beta(x) = \iota(m_\alpha(x))$. Então existe um isomorfismo $j : K[\alpha] \to L[\beta]$ tal que $j_{|_K} = \iota$ e $j(\alpha) = \beta$.

Demonstração. Sejam $K[\alpha], L[\beta]$ extensões algébricas simples de K e L, de forma que α tenha polinômio minimal $m_\alpha(x)$ sobre K e β tenha polinômio minimal $m_\beta(x)$ sobre L. Como $m_\beta(x) = \iota(m_\alpha(x))$ e ι é isomorfismo, $\partial m_\beta(x) = \partial m_\alpha(x)$, digamos, r.

Sabemos que todo elemento de $K[\alpha]$ é da forma $p(\alpha)$, para algum $p(x) \in K[x]$, tal que $\partial p(x) < \partial m_\alpha(x) = r$. Ou ainda, $K[\alpha] = \{a_0+a_1\alpha+\ldots+a_{r-1}\alpha^{r-1} \mid a_i \in K, i = 0, \ldots, r-1\}$. Da mesma forma, $L[\beta] = \{b_0 + b_1\beta + \ldots + b_{r-1}\beta^{r-1} \mid b_i \in L, i = 0, \ldots, r-1\}$. Vamos definir $j(p(\alpha)) = (\iota(p))(\beta)$, ou seja, $j(a_0 + a_1\alpha + \ldots + a_{r-1}\alpha^{r-1}) = (\iota(a_0)) + (\iota(a_1))\beta + \ldots + (\iota(a_{r-1}))\beta^{r-1}$.

É fácil ver que j está bem definida. Além disso, dado $a_0+a_1\alpha+\ldots+a_{r-1}\alpha^{r-1} \in Ker(j)$, temos:

$$\begin{aligned} a_0 + a_1\alpha + \ldots + a_{r-1}\alpha^{r-1} \in Ker(j) &\Leftrightarrow j(a_0 + a_1\alpha + \ldots + a_{r-1}\alpha^{r-1}) = 0 \\ &\Leftrightarrow (\iota(a_0)) + (\iota(a_1))\beta + \ldots + (\iota(a_{r-1}))\beta^{r-1} = 0 \\ &\Leftrightarrow \iota(a_i) = 0 \ \forall\ i = 1, \ldots, r-1 \\ &\Leftrightarrow a_i = 0 \ \forall\ i = 1, \ldots, r-1 \\ &\Leftrightarrow Ker(j) = \{0\} \end{aligned}$$

Portanto j é injetora. Agora, dado $b_0 + b_1\beta + \ldots + b_{r-1}\beta^{r-1} \in L[\beta]$, existe $\iota^{-1}(b_0) + \iota^{-1}(b_1)\alpha + \ldots + \iota^{-1}(b_{r-1})\alpha^{r-1} \in K[\alpha]$ tal que $j(\iota^{-1}(b_0) + \iota^{-1}(b_1)\alpha + \ldots + \iota^{-1}(b_{r-1})\alpha^{r-1}) = \iota(\iota^{-1}(b_0)) + \iota(\iota^{-1}(b_1))\beta + \ldots + \iota(\iota^{-1}(b_{r-1}))\beta^{r-1} = b_0 + b_1\beta + \ldots + b_{r-1}\beta^{r-1} \in L[\beta]$.

Assim concluímos que j é um isomorfismo tal que $j_{|_K} = \iota$ e $j(\alpha) = \beta$. □

Lembra-se do Exemplo 4.8 que citamos anteriormente? Pois bem, agora vamos comentar mais a respeito.

Considere a extensão $\mathbb{Q}[\sqrt[3]{2}, u]$ em que $u = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$ (a raiz cúbica da unidade, ou seja, $u^3 = 1$). Já sabemos que $m_{\sqrt[3]{2}}(x) = x^3 - 2$. Porém $(\sqrt[3]{2}u)^3 - 2 = (\sqrt[3]{2})^3 \cdot u^3 - 2 = 2 \cdot 1 - 2 = 0$, ou seja, $m_{\sqrt[3]{2}}(\sqrt[3]{2}u) = 0$. Como $x^3 - 2$ é irredutível sobre $\mathbb{Q}$, pelo Corolário 4.31 concluímos que $\mathbb{Q}[\sqrt[3]{2}] \simeq \mathbb{Q}[\sqrt[3]{2}u]$.

Além disso, como $u = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$ temos $u^2 = \left(\frac{-1}{2} + \frac{\sqrt{3}}{2}i\right) \cdot \left(\frac{-1}{2} + \frac{\sqrt{3}}{2}i\right) = \frac{-1}{2} - \frac{\sqrt{3}}{2}i = \overline{u}$. Observe também que $-1 - u = -1 - \left(\frac{-1}{2} + \frac{\sqrt{3}}{2}i\right) = \frac{-1}{2} - \frac{\sqrt{3}}{2}i = u^2$. E $(\sqrt[3]{2} \cdot u^2)^3 - 2 = 2 \cdot u^6 - 2 = 2 \cdot 1 - 2 = 2 - 2 = 0$, portanto $\sqrt[3]{2}u^2$ também é raiz de $x^3 - 2$. Novamente, pelo Corolário 4.31, concluímos que $\mathbb{Q}[\sqrt[3]{2}] \simeq \mathbb{Q}[\sqrt[3]{2}u] \simeq \mathbb{Q}[\sqrt[3]{2}u^2]$. Portanto $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{2}] \simeq \mathbb{Q}[\sqrt[3]{2}u] \simeq \mathbb{Q}[\sqrt[3]{2}u^2] \subseteq \mathbb{C}$.

4.2 Corpo de decomposição de um polinômio

Nesta seção daremos continuidade aos estudos de extensões de corpos e polinômios. Assim, vamos considerar K um subcorpo de $\mathbb{C}$, com $\mathbb{C}$ sendo um corpo algebricamente

fechado, ou seja, $\forall\, f(x) \in \mathbb{C}[x]$, $\exists\, \alpha \in \mathbb{C}$ tal que $f(\alpha) = 0$. Dessa forma, podemos escrever $f(x)$ como um produto de fatores lineares, ou seja, $f(x) = c\cdot(x-\alpha_1)^{n_1}\cdot\ldots\cdot(x-\alpha_m)^{n_m} \in \mathbb{C}[x]$, em que $c \in \mathbb{C}$ e $n_1, \ldots, n_m$ são inteiros positivos. Agora, vamos introduzir uma definição:

Definição 4.34. *Se $f(x) = a_0 + a_1x + \ldots + a_nx^n \in K[x]$ define-se o polinômio $f'(x) = a_1 + 2a_2x + \ldots + na_nx^{n-1} \in K[x]$ como sendo a* ***derivada*** *de $f(x)$.*

Se $\partial f = n \geq 1$ então $f'(x) \neq 0$ e $\partial f'(x) = n - 1$. Além disso, se $f(x), g(x) \in K[x]$, a derivada satisfaz algumas propriedades importantes:

1. $(f(x) + g(x))' = f'(x) + g'(x)$;
2. $(a \cdot f(x))' = a \cdot f'(x)$;
3. $(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x)$.

Por meio desse novo conceito apresentado, podemos explorar ainda mais o campo dos polinômios e extensões de corpos, ampliando a quantidade de resultados que nos fornecem informações importantes para a teoria, como é o caso do próximo teorema.

Teorema 4.35. *Sejam $f(x) \in K[x]$, $\partial f = n > 1$ e $\alpha \in \mathbb{C}$ uma raiz de $f(x)$. Então:*

i) α é uma raiz simples de $f(x)$ se e somente se $f(\alpha) = 0$ e $f'(\alpha) \neq 0$.

ii) Se $f(x)$ é irredutível sobre K então todas as raízes de $f(x)$ são simples.

Demonstração. i) Sejam $f(x) \in K[x]$ com $\partial f = n > 1$ e $\alpha \in \mathbb{C}$ uma raiz de $f(x)$. Por hipótese, α é uma raiz simples de $f(x) \in K[x]$, logo $(x - \alpha) \mid f(x)$. Assim, existe $g(x) \in K[x]$ tal que $f(x) = (x - \alpha) \cdot g(x)$. Observe que $f(\alpha) = (\alpha - \alpha) \cdot g(\alpha) = 0 \cdot g(\alpha) = 0$. Além disso, como α é simples, $g(\alpha) \neq 0$. Pela regra do produto, temos $f'(x) = 1 \cdot g(x) + (x - \alpha) \cdot g'(x) = g(x) + (x - \alpha) \cdot g'(x)$. Portanto $f'(\alpha) = g(\alpha) + (\alpha - \alpha) \cdot g'(\alpha) = g(\alpha) + 0 \cdot g'(\alpha) = g(\alpha) \neq 0$.

Por outro lado, vamos supor agora que $f(\alpha) = 0$ e que $f'(\alpha) \neq 0$. Como $f(\alpha) = 0$, α é raiz de $f(x)$, então pelo Corolário 3.38 segue que $(x - \alpha) \mid f(x)$. Assim existe $g(x) \in K[x]$ tal que $f(x) = (x-\alpha)\cdot g(x)$. Mas $f(x) = (x-\alpha)\cdot g(x) \Rightarrow f'(x) = g(x)+(x-\alpha)\cdot g'(x)$. Como $f'(\alpha) \neq 0$, segue que $g(\alpha)+(\alpha-\alpha)\cdot g'(\alpha) \neq 0 \Rightarrow g(\alpha) \neq 0$. Como $g(\alpha) \neq 0$, podemos concluir que $(x - \alpha) \nmid g(x)$. Como $(x - \alpha) \mid f(x)$ e $(x - \alpha)^2 \nmid f(x)$, concluímos que α é raiz simples de $f(x)$.

ii) Vamos demonstrar pela contra-positiva, ou seja, se existe uma raiz de $f(x)$ que não é simples então $f(x)$ é redutível sobre K.

De fato, se existe $\alpha \in \mathbb{C}$ raiz de $f(x)$ que não é simples, podemos escrever $f(x)$ da seguinte forma:

$$f(x) = (x - \alpha)^m \cdot q(x), \qquad q(\alpha) \neq 0, m \in \mathbb{Z}, m > 1, \partial f = n, n \geq m.$$

Assim $f(\alpha) = (\alpha - \alpha)^m \cdot q(\alpha) = 0 \cdot q(\alpha) = 0$. Pelo item i) do Teorema 4.35, como α não é simples, então $f(\alpha) \neq 0$ ou $f'(\alpha) = 0$. Como $f(\alpha) = 0$, temos $f'(\alpha) = 0$. Agora, pelo algoritmo da divisão, sabemos que existe $q_1(x), r_1(x) \in K[x]$ tais que

$$f(x) = f'(x) \cdot q_1(x) + r_1(x), \qquad \partial r_1 < \partial f' \text{ ou } r_1(x) = 0.$$

Dessa forma $f(\alpha) = f'(\alpha) \cdot q_1(\alpha) + r_1(\alpha) \Rightarrow 0 = 0 \cdot q_1(\alpha) + r_1(\alpha) \Rightarrow r_1(\alpha) = 0$. Novamente pelo algoritmo da divisão sabemos que existem $q_2(x), r_2(x) \in K[x]$ tais que $f'(x) = r_1(x) \cdot q_2(x) + r_2(x)$, $\partial r_2 < \partial r_1$ ou $r_2(x) = 0$. Assim $f'(\alpha) = r_1(\alpha) \cdot q_2(\alpha) + r_2(\alpha) \Rightarrow 0 = 0 \cdot q_2(\alpha) + r_2(\alpha) \Rightarrow r_2(\alpha) = 0$. Realizando-se esse processo indutivamente, obteremos $r_1(\alpha) = r_2(\alpha) = \ldots = r_k(\alpha) = 0$, com $\partial r_k < \partial r_{k-1} < \ldots < \partial r_2 < \partial r_1$ ou $r_i(x) = 0$, para algum $i = 1, \ldots, k$. Como $\partial r_1 < \partial f = n$, em algum momento teremos $\partial r_i = 0$ para algum $i = 1, \ldots, k$. Como $r_i(\alpha) = 0$, concluímos que $r_i(x) = 0$. Assim $r_{i-1}(x) = r_{i-2}(x) \cdot q_i(x) + 0$, ou seja, r_{i-1} será redutível e assim basta substituir em $r_{i-2}(x), \ldots, r_1(x), f'(x)$ e $f(x)$. Portanto $f(x)$ é redutível sobre K.

□

Corolário 4.36. *Sejam $f(x) \in K[x]$, $\partial f = n > 1$ e $\alpha \in \mathbb{C}$ uma raiz de $f(x)$. Então α é raiz múltipla de $f(x)$ se e somente se $f(x)$ e $f'(x)$ tem um fator de grau maior ou igual a 1 em comum.*

Demonstração. O resultado decorre da contrapositiva do Item i) do Teorema 4.35. De fato, pela contrapositiva, temos que α é raiz múltipla de f se e somente se $f(\alpha) \neq 0$ ou $f'(\alpha) = 0$. Como α é raiz de $f(x)$, então $f(\alpha) = 0$ e assim α é raiz múltipla de f se e somente se $f'(\alpha) = 0$, portanto $f(x)$ e $f'(x)$ possuem um fator em comum. □

Agora, vamos apresentar uma definição muito importante:

Definição 4.37. *Chamamos de **corpo de decomposição** de um polinômio $f(x) \in K[x]$ sobre $K \subseteq \mathbb{C}$, que denotaremos por $L = Gal(f, K)$, o menor subcorpo de $\mathbb{C}$ que contém K e todas as raízes de $f(x)$ em $\mathbb{C}$.*

Observe que este subcorpo existe e é igual a intersecção de todos os subcorpos de $\mathbb{C}$ contendo K e todas as raízes de $f(x)$ em $\mathbb{C}$. Além disso, o corpo de decomposição de um polinômio $f(x)$ sobre K é único.

Dado um polinômio $f(x) \in K[x]$, vamos apresentar uma maneira de construir $Gal(f, K)$. Assim, como $\mathbb{C}$ é um corpo algebricamente fechado, sabemos que $f(x)$ pode ser escrito da forma $f(x) = c \cdot (x - \alpha_1)^{n_1} \cdot \ldots \cdot (x - \alpha_r)^{n_r}$ em que $\alpha_1, \ldots, \alpha_r \in \mathbb{C}$. Agora, considere $K_0 = K, K_1 = K[\alpha_1], K_2 = K_1[\alpha_2], \ldots, K_r = K_{r-1}[\alpha_r]$, com $K \subseteq K_1 \subseteq \ldots \subseteq K_r$. Observe que K_r é o menor subcorpo de $\mathbb{C}$ contendo K e $\alpha_1, \ldots, \alpha_r$, portanto $K_r = Gal(f, K)$. Além disso, como $K_r = K_{r-1}[\alpha_r]$, podemos denotar $K_r = K[\alpha_1, \alpha_2, \ldots, \alpha_r] = Gal(f, K)$. Vale ressaltar também que, qualquer que seja a ordem de $\alpha_1, \ldots, \alpha_r$ ainda teremos o mesmo corpo de decomposição. Esse processo é conhecido como adjunção de raízes.

Além disso, podemos interpretar o corpo de decomposição de outra maneira. Dado $f(x)$ um polinômio sobre K, dizemos que $f(x)$ se divide sobre K se pode ser expresso como uma produto de fatores lineares $f(x) = k(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$, $k, \alpha_1, \ldots, \alpha_n \in K$. Dessa

forma, podemos interpretar o corpo de decomposição de $f(x)$ sobre K como o menor corpo na qual $f(x)$ se divide, ou seja, $Gal(f(x), K) = K[\alpha_1, \ldots, \alpha_n]$, como visto anteriormente.

Agora, vamos construir o corpo de decomposição de $p(x) = x^3 - 2 \in \mathbb{Q}[x]$. Já calculamos as raízes de $p(x)$ que são $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2}u$ e $\alpha_3 = \sqrt[3]{2}u^2$. Assim $Gal(x^3 - 2, \mathbb{Q}) = \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}u, \sqrt[3]{2}u^2]$. Como $\sqrt[3]{2}u^2 = \overline{\sqrt[3]{2}u}$ temos $Gal(x^3 - 2, \mathbb{Q}) = \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}u, \sqrt[3]{2}u^2] = \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}u, \overline{\sqrt[3]{2}u}] = \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}u]$. Porém, podemos simplificar ainda mais a notação de $Gal(x^3-2, \mathbb{Q})$. Observe que $u \in \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}u]$, já que $\sqrt[3]{2} \cdot \sqrt[3]{2}u = (\sqrt[3]{2})^2 u \in \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}u] \Rightarrow \sqrt[3]{2} \cdot (\sqrt[3]{2})^2 u \in \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}u] \Rightarrow 2u \in \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}u] \Rightarrow \frac{1}{2} \cdot 2u \in \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}u] \Rightarrow u \in \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}u]$. Dessa forma como $\sqrt[3]{2}$ e $u \in \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}u]$ temos $\mathbb{Q}[\sqrt[3]{2}, u] \subseteq \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}u]$. Além disso, como $\sqrt[3]{2}$ e $\sqrt[3]{2}u \in \mathbb{Q}[\sqrt[3]{2}, u]$ temos $\mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}u] \subseteq \mathbb{Q}[\sqrt[3]{2}, u]$. Portanto $\mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}u] = \mathbb{Q}[\sqrt[3]{2}, u]$.

Para facilitar a notação, vamos adotar a partir de agora neste trabalho que $\alpha = \sqrt[3]{2}$ sempre que nos referirmos ao exemplo acima. Portanto $Gal(x^3 - 2, \mathbb{Q}) = \mathbb{Q}[\alpha, u]$.

Vamos construir também o corpo de decomposição do polinômio $f(x) = x^4 - 2$ sobre $\mathbb{Q}$. Observe que as raízes de $f(x)$ são $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}$ e $-i\sqrt[4]{2}$, assim podemos fatorar $f(x) = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2})$. Se K é o corpo de decomposição de $x^4 - 2$, veja que $K \supseteq \{\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}\}$. Como $\sqrt[4]{2} \in K$, $(\sqrt[4]{2})^2, (\sqrt[4]{2})^3$ e $(\sqrt[4]{2})^4 = 2 \in K$, o que nos dá $\mathbb{Q}[\sqrt[4]{2}] \subseteq K$. Mas $i\sqrt[4]{2}$ e $-i\sqrt[4]{2} \notin \mathbb{Q}[\sqrt[4]{2}]$. Assim $K \nsubseteq \mathbb{Q}[\sqrt[4]{2}]$.

Como faltam duas raízes de $f(x)$ em $\mathbb{Q}[\sqrt[4]{2}]$, vamos adjuntar uma delas em $\mathbb{Q}[\sqrt[4]{2}]$, digamos, $\alpha = i\sqrt[4]{2}$. Dessa forma, encontramos a extensão $\mathbb{Q}[\sqrt[4]{2}, i\sqrt[4]{2}]$. Observe que $-i\sqrt[4]{2} = (-1) \cdot i\sqrt[4]{2} \in \mathbb{Q}[\sqrt[4]{2}, i\sqrt[4]{2}]$. Mas a notação desse conjunto pode ser simplificada: como $\sqrt[4]{2}$ e $i\sqrt[4]{2} \in \mathbb{Q}[\sqrt[4]{2}, i\sqrt[4]{2}]$, temos $(i\sqrt[4]{2})\sqrt[4]{2} = i(\sqrt[4]{2})^2 \in \mathbb{Q}[\sqrt[4]{2}, i\sqrt[4]{2}]$. Novamente, $i(\sqrt[4]{2})^2\sqrt[4]{2} = i(\sqrt[4]{2})^3 \in \mathbb{Q}[\sqrt[4]{2}, i\sqrt[4]{2}]$ e assim $i(\sqrt[4]{2})^3\sqrt[4]{2} = 2i \in \mathbb{Q}[\sqrt[4]{2}, i\sqrt[4]{2}]$, o que nos dá $i \in \mathbb{Q}[\sqrt[4]{2}, i\sqrt[4]{2}]$. Dessa forma, se adjuntarmos $\{i\}$ em $\mathbb{Q}[\sqrt[4]{2}]$, teremos $i\sqrt[4]{2}$ e $-i\sqrt[4]{2} \in \mathbb{Q}[\sqrt[4]{2}, i]$. Observe que todas as raízes de $f(x)$ estão em $\mathbb{Q}[\sqrt[4]{2}, i]$. Além disso, este é o menor corpo de $\mathbb{C}$ que contém as raízes de $f(x)$, já que qualquer outro corpo conterá os elementos i e $\sqrt[4]{2}$ e dessa forma conterá $\mathbb{Q}[\sqrt[4]{2}, i]$. Portanto $Gal(x^4 - 2, \mathbb{Q}) = \mathbb{Q}[\sqrt[4]{2}, i]$.

Lema 4.38. *Suponha que $i : K \to K'$ é um isomorfismo de subcorpos de $\mathbb{C}$. Seja $f(x)$ um polinômio sobre K e $Gal(f(x), K)$ o corpo de decomposição de $f(x)$. Considere L qualquer extensão de K' tal que $i(f)$ decompõe-se linearmente sobre L. Então existe um monomorfismo $j : Gal(f, K) \to L$ tal que $j_{|_K} = i$.*

Demonstração. Observe o diagrama:

$$\begin{array}{ccc} K & \longrightarrow & Gal(f, K) \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle j} \\ K' & \longrightarrow & L \end{array}$$

em que j precisa ser encontrada. Construiremos j por indução no grau de $f(x)$. Sobre $Gal(f, K)$, podemos escrever $f(x)$ como $f(x) = k \cdot (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$.

O polinômio minimal m de α_1 sobre K é um fator irredutível de $f(x)$. Assim, $i(m)$ divide $i(f)$, o qual se decompõe sobre L, ou seja, sobre L temos $i(m) = (x-\beta_1)\cdot\ldots\cdot(x-\beta_r)$, $\beta_i \in L$. Como $i(m)$ é irredutível sobre K', então $i(m)$ é o polinômio minimal de β_1 sobre K'. Então, pelo teorema 4.33 existe um isomorfismo $j_1 : K[\alpha_1] \to K'[\beta_1]$ tal que $j_{1_{|_K}} = i$ e $j_1(\alpha_1) = \beta_1$. Deste modo $Gal(f, K)$ é o corpo de decomposição sobre $K[\alpha_1]$ do polinômio $g(x) = \frac{f(x)}{x-\alpha_1}$. Por indução, existe um monomorfismo $j : Gal(f, K) \to L$ tal que $j_{|_{K[\alpha_1]}} = j_1$. Mas assim $j_{|_K} = i$ e portanto temos o desejado. □

Teorema 4.39. *Seja $i : K \to K'$ um isomorfismo. Seja $Gal(f, K)$ o corpo de decomposição de $f(x)$ sobre K e seja $Gal'(i(f), K')$ o corpo de decomposição de $i(f(x))$ sobre K'. Então existe um isomorfismo $j : Gal(f, K) \to Gal'(i(f), K')$ tal que $j_{|_K} = i$. Em outras palavras, as extensões $Gal(f, K)$ e $Gal'(i(f), K')$ são isomorfas.*

Demonstração. Observe o diagrama:

$$\begin{array}{ccc} K & \longrightarrow & Gal(f, K) \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle j} \\ K' & \longrightarrow & Gal'(i(f), K') \end{array}$$

Devemos encontrar j para que o diagrama comute. Pelo lema anterior, sabemos que existe um monomorfismo $j : Gal(f, K) \to Gal'(i(f), K')$ tal que $j_{|_K} = i$. Ora, $j(Gal(f, K))$ é o corpo de decomposição de $i(f)$ sobre K' e está contido em $Gal'(i(f), K')$. Como $Gal'(i(f), K')$ é também o corpo de decomposição de $i(f)$ sobre K', temos que $j(Gal(f, K)) = Gal'(i(f), K'))$, portanto j é sobrejetora. Como j já era monomorfismo, segue que j é um isomorfismo. □

4.3 Grau de uma extensão

A partir de agora apresentaremos uma nova definição chamada grau de uma extensão, que está intimamente relacionada ao grau do polinômio minimal, para extensões simples. Veremos também que as extensões podem ser vistas sob um novo olhar, utilizando conceitos de álgebra linear. Esses conceitos podem ser encontrados em [COELHO; LOURENCO, 2018] e [GONÇALVES, 2012].

Dada uma extensão $L : K$, L pode ser visto como um espaço vetorial sobre K, considerando as operações

$$\begin{aligned} + : L \times L &\to L & \cdot : K \times L &\to L \\ (u, v) &\mapsto u + v & (\lambda, v) &\mapsto \lambda \cdot v \end{aligned}$$

Sabemos que todo espaço vetorial possui base, e, no caso de dimensão finita, a quantidade de elementos da base está bem definida. Então, se n denotar a quantidade de elementos da base, chamaremos n como sendo o **grau** ou a **dimensão** de L sobre K e representamos por $[L : K]$.

Vamos considerar a extensão $L : K$ a partir de agora como sendo um espaço vetorial, ou seja, L será visto como K- espaço vetorial. Adquirindo esse novo olhar sobre L, apresentamos a seguinte definição:

Definição 4.40. *Seja L uma extensão de K. Se L for um espaço vetorial de dimensão finita sobre K, dizemos que L é uma* ***extensão finita****. Caso contrário dizemos que $L : K$ é uma extensão infinita.*

Exemplo 4.41. *A extensão $\mathbb{Q}[\sqrt{2}] : \mathbb{Q}$ é uma extensão finita. Uma base para esta extensão é $B = \{1, \sqrt{2}\}$.*

De fato, como os elementos de $\mathbb{Q}[\sqrt{2}]$ são da forma $a + b\sqrt{2}$ com $a, b \in \mathbb{Q}$, temos que $\{1, \sqrt{2}\}$ gera $\mathbb{Q}[\sqrt{2}]$ como $\mathbb{Q}$-espaço vetorial. Além disso, se $a + b\sqrt{2} = 0$, temos $a = -b\sqrt{2}$. Como $a \in \mathbb{Q}$, necessariamente $a = 0$ o que implica $b = 0$ e assim $\{1, \sqrt{2}\}$ é um conjunto linearmente independente. Portanto $\{1, \sqrt{2}\}$ é uma base para o $\mathbb{Q}$-espaço vetorial $\mathbb{Q}[\sqrt{2}]$.

Exemplo 4.42. *No Exemplo 4.14 havíamos comentado a respeito de $\mathbb{R} : \mathbb{Q}$ não ser uma extensão simples. De fato, agora temos mais ferramentas para falar a respeito dessa extensão. Portanto, vamos mostrar que $\mathbb{R} : \mathbb{Q}$ não é uma extensão simples. Além disso, essa extensão é um exemplo de extensão infinita.*

Suponha por absurdo que $\mathbb{R} : \mathbb{Q}$ seja uma extensão simples, ou seja, existe $\alpha \in \mathbb{R}$ tal que $\mathbb{R} = \mathbb{Q}[\alpha]$. Se α for algébrico sobre $\mathbb{Q}$, então $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbb{Q}\}$. Portanto a cardinalidade de $\mathbb{Q}[\alpha]$ é igual a cardinalidade do conjunto $\mathbb{Q} \times \mathbb{Q} \times \ldots \times \mathbb{Q}$, visto que cada $a_i \in \mathbb{Q}$. Mas como o cartesiano finito de conjuntos enumeráveis também é enumerável[1], e $\mathbb{Q}[\alpha] = \mathbb{R}$, teríamos que $\mathbb{R}$ é enumerável. Absurdo.

Se α é transcendente sobre $\mathbb{Q}$, então $\mathbb{R} = \mathbb{Q}(\alpha) \simeq \mathbb{Q}(x)$. Porém $\mathbb{Q}(x) = \{\frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{Q}[x], g(x) \neq 0\}$. Dessa forma a cardinalidade de $\mathbb{Q}(\alpha)$ é igual a cardinalidade de $\mathbb{Q} \times \ldots \times \mathbb{Q}$. Novamente teríamos que $\mathbb{Q}(\alpha)$ é uma extensão enumerável, mas por hipótese $\mathbb{Q}(\alpha) = \mathbb{R}$, assim teríamos $\mathbb{R}$ enumerável. Absurdo.

Logo não existe $\alpha \in \mathbb{R}$ tal que $\mathbb{R} = \mathbb{Q}(\alpha)$. Portanto a extensão $\mathbb{R} : \mathbb{Q}$ não é simples.

Além disso, essa extensão é infinita.

Com efeito, vamos provar que o conjunto $\{\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots\}$ é linearmente independente sobre $\mathbb{Q}$. Suponha por absurdo que esse conjunto é linearmente dependente, ou seja, existem $a_1, a_2, \ldots, a_k \in \mathbb{Q}$ e p primo suficientemente grande tais que:

$$a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{5} + \ldots + a_k\sqrt{p} = 0,$$

com algum $a_i \neq 0$ para $i = 1, \ldots, k$. Mas assim teríamos

[1] Ver [LIMA, 2008], p. 51.

$$\begin{aligned} & a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{5} + \ldots + a_i\sqrt{p_i} + \ldots + a_k\sqrt{p} = 0 \\ \Rightarrow \quad & a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{5} + \ldots + a_p\sqrt{p} = -a_i\sqrt{p_i} \\ \Rightarrow \quad & -a_1\frac{\sqrt{2}}{\sqrt{p_i}} - a_2\frac{\sqrt{3}}{\sqrt{p_i}} - a_3\frac{\sqrt{5}}{\sqrt{p_i}} - \ldots - a_p\frac{\sqrt{p}}{\sqrt{p_i}} = a_i \end{aligned}$$

Observe que os elementos $\frac{\sqrt{2}}{\sqrt{p_i}}, \frac{\sqrt{3}}{\sqrt{p_i}}, \frac{\sqrt{5}}{\sqrt{p_i}}, \ldots \notin \mathbb{Q}$. Assim $a_i \notin \mathbb{Q}$, a menos que os elementos $a_1, a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_k$ sejam nulos, o que nos dá $a_i = 0$. Absurdo, pois supomos que algum $a_i \neq 0$ para $i = 1, \ldots, k$.

Portanto concluímos que $\{\sqrt{2}, \sqrt{3}, \sqrt{5} \ldots\}$ é linearmente independente. Como este conjunto é infinito, qualquer base de $\mathbb{R}$ visto como $\mathbb{Q}$-espaço vetorial será infinita também, donde segue que a extensão $\mathbb{R} : \mathbb{Q}$ é infinita.

Exemplo 4.43. *A extensão $\mathbb{Q}[i, \sqrt{5}] : \mathbb{Q}$ tem dimensão 4, visto que $\{1, i, \sqrt{5}, i\sqrt{5}\}$ é base de $\mathbb{Q}[i, \sqrt{5}]$, como será visto mais detalhadamente no Exemplo 4.48.*

Proposição 4.44. *Seja $L : K$ uma extensão de corpos. Então $L = K$ se e somente se $[L : K] = 1$.*

Demonstração. Suponha que $L = K$, assim $\{1\}$ é uma base de $L : K$, já que $\forall\, x \in K$ temos $x = 1 \cdot x$. Portanto $[L : K] = 1$. Reciprocamente, suponha agora que $[L : K] = 1$. Assim existe $x \in L$, $x \neq 0$ tal que $\{x\}$ é base de $L : K$. Como L é corpo, existe $a \in K$ tal que $a \cdot x = 1$. Mas assim $x = a^{-1} \in K$ e portanto $\forall\, y \in L$, podemos escrever $y = bx$, $b \in K$, o que implica que $y = ba^{-1} \in K$. Logo $L \subseteq K$ e como $K \subseteq L$ por ser extensão, podemos concluir que $L = K$. □

Proposição 4.45. *Seja K um corpo e $L \supseteq K$ uma extensão de K. Então*

i) Se $L : K$ é finita então $L : K$ é algébrica.

ii) Se $\alpha \in L \supseteq K$ é um elemento algébrico sobre K e o grau do polinômio $m_\alpha(x)$ é igual a n então $1, \alpha, \ldots, \alpha^{n-1}$ é uma base do espaço vetorial $K[\alpha]$ sobre K e $[K[\alpha] : K] = n < \infty$.

iii) Se $\alpha \in L \supseteq K$ é um elemento transcendente sobre K então $K(\alpha) \supseteq K$ é uma extensão infinita.

Demonstração. i) Seja K um corpo e $L \supseteq K$ uma extensão de K. Sabemos que L pode ser visto como um $K-$espaço vetorial, assim, como por hipótese L é uma extensão finita, sabemos pela definição que $[L : K] = n < \infty$. Portanto um conjunto com $n + 1$ elementos será linearmente dependente.

Seja $\alpha \in L$ e considere o conjunto $B = \{1, \alpha, \ldots, \alpha^{n-1}\}$ com n elementos. Ao consideramos o conjunto $B \cup \{\alpha\}$, como $B \cup \{\alpha\}$ tem $n + 1$ elementos, será L. D. Portanto existem escalares $\lambda_0, \lambda_1, \ldots, \lambda_n \in K$ tais que $\lambda_0 \cdot 1 + \lambda_1 \cdot \alpha + \ldots + \lambda_n \cdot \alpha^n = \lambda_0 + \lambda_1\alpha + \ldots + \lambda_n\alpha^n = 0$, com $\lambda_i \neq 0$, para algum $i \in \{0, \ldots, n\}$. Dessa forma considere o polinômio $f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n$. Observe que $f(\alpha) = 0$, portanto α é algébrico sobre K. Como α é um elemento qualquer de L, segue que $L : K$ é uma extensão algébrica.

ii) Sejam α um elemento algébrico sobre K e $m_\alpha(x) \in K[x]$, com $\partial m_\alpha = n$.

Seja $f(x) \in K[x]$. Pelo algoritmo da divisão existem $q(x), r(x) \in K[x]$ tais que $f(x) = q(x) \cdot m_{\alpha(x)} + r(x)$, com $\partial r < \partial m_\alpha$ ou $r(x) = 0$. Portanto $f(\alpha) = q(\alpha) \cdot m_\alpha(\alpha) + r(\alpha) \Rightarrow f(\alpha) = q(\alpha) \cdot 0 + r(\alpha) \Rightarrow f(\alpha) = r(\alpha)$. Como $\partial r < \partial m_\alpha$ temos $f(\alpha) = a_0 + a_1 x + \ldots + a_{n-1}\alpha^{n-1}$, $a_i \in K, i = 0, \ldots, n-1$. Assim, $f(\alpha)$ pode ser expresso como um produto de constantes $a_0, a_1, \ldots, a_{n-1}$ pelos elementos de $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. Dessa forma B gera $K[\alpha]$. Agora, resta mostrar que é linearmente independente. Desse modo, suponha por absurdo que B é linearmente dependente. Portanto, existem escalares $\lambda_0, \lambda_1, \ldots, \lambda_{n-1} \in K$ tais que $\lambda_0 \cdot 1 + \lambda_1 \cdot \alpha + \ldots + \lambda_{n-1} \cdot \alpha^{n-1} = \lambda_0 + \lambda_1\alpha + \ldots + \lambda_{n-1}\alpha^{n-1} = 0$, com $\lambda_i \neq 0$, para algum $i \in \{0, \ldots, n-1\}$. Mas dessa forma o polinômio $f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_{n-1}x^{n-1}$ é tal que $f(\alpha) = 0$ e $\partial f < \partial m_\alpha$. Absurdo. Portanto o conjunto B é linearmente independente e como gera $K[\alpha]$, podemos inferir que é uma base de $K[\alpha]$.

Além disso, como B possui n elementos, podemos concluir que $[K[\alpha] : K] = n$.

iii) Pela contra-positiva, se $K(\alpha) \supseteq K$ é uma extensão finita então α não é um elemento transcendente sobre K. De fato, pelo item i) segue que se $L \supseteq K$ é uma extensão finita então $L : K$ é uma extensão algébrica, assim para todo $\alpha \in L \supseteq K$ temos que α é algébrico sobre K, ou seja, α não é transcendente sobre K.

□

Corolário 4.46. *Seja $\alpha \in L \supseteq K$. Então as seguintes afirmações são equivalentes:*

i) α é algébrico sobre K;

ii) $[K[\alpha] : K] < \infty$;

iii) $K[\alpha]$ é uma extensão algébrica de K.

Demonstração. i) $\Rightarrow$ *ii*) Como α é algébrico sobre K, sabemos que existe um polinômio $f(x) \in K[x]$ tal que $f(\alpha) = 0$. Pelo Teorema 4.21 sabemos que existe o polinômio $m_\alpha(x)$ de menor grau tal que α é raiz. Portanto, pelo Item *ii*) da Proposição 4.45 podemos concluir que $[K[\alpha] : K] < \infty$.

ii) $\Rightarrow$ *iii*) Como $[K[\alpha] : K] < \infty$, $K[\alpha]$ é uma extensão finita, assim pelo Item i) da Proposição 4.45 podemos concluir que $K[\alpha]$ é uma extensão algébrica de K.

iii) $\Rightarrow$ i) Por hipótese $K[\alpha]$ é uma extensão algébrica sobre K, assim segue diretamente da definição que para todo $\alpha \in K[\alpha]$, α é algébrico sobre K.

□

O próximo teorema que apresentaremos é muito conhecido e será muito utilizado daqui por diante.

Teorema 4.47. *(Pequena Lei da Torre) Sejam $M \supseteq L \supseteq K$ corpos tais que $[M : L]$ e $[L : K]$ são finitas, então $[M : K]$ é finita e $[M : K] = [M : L] \cdot [L : K]$.*

Demonstração. Sejam $M \supseteq L \supseteq K$ corpos tais que $[M : L]$ e $[L : K]$ são finitas. Suponha sem perda de generalidade que $[M : L] = n$ e $[L : K] = m$. Sejam $\{\alpha_1, \ldots, \alpha_n\}$ uma base de $M : L$ e $\{\beta_1, \ldots, \beta_m\}$ uma base de $L : K$. Vamos mostrar que $\tau = \Big\{\alpha_i\beta_j \mid i = 1, \ldots, n,\ j = 1, \ldots, m\Big\}$ é base de M sobre K.

Vamos mostrar que τ é um conjunto linearmente independente. Dessa forma considere $\sum_{j=1}^{m}\sum_{i=1}^{n} \lambda_{ij}\alpha_i\beta_j = 0$, com $\lambda_{ij} \in K$. Vamos mostrar que $\lambda_{ij} = 0\ \forall\ i, j$.

Para tal, vamos expandir o somatório de forma a utilizar a hipótese:

$$\begin{aligned}
\sum_{j=1}^{m}\sum_{i=1}^{n} \lambda_{ij}\alpha_i\beta_j = 0 \quad &\Rightarrow \quad \sum_{j=1}^{m}[(\lambda_{1j}\alpha_1\beta_j) + \ldots + (\lambda_{nj}\alpha_n\beta_j)] = 0 \\
&\Rightarrow \quad \sum_{j=1}^{m} \lambda_{1j}\alpha_1\beta_j + \ldots + \sum_{j=1}^{m} \lambda_{nj}\alpha_n\beta_j = 0 \\
&\Rightarrow \quad \alpha_1 \sum_{j=1}^{m} \lambda_{1j}\beta_j + \ldots + \alpha_n \sum_{j=1}^{m} \lambda_{nj}\beta_j = 0
\end{aligned}$$

Como $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de $M : L$, podemos concluir que

$$\begin{cases}
\sum_{j=1}^{m} \lambda_{1j}\beta_j = 0 \\
\sum_{j=1}^{m} \lambda_{2j}\beta_j = 0 \\
\vdots \qquad\qquad\qquad \vdots \\
\sum_{j=1}^{m} \lambda_{nj}\beta_j = 0
\end{cases}$$

o que nos dá

$$\begin{cases}
\lambda_{11}\beta_1 + \lambda_{12}\beta_2 + \ldots + \lambda_{1m}\beta_m = 0 & (1) \\
\lambda_{21}\beta_1 + \lambda_{22}\beta_2 + \ldots + \lambda_{2m}\beta_m = 0 & (2) \\
\vdots \qquad\qquad \vdots \qquad\qquad\qquad \vdots & \vdots \\
\lambda_{n1}\beta_1 + \lambda_{n2}\beta_2 + \ldots + \lambda_{nm}\beta_m = 0 & (n)
\end{cases}$$

Observe agora a Equação (1). Como $\{\beta_1, \ldots, \beta_m\}$ é uma base de $L : K$, podemos concluir que os escalares $\lambda_{11} = \lambda_{12} = \ldots = \lambda_{1m} = 0$. Expandindo esse raciocínio para as Equações $(2), (3), \ldots, (n)$, podemos concluir que $\lambda_{21} = \lambda_{22} = \ldots = \lambda_{2m} = \lambda_{31} = \lambda_{32} = \ldots = \lambda_{3m} = \ldots = \lambda_{n1} = \lambda_{n2} = \ldots = \lambda_{nm} = 0$. Portanto, $\forall\ i = 1, \ldots, n$ e $\forall\ j = 1, \ldots, m$ temos $\lambda_{ij} = 0$. Assim τ é um conjunto linearmente independente. Agora, vamos mostrar que τ gera M sobre K.

Seja $y \in M$. Como $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de M sobre L, existem escalares $\mu_1, \ldots, \mu_n \in L$ tais que $y = \sum_{k=1}^{n} \mu_k\alpha_k = \mu_1\alpha_1 + \mu_2\alpha_2 + \ldots + \mu_n\alpha_n$. Porém como cada $\mu_i \in L, i = 1, \ldots, n$, existem escalares $\lambda_{i1}, \ldots, \lambda_{im} \in K$ tais que

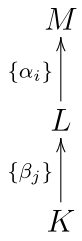
$$\mu_i = \lambda_{i1}\beta_1 + \lambda_{i2}\beta_2 + \ldots + \lambda_{im}\beta_m$$

Portanto:

$$\begin{aligned}
y = \sum_{k=1}^{n} \mu_k \alpha_k \quad &\Rightarrow \quad y = \mu_1\alpha_1 + \mu_2\alpha_2 + \ldots + \mu_n\alpha_n \\
&\Rightarrow \quad y = (\lambda_{11}\beta_1 + \ldots + \lambda_{1m})\beta_m\alpha_1 + \\
&\qquad (\lambda_{21}\beta_1 + \ldots + \lambda_{2m}\beta_m)\alpha_2 + \ldots + (\lambda_{n1}\beta_1 + \ldots + \lambda_{nm}\beta_m)\alpha_n \\
&\Rightarrow \quad y = \Big(\sum_{j=1}^{m} \lambda_{1j}\beta_j\Big)\alpha_1 + \Big(\sum_{j=1}^{m} \lambda_{2j}\beta_j\Big)\alpha_2 + \ldots + \Big(\sum_{j=1}^{m} \lambda_{nj}\beta_j\Big)\alpha_n \\
&\Rightarrow \quad y = \Big(\sum_{j=1}^{m} \lambda_{1j}\alpha_1\beta_j\Big) + \Big(\sum_{j=1}^{m} \lambda_{2j}\alpha_2\beta_j\Big) + \ldots + \Big(\sum_{j=1}^{m} \lambda_{nj}\alpha_n\beta_j\Big) \\
&\Rightarrow \quad y = \sum_{j=1}^{m}\sum_{i=1}^{n} \lambda_{ij}\alpha_i\beta_j
\end{aligned}$$

Dessa forma como $\lambda_{ij} \in K$ e y pode ser escrito como combinação linear dos elementos $\alpha_i\beta_j$, $i = 1, \ldots, n$ e $j = 1, \ldots, m$ podemos concluir que τ gera M sobre K.

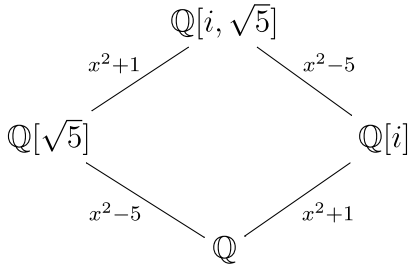
Logo τ é base de M sobre K. Dessa forma, como τ possui $n \cdot m$ elementos, temos que $[M : K] = n \cdot m = [M : L] \cdot [L : K]$. □



Exemplo 4.48. *Vamos considerar as extensões* $K = \mathbb{Q}$, $L = \mathbb{Q}[\sqrt{5}]$ *e* $M = \mathbb{Q}[i, \sqrt{5}]$. *Sabemos que o polinômio minimal associado a extensão* $L : K$ *é* $m_{\sqrt{5}} = x^2 - 5$. *Além disso, como* $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$, *temos que* $B' = \{1, \sqrt{5}\}$ *é base de* $\mathbb{Q}[\sqrt{5}]$. *Além disso, como* i *é algébrico sobre* $\mathbb{Q}[\sqrt{5}]$, *o polinômio minimal associado a extensão* $\mathbb{Q}[i, \sqrt{5}] : \mathbb{Q}[\sqrt{5}]$ *é* $m_i = x^2 + 1$. *Portanto uma base para a extensão* $\mathbb{Q}[i, \sqrt{5}] : \mathbb{Q}[\sqrt{5}]$ *é* $B'' = \{1, i\}$. *Assim, a dimensão da extensão* $\mathbb{Q}[i, \sqrt{5}] : \mathbb{Q}$ *é* $[\mathbb{Q}[i, \sqrt{5}] : \mathbb{Q}] = [\mathbb{Q}[i, \sqrt{5}] : \mathbb{Q}[\sqrt{5}]] \cdot [\mathbb{Q}[\sqrt{5}] : \mathbb{Q}] = 2 \cdot 2 = 4$.

Poderíamos ter pensado também em $K = \mathbb{Q}$, $L = \mathbb{Q}[i]$ e $M = \mathbb{Q}[i, \sqrt{5}]$. O resultado seria o mesmo, a menos da ordem dos polinômios.

Assim, podemos construir o seguinte diagrama para facilitar a visualização:



Dessa forma, como sabemos pelo Exemplo 4.13 que $\mathbb{Q}[i,\sqrt{5}] \simeq \mathbb{Q}[i+\sqrt{5}]$ e a dimensão dessa extensão é 4, podemos caraterizar os elementos desse conjunto.

Como vimos que na Proposição 4.32, se o grau do polinômio é n então $K[\alpha] = \{a_0 + a_1x + \ldots + a_{n-1}\alpha^{n-1} \mid a_i \in K\}$. Dessa forma, como o grau do polinômio associado a extensão $K[i+\sqrt{5}]$ é 4, podemos concluir que $K[i+\sqrt{5}] = \{a + b(i+\sqrt{5}) + c(i+\sqrt{5})^2 + d(i+\sqrt{5})^3 \mid a,b,c,d \in \mathbb{Q}\}$. Como $(i+\sqrt{5})^2 = 4+2i\sqrt{5}$ e $(i+\sqrt{5})^3 = 2\sqrt{5}+14i$, o conjunto anteriormente obtido pode ser descrito da forma $a+b(i+\sqrt{5})+c(i+\sqrt{5})^2+d(i+\sqrt{5})^3 = a+bi+b\sqrt{5}+4c+2ci\sqrt{5}+2d\sqrt{5}+14di = (a+4c)+(b+14d)i+(b+2d)\sqrt{5}+2ci\sqrt{5}$. Portanto podemos reescrever os elementos da extensão, obtendo assim $\mathbb{Q}[i,\sqrt{5}] = \mathbb{Q}[i+\sqrt{5}] = \{x+yi+z\sqrt{5}+wi\sqrt{5} \mid x,y,z,w \in \mathbb{Q}\}$.

Além disso, podemos determinar o polinômio minimal associado ao elemento $\alpha = i+\sqrt{5}$.

Como $\mathbb{Q}[i,\sqrt{5}] \simeq \mathbb{Q}[i+\sqrt{5}]$, $m_{i+\sqrt{5}}(x)$ tem grau 4. Logo, considere o polinômio mônico $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$. Vamos calcular a_0, a_1, a_2 e a_3 de modo que $f(x)$ seja o polinômio minimal associado a $\alpha = i+\sqrt{5}$. Como queremos $f(x) = m_{i+\sqrt{5}}(x)$, precisamos ter $f(i+\sqrt{5}) = 0$. Assim:

$$\begin{aligned} f(i+\sqrt{5}) = 0 &\Rightarrow (i+\sqrt{5})^4 + a_3(i+\sqrt{5})^3 + a_2(i+\sqrt{5})^2 + a_1(i+\sqrt{5}) + a_0 = 0 \\ &\Rightarrow (-4+16i\sqrt{5}) + a_3(14i+2\sqrt{5}) + a_2(4+2i\sqrt{5}) + a_1(i+\sqrt{5}) + a_0 = 0 \\ &\Rightarrow (-4+4a_2+a_0) + (14a_3+a_1)i + (2a_3+a_1)\sqrt{5} + (16+2a_2)i\sqrt{5} = 0 \end{aligned}$$

Portanto, temos:

$$\begin{cases} -4+4a_2+a_0 = 0 \\ 4a_3+a_1 = 0 \\ 2a_3+a_1 = 0 \\ 16+2a_2 = 0 \end{cases}$$

Resolvendo o sistema acima encontramos $a_0 = 36, a_1 = 0, a_2 = -8$ e $a_3 = 0$. Assim o polinômio minimal será $m_{i+\sqrt{5}} = x^4 - 8x^2 + 36$. Observe que as demais raízes de $m_{i+\sqrt{5}}$ são $i-\sqrt{5}$, $-i+\sqrt{5}$ e $-i-\sqrt{5}$.

Teorema 4.49. *(Lei da Torre) Se $K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n$ são subcorpos de $\mathbb{C}$, então $[K_n : K_0] = [K_n : K_{n-1}] \cdot [K_{n-1} : K_{n-2}] \cdot \ldots \cdot [K_2 : K_1] \cdot [K_1 : K_0]$.*

Demonstração. Sejam $K_0, K_1, \ldots, K_n$ subcorpos de $\mathbb{C}$. Vamos mostrar por indução que o teorema é válido.

Se $n = 1$, temos $[K_1 : K_0] = [K_1 : K_{1-1}] = [K_1 : K_0]$. Portanto para $n = 1$ vale o teorema.

Agora suponha que o teorema é válido para algum $n = k \in \mathbb{N}$. Assim

$$[K_k : K_0] = [K_k : K_{k-1}] \cdot \ldots \cdot [K_1 : K_0]$$

Precisamos mostrar que para $k+1$ o teorema é válido. Portanto, considere a extensão $[K_{k+1} : K_0]$. Pelo Teorema 4.47 sabemos que $[K_{k+1} : K_0] = [K_{k+1} : K_k] \cdot [K_k : K_0]$. Mas, pela hipótese de indução, $[K_k : K_0] = [K_k : K_{k-1}] \cdot \ldots \cdot [K_1 : K_0]$. Logo $[K_{k+1} : K_0] = [K_{k+1} : K_k] \cdot [K_k : K_0] = [K_{k+1} : K_k] \cdot [K_k : K_{k-1}] \cdot \ldots \cdot [K_1 : K_0]$. Portanto o teorema é válido para qualquer $n \in \mathbb{N}$. □

Exemplo 4.50. *A recíproca do Item i) da Proposição 4.45 só é verdadeira se $L : K$ é uma extensão algébrica e além disso, existe um número finito de elementos algébricos $\alpha_1, \ldots, \alpha_n \in L$ tais que $L = K[\alpha_1, \ldots, \alpha_n]$. Equivalentemente, $L : K$ será finita se existir $\alpha_1, \ldots \alpha_n \in L$ algébricos sobre K tais que $L = K[\alpha_1, \ldots, \alpha_n]$.*

De fato, se $L : K$ é uma extensão algébrica e $L = K[\alpha_1, \ldots, \alpha_n]$, temos $K \subseteq K[\alpha_1] \subseteq K[\alpha_1, \alpha_2] \subseteq \ldots \subseteq K[\alpha_1, \ldots, \alpha_{n-1}] \subseteq K[\alpha_1, \ldots, \alpha_n] = L$. Assim, pelo Teorema 4.49, segue que $[L : K] = [K[\alpha_1, \ldots, \alpha_n] : K] = [K[\alpha_1, \ldots, \alpha_n] : [K[\alpha_1, \ldots, \alpha_{n-1}]] \cdot [K[\alpha_1, \ldots, \alpha_{n-1}] : K[\alpha_1, \ldots, \alpha_{n-2}] \cdot \ldots \cdot [K[\alpha_1, \alpha_2] : K[\alpha_1]] \cdot [K[\alpha_1] : K]$. Mas $[K[\alpha_1, \ldots, \alpha_n] : [K[\alpha_1, \ldots, \alpha_{n-1}]]$, $[K[\alpha_1, \ldots, \alpha_{n-1}] : K[\alpha_1, \ldots, \alpha_{n-2}], \ldots, [K[\alpha_1, \alpha_2] : K[\alpha_1]], [K[\alpha_1] : K] \in \mathbb{N}$, segue que $[K[\alpha_1, \ldots, \alpha_n] : [K[\alpha_1, \ldots, \alpha_{n-1}]] \cdot [K[\alpha_1, \ldots, \alpha_{n-1}] : K[\alpha_1, \ldots, \alpha_{n-2}] \cdot \ldots \cdot [K[\alpha_1, \alpha_2] : K[\alpha_1]] \cdot [K[\alpha_1] : K] \in \mathbb{N}$, portanto a extensão $[L : K]$ é finita.

Proposição 4.51. *Se $M : L$ e $L : K$ são extensões algébricas, então $M : K$ também será uma extensão algébrica.*

Demonstração. Seja $\alpha \in M$ um elemento qualquer. Vamos mostrar que α é algébrico sobre K.

Como por hipótese $M : L$ é uma extensão algébrica, sabemos que existe $f(x) \in L[x]$ tal que $f(\alpha) = 0$. Suponha que $f(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + a_n x^n$, com $a_i \in L \ \forall \ i = 0, \ldots, n$. Agora, considere a extensão $L' = K[a_0, \ldots, a_n]$. A extensão $L' : K$ é finita, pois adjuntamos uma quantidade finita de elementos algébricos (observe que $a_0, \ldots, a_n$ são algébricos sobre K pois por hipótese $L : K$ é uma extensão algébrica). Além disso, $L'[\alpha] : L'$ é uma extensão finita, já que α é algébrico sobre L'. Portanto $[L'[\alpha] : L'] \cdot [L' : K] < \infty$ o que implica que $[L'[\alpha] : K] < \infty$, obtendo assim que $L'[\alpha] : K$ é uma extensão finita. Pelo Item i) da Proposição 4.45 segue que $L'[\alpha] : K$ é uma extensão algébrica, assim todos os elementos de $L'[\alpha]$ são algébricos sobre K, inclusive α. Como α é um elemento qualquer de M, podemos concluir que $M : K$ é uma extensão algébrica. □

Vamos apresentar um contraexemplo para a recíproca do Item i) da Proposição 4.45.

Considere a extensão $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots] : \mathbb{Q}$.

Primeiro, vamos mostrar que $[\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots, \sqrt{p_n}] : \mathbb{Q}] = 2^n$, em que p_n denota o n-ésimo número primo. Para isso, vamos mostrar por indução que $B_n = \{\sqrt{p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}} \mid (e_1, \ldots, e_n) \in \{0, 1\}^n\}$ é uma base para $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots, \sqrt{p_n}]$ como $\mathbb{Q}$-espaço vetorial.

Se $n = 1$, já vimos no Exemplo 4.41 que $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2 = 2^1$. Suponha agora que vale para $n-1$, ou seja, $B_{n-1} = \{\sqrt{p_1^{e_1} \cdot \ldots \cdot p_{n-1}^{e_{n-1}}} \mid (e_1, \ldots, e_{n-1}) \in \{0, 1\}^{n-1}\}$ é base para

$\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5},\ldots,\sqrt{p_{n-1}}]$ visto como $\mathbb{Q}$-espaço vetorial. Vamos mostrar que B_n é base para $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5},\ldots,\sqrt{p_n}]$.

Observe que $B_n = B_{n-1} \cup \sqrt{p_n}\cdot B_{n-1}$ e $B_{n-1} \cap \sqrt{p_n}\cdot B_{n-1} = \varnothing$. Vamos primeiramente mostrar que B_n é L.I, assim considere $\sum_{i=1}^{m} q_i x_i = 0$, com $x_i \in B_n$ e $q_i \in \mathbb{Q}$, $\forall\ i = 1,\ldots,m$. Como cada $x_i \in B_n$, $x_i = \sqrt{p_1^{e_{1_i}} \cdot \ldots \cdot p_n^{e_{n_i}}}$, com $(e_{1_i},\ldots e_{n_i}) \in \{0,1\}^n$.

Para $e_{n_i} = 1$, podemos reordenar os termos e reescrever $x_i = \sqrt{p_n}\cdot\sqrt{p_1^{e_{1_i}} \cdot \ldots \cdot p_n^{e_{n-1_i}}}$. Assim:

$$\begin{aligned}
0 = \sum_{i=1}^{m} q_i x_i &= \sum_{i=1}^{k} q_i \cdot \sqrt{p_n}\cdot x_i^{'} + \sum_{i=k}^{m} q_i x_i^{''} \qquad x_i^{'}, x_i^{''} \in B_{n-1}\ \forall\ i = 1,\ldots,m \\
&= \sqrt{p_n}\cdot\sum_{i=1}^{k} q_i \cdot x_i^{'} + \sum_{i=k}^{m} q_i x_i^{''} \qquad x_i^{'}, x_i^{''} \in B_{n-1}\ \forall\ i = 1,\ldots,m \\
\Rightarrow \sqrt{p_n} &= \frac{-\sum_{i=k}^{m} q_i x_i^{''}}{\sum_{i=1}^{k} q_i \cdot x_i^{'}} \in \mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5},\ldots,\sqrt{p_{n-1}}]
\end{aligned}$$

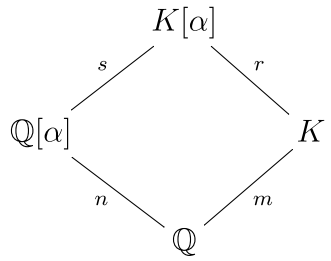
Como $\sqrt{p_n} \notin \mathbb{Q}[\sqrt{2},\sqrt{3},\ldots,\sqrt{p_{n-1}}]$, concluímos que $\sum_{i=1}^{k} q_i \cdot x_i^{'} = 0$ e $\sum_{i=k}^{m} q_i x_i^{''} = 0$. Como $x_i^{'}$ e $x_i^{''} \in B_{n-1}$, e por hipótese de indução, B_{n-1} é uma base, concluímos que $q_i = 0\ \forall\ i = 1,\ldots,m$. Portanto B_n é um conjunto linearmente independente. Agora, resta ver que B_n gera $\mathbb{Q}[\sqrt{2},\sqrt{3},\ldots,\sqrt{p_n}]$. Como $\mathbb{Q}[\sqrt{2},\sqrt{3},\ldots,\sqrt{p_n}] = \mathbb{Q}[\sqrt{2},\sqrt{3},\ldots,\sqrt{p_{n-1}}][\sqrt{p_n}]$, dado $x \in \mathbb{Q}[\sqrt{2},\sqrt{3},\ldots,\sqrt{p_n}]$, podemos escrever $x = a + b\sqrt{p_n}$ com $a, b \in \mathbb{Q}[\sqrt{2},\ldots,\sqrt{p_{n-1}}]$. Logo, se $a = \sum_{i=1}^{r} u_i x_i$ e $b = \sum_{i=1}^{s} v_i x_i$ com $x_i \in B_{n-1}$, temos $x = \sum_{i=1}^{r} u_i x_i + \sum_{i=1}^{s} v_i x_i \cdot \sqrt{p_n} = \sum_{i=1}^{max\{r,s\}} u_i x_i + v_i x_i^{'} \in \mathbb{Q}[\sqrt{2},\ldots,\sqrt{p_n}]$, onde $x' \in B_n$. Portanto B_n gera $\mathbb{Q}[\sqrt{2},\sqrt{3},\ldots,\sqrt{p_n}]$ e assim é uma base para $\mathbb{Q}[\sqrt{2},\ldots,\sqrt{p_n}]$ com 2^n elementos, como queríamos. Observe que se $n \to \infty$, B_n terá infinitos elementos.

Agora, vamos mostrar que a extensão $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5},\ldots]$ é algébrica. Seja $x \in \mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5},\ldots]$, assim $x = \sum_{i=0}^{n} q_i\sqrt{m_i}$ onde m_i não são quadrados perfeitos. Como cada $\sqrt{m_i}$ é algébrico sobre $\mathbb{Q}$, pois é raiz do polinômio $x^2 - m_i$, segue que x é algébrico sobre $\mathbb{Q}$ (pois é soma de elementos algébricos). Como x é arbitrário, segue que a extensão $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5},\ldots]$ é algébrica.

Portanto $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5},\ldots]$ é uma extensão algébrica e como possui uma base que não é finita, concluímos que não é uma extensão finita.

Corolário 4.52. *Seja $K \supseteq \mathbb{Q}$ uma extensão tal que $[K : \mathbb{Q}] = m$ e seja $p(x) \in \mathbb{Q}[x]$ um polinômio irredutível de grau n. Se m e n são primos entre si, então $p(x)$ é um polinômio irredutível sobre K.*

Demonstração. Seja $\alpha \in \mathbb{C}$ uma raiz de $p(x)$. Considere os corpos $\mathbb{Q}[\alpha] \subset K[\alpha]$ e suponhamos que $[K[\alpha] : K] = r$ e $[K[\alpha] : \mathbb{Q}[\alpha]] = s$. Como $\partial p = n$ e $p(x) \in \mathbb{Q}[x]$ é irredutível sobre $\mathbb{Q}$, segue que $[\mathbb{Q}[\alpha] : \mathbb{Q}] = n$.



Vamos mostrar que $r = n$. Como n é o grau do polinômio irredutível $p(x)$ sobre $\mathbb{Q}$, podemos ter que, ao considerar a extensão $K \supseteq \mathbb{Q}$, o polinômio $p(x)$ continue sendo irredutível, assim $p(x)$ continuará sendo o polinômio minimal da extensão $K[\alpha] : K$, logo $[K[\alpha] : K] = r = n$.

Mas, se $p(x)$ for redutível sobre K, existirão polinômios $f(x), g(x) \in K[x]$ tais que $p(x) = f(x) \cdot g(x)$. Como α é raiz de $p(x)$, α será raiz de $f(x)$ ou $g(x)$, e dessa forma o polinômio minimal associado a extensão $K[\alpha] : K$ terá grau menor que $p(x)$, ou seja, $r < n$. Em ambos os casos, o grau da extensão $[K[\alpha] : K] = r$ é no máximo n.

Pelo Teorema 4.47, segue que $s \cdot n = r \cdot m$. Como, por hipótese, m e n são primos entre si, concluímos que $n \mid r$, assim $n \leq r$. Como $n \leq r$ e $r \leq n$ segue que $r = n$, donde concluímos que $p(x)$ é irredutível sobre K. □

4.4 Extensões galoisianas, normais e separáveis

Estamos quase findando este capítulo e nesta seção falaremos sobre extensões normais, galoisianas e separáveis. Estas extensões são muito interessantes, e serão essenciais para a compreensão da teoria desenvolvida por Galois.

Definição 4.53. *Seja $L : K$ uma extensão finita. Se existe $f(x) \in K[x]$ tal que $L = Gal(f(x), K)$ a extensão $L : K$ é chamada **extensão galoisiana**.*

Definição 4.54. *Uma extensão $L : K$ é dita **normal** se todo polinômio irredutível sobre K que tem pelo menos uma raiz em L, tem todas as raízes em L.*

Em outras palavras, se $L : K$ é normal então os polinômios irredutíveis com coeficientes em K ou não têm raízes em L ou têm todas as raízes em L.

Por exemplo, a extensão $\mathbb{C} : \mathbb{R}$ é normal, visto que todo polinômio com coeficientes reais se decompõe em $\mathbb{C}$. Já a extensão $\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}$ não é normal, já que $u \notin \mathbb{Q}[\sqrt[3]{2}]$.

Teorema 4.55. *Uma extensão de corpos $L : K$ é normal e finita se e somente se L é um corpo de decomposição para algum polinômio $f(x)$ sobre K.*

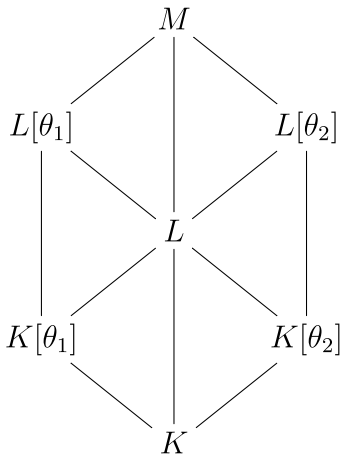
Demonstração. Vamos supor $L : K$ é uma extensão normal e finita. Como L é finita, segue através do Exemplo 4.50 que $L = K[\alpha_1, \ldots, \alpha_n]$, com α_i algébrico sobre K para todo $i = 1, .., n$. Além disso, seja $m_i(x)$ o polinômio minimal de α_i sobre K, e considere o polinômio $f(x) = m_1(x) \cdot \ldots \cdot m_n(x) \in K[x]$. Como cada m_i é irredutível sobre K e tem uma raiz $\alpha_i \in L$, pela hipótese de L ser uma extensão normal, segue que cada m_i possui todas as raízes em L, e assim m_i se divide sobre L. Dessa forma f se divide sobre L, e como L é gerado por K e pelas raízes de $f(x)$, podemos concluir que L é o corpo de decomposição de $f(x)$ sobre K.

Reciprocamente, vamos supor que L é o corpo de decomposição de um polinômio $g(x) \in K[x]$, ou seja, L é o menor subcorpo que contém K e todas as raízes de $g(x)$, assim $L = K[\alpha_1, \ldots, \alpha_n]$. Como cada α_i é algébrico sobre K, L é uma extensão algébrica, e pelo Exemplo 4.50 segue que L é uma extensão finita. Agora, resta mostrar que L é uma extensão normal.

Assim, seja $f(x) \in K[x]$ um polinômio irredutível sobre K com uma raiz θ_1 em L. Vamos mostrar que as demais raízes de $f(x)$ também estão em L.

Seja $M \supseteq L$ o corpo de decomposição do polinômio $f(x) \cdot g(x)$ sobre K. Suponha que θ_2 é uma raiz de $f(x)$ em M. Como $f(x)$ é irredutível sobre K, $f(x)$ é o polinômio minimal de θ_1 e θ_2 sobre K. Vamos mostrar que se $[L[\theta_1] : L] = 1$ então $[L[\theta_2] : L] = 1$.

Considere o seguinte diagrama:



Observe que há duas torres importantes:

$$K \subseteq K[\theta_1] \subseteq L[\theta_1] \subseteq M \qquad \text{e} \qquad K \subseteq K[\theta_2] \subseteq L[\theta_2] \subseteq M$$

Além disso, $K \subseteq K[\theta_1]$, $K \subseteq K[\theta_2]$, $L \subseteq L[\theta_1]$, $L \subseteq L[\theta_2]$ e $K \subseteq L \subseteq M$. Assim, pela lei da torre:

$$[L[\theta_1] : L] \cdot [L : K] = [L[\theta_1] : K[\theta_1]] \cdot [K[\theta_1] : K] \tag{4.1}$$

$$[L[\theta_2] : L] \cdot [L : K] = [L[\theta_2] : K[\theta_2]] \cdot [K[\theta_2] : K] \tag{4.2}$$

Como θ_1 e θ_2 são raízes do mesmo polinômio irredutível $f(x)$ segue pelo Corolário 4.31 que $K[\theta_1] \simeq K[\theta_2]$. Portanto $[K\theta_1] : K] = [K[\theta_2] : K]$. Ademais, como L é o corpo de decomposição de $g(x)$ sobre K, segue que $L[\theta_1]$ é o corpo de decomposição de $g(x)$ sobre

$K[\theta_1]$. Da mesma forma afirmamos que $L[\theta_2]$ é o corpo de decomposição de $g(x)$ sobre $K[\theta_2]$. Porém como $K[\theta_1] \simeq K[\theta_2]$, podemos concluir que $[L[\theta_1] : K[\theta_1]] = [L[\theta_2] : K[\theta_2]]$.

Portanto, através das Equações 4.1 e 4.2 obtemos:

$$\begin{aligned} & [L[\theta_1] : K[\theta_1]] \cdot [K[\theta_1] : K] = [L[\theta_2] : K[\theta_2]] \cdot [K[\theta_2] : K] \\ \Rightarrow \quad & [L[\theta_1] : L] \cdot [L : K] = [L[\theta_2] : L] \cdot [L : K] \\ \Rightarrow \quad & [L[\theta_1] : L] = [L[\theta_2] : L] \end{aligned}$$

Agora, se $\theta_1 \in L$, segue pela Proposição 4.44 que $[L[\theta_1] : L] = 1$. Mas como $[L[\theta_1] : L] = [L[\theta_2] : L]$, podemos concluir que $[L[\theta_2] : L] = 1$ e assim $\theta_2 \in L$. Como θ_1 e θ_2 são raízes quaisquer de $f(x)$ concluímos que se uma raiz de $f(x) \in L$ então todas as raízes de $f(x)$ estão em L. Portanto L é uma extensão normal sobre K, como queríamos. □

Corolário 4.56. *Se $L : K$ é uma extensão normal e finita, e M é um corpo intermediário entre L e K então a extensão $L : M$ é normal.*

Demonstração. Suponha que $L : K$ é uma extensão normal e finita. Assim, pelo Teorema 4.55 existe $f(x) \in K[x]$ tal que $L = Gal(f(x), K)$. Como $f(x) \in K[x] \subseteq M[x]$, segue que $L = Gal(f(x), M)$. Portanto, novamente pelo Teorema 4.55, concluímos que $L : M$ é normal. □

Agora, vamos apresentar uma definição importante:

Definição 4.57. *Um polinômio irredutível $f(x) \in K[x]$ é dito **separável** sobre K se ele não tem raízes múltiplas em $\mathbb{C}$, ou equivalentemente, em um corpo de decomposição, ou seja*

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

onde $\alpha_i \neq \alpha_j \ \forall \ i \neq j$. Se $f(x)$ não é separável dizemos que $f(x)$ é inseparável.

Exemplo 4.58. *Por exemplo, considere o polinômio $f(x) = x^2 + 1$. Dizemos que $f(x)$ é separável sobre $\mathbb{Q}$, pois pode ser escrito como $f(x) = (x + i)(x - i)$.*

Exemplo 4.59. *O polinômio $f(x) = x^4 - 4x^2 + 4$ é inseparável sobre $\mathbb{Q}$, já que $f(x) = (x^2 - 2)^2$, que não pode ser expresso da forma $f(x) = (x - \alpha_1)(x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n)$, com $\alpha_i \neq \alpha_j$ para $i \neq j$.*

Proposição 4.60. *Se K é um subcorpo de $\mathbb{C}$, então todo polinômio irredutível sobre K é separável.*

Demonstração. Sabemos pelo Corolário 4.36 que um polinômio $f(x) \in K[x]$ é inseparável se e somente se $f(x)$ e $f'(x)$ possuem um fator em comum de grau maior ou igual a 1. Suponha por absurdo que $f(x)$ seja inseparável, assim o fator em comum entre $f(x)$ e $f'(x)$ é o próprio $f(x)$, já que $f(x)$ é irredutível. Mas como $\partial f' < \partial f$, o único múltiplo de $f(x)$ tendo grau menor é 0, assim $f'(x) \equiv 0$. Portanto como $f'(x) = 0$ temos $f(x) = c \in K$, mas assim $f(x)$ e $f'(x)$ não possuem um fator em comum. Absurdo. Portanto $f(x)$ é separável sobre K. □

Através da definição de polinômio separável, podemos estender essa noção:

Definição 4.61. *Se $L : K$ é uma extensão de corpos, então $\alpha \in L$ é* ***separável*** *sobre K se seu polinômio minimal é separável sobre K.*

Definição 4.62. *Se $L : K$ é uma extensão algébrica, dizemos que $L : K$ é uma* ***extensão separável*** *se todo $\alpha \in L$ é separável sobre K.*

Lema 4.63. *Seja $L : K$ uma extensão algébrica separável e M um corpo intermediário. Então $L : M$ e $M : K$ são separáveis.*

Demonstração. Seja $\alpha \in M$. Como $M \subseteq L$, então $\alpha \in L$ e como $L : K$ é separável segue que α é um elemento separável, portanto a extensão $M : K$ é separável.

Agora, resta mostrar que $L : M$ é separável. Assim, seja m_{α_M} e m_{α_K} os polinômios minimais associados as extensões $L : M$ e $L : K$. Como $K \subseteq M$, temos que $m_{\alpha_K} \in M[x]$. Além disso, $m_{\alpha_K}(\alpha) = 0$, portanto segue que m_{α_K} é um múltiplo de m_{α_M}. Mas como m_{α_K} é um produto de fatores lineares, já que a extensão $L : K$ é separável, segue que m_{α_M} também será um produto de fatores lineares e portanto a extensão $L : M$ é separável. □

Corolário 4.64. *Seja $L : K$ uma extensão algébrica de corpos de $\mathbb{C}$. Então $L : K$ é separável.*

5 Teoria de Galois

Estamos em condição de estabelecer propriedades fundamentais sobre a correspondência de Galois, que relaciona as extensões de corpos e os grupos de Galois, auge desta teoria. Desta forma, apresentaremos neste capítulo as peças restantes deste lindo quebra cabeça, a fim de montá-lo através do teorema fundamental de Galois. Terminaremos apresentando vários exemplos da aplicação do teorema.

5.1 Adentrando à teoria de Galois

Nesta seção apresentaremos a ideia inicial da teoria de Galois, comentando a respeito dos corpos fixos e grupos de Galois, bem como suas propriedades.

Definição 5.1. *Seja $L : K$ uma extensão de corpos, tal que K é um subcorpo de um corpo L de $\mathbb{C}$. Um automorfismo $\sigma : L \to L$ é chamado* ***K-automorfismo de*** *L se $\sigma(k) = k \ \forall \ k \in K$, ou seja, se σ fixa os elementos de K.*

Teorema 5.2. *Se $L : K$ é uma extensão de corpos, então o conjunto $Aut_K L$ dos $K-$auto morfismos de L formam um grupo com a operação de composição de funções.*

Demonstração. Sejam α e β $K-$automorfismos de L. Vamos mostrar que $\alpha \circ \beta$ também é um $K-$automorfismo de L. De fato, dados $x, y \in L$, temos $(\alpha \circ \beta)(x+y) = \alpha(\beta(x+y)) = \alpha(\beta(x) + \beta(y)) = \alpha(\beta(x)) + \alpha(\beta(y)) = (\alpha \circ \beta)(x) + (\alpha \circ \beta)(y)$. Portanto $\alpha \circ \beta$ também é um automorfismo de L. Agora, dado $k \in K$, temos $(\alpha \circ \beta)(k) = \alpha(\beta(k)) = \alpha(k) = k$. Logo $\alpha \circ \beta$ é um $K-$automorfismo de L, assim $Aut_K L$ é fechado para a operação.

Dados $\alpha, \beta, \delta \in Aut_K L$ e $l \in L$, temos que $[(\alpha \circ \beta) \circ \delta](l) = (\alpha \circ \beta)(\delta(l)) = \alpha(\beta(\delta(l))) = \alpha \circ (\beta \circ \delta)(l) = [\alpha \circ (\beta \circ \delta)](l)$, portanto a operação $\circ$ é associativa. Além disso, a função identidade $Id : L \to L$ também é um $K-$automorfismo de L, visto que $Id(k) = k \ \forall k \in K$. A função identidade é o elemento neutro do grupo.

Dado $\alpha \in Aut_K L$, como α é bijeção, existe $\alpha^{-1} : L \to L$ e α^{-1} também é um automorfismo de L. Dado $k \in K$, temos $k = (\alpha^{-1} \circ \alpha)(k) = \alpha^{-1}(\alpha(k)) = \alpha^{-1}(k)$. Portanto para todo $\alpha \in Aut_K L$, existe $\alpha^{-1} \in Aut_K L$ tal que $\alpha \circ \alpha^{-1} = \alpha^{-1} \circ \alpha = Id$. Dessa forma concluímos que $Aut_K L$ é grupo com a operação composição de funções. □

Definição 5.3. *O* ***grupo de Galois*** *$\Gamma(L : K)$ de uma extensão $L : K$ é o grupo de todos os $K-$automorfismos de L com a operação de composição de funções.*

Exemplo 5.4. *Vamos calcular os $\mathbb{R}-$automorfismos de $\mathbb{C}$. Assim, suponha que $\sigma \in \Gamma(\mathbb{C} : \mathbb{R})$ e seja $j = \sigma(i)$, em que $i = \sqrt{-1}$. Então $j^2 = (\sigma(i))^2 = \sigma(i^2) = \sigma(-1) = -1$. Assim j é raiz do polinômio $f(x) = x^2 + 1$, portanto $j = \pm i$. Dado $a + bi \in \mathbb{C}$, com $a, b \in \mathbb{R}$ temos $\sigma(a + bi) = \sigma(a) + \sigma(b)\sigma(i) = a + bj$. Dessa forma há dois $\mathbb{R}-$automorfismos: $\sigma_1 : a + bi \mapsto a + bi$ e $\sigma_2 : a + bi \mapsto a - bi$.*

Observe que $\sigma_1 = Id$ e σ_2 é a função conjugado. Temos ainda que $\sigma_2^2 = Id$, assim $\Gamma(\mathbb{C} : \mathbb{R}) = \{Id = \sigma_1, \sigma_2\} \simeq S_2$.

Exemplo 5.5. *Vamos calcular os $\mathbb{Q}-$automorfismos da extensão $\mathbb{Q}[\sqrt[3]{2}]$. Dado $\alpha \in \Gamma(\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q})$, se $j = \alpha(\sqrt[3]{2})$, temos $j^3 = (\alpha(\sqrt[3]{2}))^3 = \alpha((\sqrt[3]{2})^3) = \alpha(2) = 2$. Portanto j é raiz do polinômio $f(x) = x^3 - 2$. Logo $j = \sqrt[3]{2}$, $j = \sqrt[3]{2}u$ ou $j = \sqrt[3]{2}u^2$, em que u denota a raiz cúbica da unidade. Mas $u \notin \mathbb{Q}[\sqrt[3]{2}]$, portanto o único automorfismo possível é $j = \alpha(\sqrt[3]{2}) = \sqrt[3]{2}$. Observe que neste caso $\alpha = Id$ e dessa forma $\Gamma(\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}) = \{Id\}$.*

Galois descobriu que sob certas condições, existe uma correspondência biunívoca entre os subgrupos de $\Gamma(L : K)$ e os subcorpos de L que contém K. De modo geral, essa correspondência reverte inclusões: subcorpos "maiores" correspondem a grupos "menores", e vice-versa. Vamos explicar melhor como isso ocorre.

Para cada corpo intermediário M com $K \subseteq M \subseteq L$ definimos o grupo $M^* = \Gamma(L : M)$ de todos os $M-$automorfismos de L. Assim $K^* = \Gamma(L : K)$ é todo o grupo de Galois e $L^* = \Gamma(L : L) = \{Id\}$, já que o único automorfismo de L que fixa todos os elementos de L é a própria função identidade.

Note que se $M \subseteq N$, então $M^* \supseteq N^*$. De fato, basta notar que todos os automorfismos de L que fixam os elementos de N certamente fixam os elementos de M, portanto $\forall\, \sigma \in N^*$ tem-se $\sigma \in M^*$.

Agora, a cada subgrupo H de $\Gamma(L : K)$, associamos o conjunto $H^\dagger = \{x \in L \mid \sigma(x) = x,\ \forall\ \sigma \in H\}$. Observe que este conjunto é um corpo intermediário, como provaremos a seguir.

Lema 5.6. *Se H é um subgrupo de $\Gamma(L : K)$, então $H^\dagger$ é um subcorpo de L contendo K.*

Demonstração. Dados $a, b \in H^\dagger$ e $\sigma \in H$, temos $\sigma(a) = a$ e $\sigma(b) = b$. Logo $\sigma(a - b) = \sigma(a) - \sigma(b) = a - b$, e assim σ fixa $a - b$. Como σ é qualquer, concluímos que $a - b \in H^\dagger$. Da mesma forma, tem-se $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b) = a \cdot b$, portanto $a \cdot b \in H^\dagger$.

Agora, como $1 \in K$ e $\sigma(1) = 1\ \forall\ \sigma \in H$, temos que $1 \in H^\dagger$. Assim, se $a \in H^\dagger$ é tal que $a \neq 0$, então $a \cdot a^{-1} = 1 \Rightarrow \sigma(a \cdot a^{-1}) = \sigma(1) \Rightarrow \sigma(a) \cdot \sigma(a^{-1}) = 1 \Rightarrow a \cdot \sigma(a^{-1}) = 1 \Rightarrow a^{-1} \cdot a \cdot \sigma(a^{-1}) = a^{-1} \cdot 1 \Rightarrow \sigma(a^{-1}) = a^{-1} \Rightarrow a^{-1} \in H^\dagger$.

Logo $H^\dagger$ é subcorpo de L. Além disso, para todo $k \in K$ e para todo $\sigma \in H$ tem-se $\sigma(k) = k$, portanto $k \in H^\dagger$ e assim $K \subseteq H^\dagger$. □

Definição 5.7. *O corpo $H^\dagger$ é chamado* ***corpo fixo*** *de H.*

Assim como a aplicação $*$, a aplicação $\dagger$ também é uma inclusão reversa, isto é, se $H \subseteq G$, então $H^\dagger \supseteq G^\dagger$. De fato, basta ver que todos os elementos de $G^\dagger$ são fixados pelos automorfismos de G, porém como $H \subseteq G$, os elementos de $G^\dagger$ são fixados pelos automorfismos de H também e dessa forma $G^\dagger \subseteq H^\dagger$.

Proposição 5.8. *Sejam M um corpo intermediário de uma extensão $L : K$ e H um subgrupo de $\Gamma(L : K)$, então $M \subseteq M^{*\dagger}$ e $H \subseteq H^{\dagger *}$.*

Demonstração. Temos $M^{*\dagger} = (M^*)^\dagger = \{x \in L \mid \sigma(x) = x\ \forall\ \sigma \in M^*\}$.

Agora, seja $x \in M$ e $\sigma \in M^* = \Gamma(L : M)$ um $M-$automorfismo de L qualquer. Como $\sigma(x) = x$ para todo $x \in M$ (já que σ é um $M-$automorfismo) e como σ é qualquer, concluímos que $x \in M^{*\dagger} = \{x \in L \mid \sigma(x) = x \ \forall \ \sigma \in M^*\}$. Portanto $M \subseteq M^{*\dagger}$.

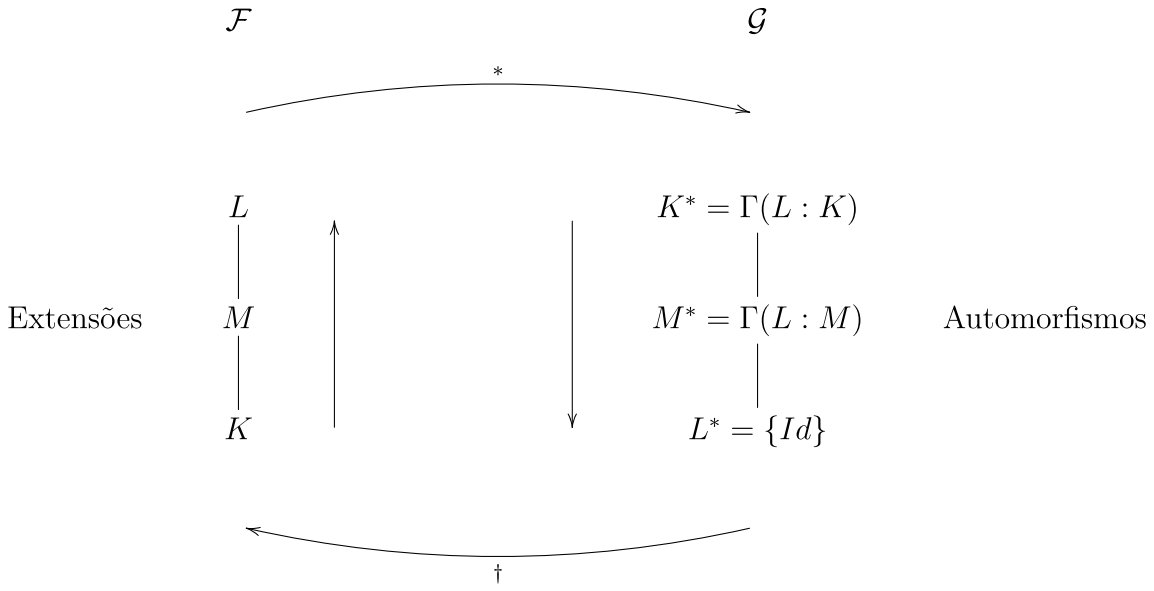
Além disso, temos $H^{\dagger *} = \Gamma(L : H^\dagger)$ o conjunto de todos os $H^\dagger-$automorfismos de L. Seja $\sigma \in H$ um $K-$automorfismo de L qualquer. Sabemos que $H^\dagger = \{x \in L \mid \sigma(x) = x \ \forall \ \sigma \in H\}$, ou seja, são todos os elementos $x \in L$ que são fixados por todos os $\sigma \in H$. Mas, pela própria construção de $H^\dagger$, σ fixa os elementos de $H^\dagger$, e portanto σ é um $H^\dagger-$automorfismo de L. Logo $\sigma \in H^{\dagger *}$ e assim $H \subseteq H^{\dagger *}$. □

Se denotarmos $\mathcal{F}$ como o conjunto dos corpos intermediários e $\mathcal{G}$ como o conjunto dos subgrupos do grupo de Galois, temos definidas duas aplicações:

$$* : \mathcal{F} \to \mathcal{G} \qquad\qquad \dagger : \mathcal{G} \to \mathcal{F}$$

que invertem as inclusões e satisfazem as continências $M \subseteq M^{*\dagger}$ e $H \subseteq H^{\dagger *}$.

As duas funções $*$ e $\dagger$ constituem a correspondência de Galois entre $\mathcal{F}$ e $\mathcal{G}$.



Teorema 5.9. *Seja G um subgrupo finito do grupo de automorfismos de um corpo K, e seja K_0 o corpo fixo de G. Então $[K : K_0] = o(G)$.*

Demonstração. A demonstração pode ser encontrada em [STEWART I, 2015], p. 120. □

5.2 Automorfismos de corpos

Nesta seção apresentaremos conceitos e teoremas importantes sobre os automorfismos de corpos. Falaremos também sobre o fecho normal, uma ferramenta que permite construir extensões normais a partir de extensões finitas. Além disso, estaremos trabalhando com corpos com característica zero, onde a separabilidade é automática.

Definição 5.10. *Suponha que K é um subcorpo dos subcorpos M e L de $\mathbb{C}$. Assim, um $K-$**monomorfismo de** M **em** L é um monomorfismo $\phi : M \to L$ tal que $\phi(k) = k$, $\forall\, k \in K$.*

Observe que se $K \subseteq M \subseteq L$ e $\phi : L \to L$ é um $K-$automorfismo então $\phi_{|M} : M \to L$ é um $K-$monomorfismo.

Exemplo 5.11. *Suponha que $K = \mathbb{Q}$, $M = \mathbb{Q}[\alpha]$ em que $\alpha = \sqrt[3]{2}$ e $L = \mathbb{C}$. Podemos definir um $K-$monomorfismo $\phi : M \to L$ por $\phi(\alpha) = \alpha u$, em que u é a raiz cúbica da unidade. Como todo elemento de M é da forma $a + b\alpha + c\alpha^2$, em que $a, b, c \in \mathbb{Q}$, temos $\phi(a+b\alpha+c\alpha^2) = a+b\alpha u+c\alpha^2u^2$. Além disso, como α e αu são raízes do mesmo polinômio irredutível $f(x) = x^3 - 2$, o Corolário 4.31 nos garante que ϕ é um monomorfismo.*

Note que há ainda dois $K-$monomorfismos: $\sigma : M \to L$ tal que $\sigma(\alpha) = \alpha u^2$ e $Id : M \to L$, a função identidade.

O próximo teorema nos auxiliará a construir $K-$automorfismos.

Teorema 5.12. *Suponha que $L : K$ é uma extensão normal e finita, e que $K \subseteq M \subseteq L$. Seja τ um $K-$monomorfismo de M em L. Então existe um $K-$automorfismo σ de L tal que $\sigma_{|M} = \tau$.*

Demonstração. Pelo Teorema 4.55 sabemos que se $L : K$ é uma extensão normal e finita, então $L : K$ é o corpo de decomposição de algum polinômio $f(x) \in K[x]$. Como $K \subseteq M$, L também é o corpo de decomposição de $f(x)$ sobre M. Agora, como τ é um $K-$monomorfismo de M em L, segue que L é o corpo de decomposição de $\tau(f)$ sobre $\tau(M)$. Mas $\tau_{|K} = Id$, portanto $\tau(f) = f$. Assim, obtemos o diagrama:

$$\begin{array}{ccc} M & \xrightarrow{\tau} & L \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \sigma} \\ \tau(M) & \longrightarrow & L \end{array}$$

Precisamos encontrar tal σ. Para isso, pelo Teorema 4.39, sabemos que existe um isomorfismo $\sigma : L \to L$ tal que $\sigma_{|M} = \tau$. Deste modo, σ é um automorfismo de L, e como $\sigma_{|K} = Id$, σ é um $K-$automorfismo de L. □

Proposição 5.13. *Suponhamos que $L : K$ seja uma extensão normal e finita, e α, β sejam as raízes em L de um polinômio irredutível $p(x) \in K[x]$. Então existe um $K-$automorfismo σ de L tal que $\sigma(\alpha) = \beta$.*

Demonstração. Pelo corolário 4.31, sabemos que $K[\alpha] \simeq K[\beta]$, ou seja, existe um isomorfismo $\tau : K[\alpha] \to K[\beta]$ de modo que $\tau_{|K} = Id$ e $\tau(\alpha) = \beta$. Como $K \subseteq K[\alpha] \subseteq L$, pelo teorema anterior podemos estender τ a um $K-$automorfismo σ de L. □

5.2.1 Fecho normal

Apresentaremos nessa subseção o fecho normal, que nos auxiliará a recuperar a normalidade de uma extensão, tornando-a, se preciso, maior.

Definição 5.14. *Seja L uma extensão finita de K. Um* ***fecho normal de*** *$L : K$ é uma extensão N de L, tal que as condições abaixo sejam satisfeitas:*

i) $N : K$ *é normal;*

ii) Se $L \subseteq M \subseteq N$ *e* $M : K$ *é normal, então* $M = N$.

Assim, N é a menor extensão de L que é normal sobre K.

Observe que o fecho normal tem propriedades muito interessantes. Além disso, o próximo teorema nos mostra que sobre $\mathbb{C}$, ele é único.

Teorema 5.15. *Se $L : K$ é uma extensão finita em $\mathbb{C}$, então existe um único fecho normal $N \subseteq \mathbb{C}$ de $L : K$, que é uma extensão finita de K.*

Demonstração. Como $L : K$ é uma extensão finita, seja $\{x_1, \ldots, x_n\} \subset L$ uma base para a extensão $L : K$. Seja m_j o polinômio minimal de x_j sobre K e considere $f = m_1 \cdot m_2 \cdot \ldots \cdot m_n$ sobre L. Se N é o corpo de decomposição de f sobre L, então N também é o corpo de decomposição de f sobre K. Portanto $N : K$ também é uma extensão normal e finita pelo Teorema 4.55.

Suponha agora que exista uma extensão $P : K$ normal e $L \subseteq P \subseteq N$. Note que cada polinômio m_j tem uma raiz $x_j \in P \supseteq L$. Como P é normal sobre K, P contém todas as raízes de m_j e portanto f se decompõe em $P : K$. Mas N é o corpo de decomposição de f, portanto $P = N$. Logo N é o fecho normal de $L : K$.

Unicidade: Suponha agora que M e N sejam ambos fechos normais. O polinômio f acima se divide em M e N, então tanto M quanto N contém o corpo de decomposição Σ de f sobre K, assim $L \subseteq \Sigma \subseteq M$ e $L \subseteq \Sigma \subseteq N$. Como $\Sigma : K$ é normal e por hipótese M e N são fechos normais, concluímos que $\Sigma = M$ e $\Sigma = N$, logo $M = N$ e portanto o fecho normal é único. □

Exemplo 5.16. *Consideremos a extensão $\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}$. Essa extensão não é normal, visto que não possui todas as raízes do polinômio $f(x) = x^3 - 2$ (apenas $\alpha = \sqrt[3]{2} \in \mathbb{Q}[\sqrt[3]{2}]$). Se consideramos K como o corpo de decomposição para $x^3 - 2$ sobre $\mathbb{Q}$, contido em $\mathbb{C}$, teremos $K = \mathbb{Q}[\alpha, \alpha u, \alpha u^2]$, em que u é a raiz cúbica da unidade. Porém, observe que os elementos adjuntados neste caso são obtidos por meio de α e u, logo o corpo de decomposição de $f(x) = x^3 - 2$ é $\mathbb{Q}[\alpha, u]$, que é uma extensão normal, e portanto o fecho normal de $\mathbb{Q}[\alpha]$.*

Observe que no exemplo anterior obtivemos o fecho normal adicionando todas as raízes que faltavam. Além disso, fechos normais nos permitem estipular restrições na imagem de um monomorfismo.

Lema 5.17. *Suponhamos que $K \subseteq L \subseteq N \subseteq M$ onde $L : K$ é finita e N é o fecho normal de $L : K$. Seja τ qualquer $K-$monomorfismo de L em M. Então $\tau(L) \subseteq N$.*

Demonstração. Sejam $\alpha \in L$ e $m(x)$ o polinômio minimal de α sobre K. Então $m(\alpha) = 0$ e portanto $\tau(m(\alpha)) = \tau(0) = 0$. Mas $\tau(m(\alpha)) = m(\tau(\alpha))$ (se $m(x) = a_0 + a_1 x + \ldots + x^n$, temos $m(\alpha) = a_0 + a_1\alpha + \ldots + \alpha^n$, e como τ é um $K-$monomorfismo, segue que $\tau(m(\alpha)) = a_0 + a_1\tau(\alpha) + \ldots + \tau(\alpha)^n = m(\tau(\alpha))$). Como $\tau(m(\alpha)) = m(\tau(\alpha)) = 0$, concluímos que

$\tau(\alpha)$ é raiz de $m(x)$. Portanto como N é o fecho normal segue que $\tau(\alpha) \in N$. Como α é qualquer, concluímos que $\tau(L) \subseteq N$. □

O próximo teorema nos fornece uma caracterização para a normalidade:

Teorema 5.18. *Para uma extensão finita $L : K$ as afirmações a seguir são equivalentes:*

1. *$L : K$ é normal;*
2. *Existe uma extensão normal e finita $K \subseteq L \subseteq N$ tal que todo $K-$monomorfismo $\tau : L \to N$ é um $K-$automorfismo de L.*
3. *Para toda extensão finita M de K contendo L, todo K-monomorfismo $\tau : L \to M$ é um $K-$automorfismo de L.*

Demonstração. Vamos provar (1) $\Rightarrow$ (3) $\Rightarrow$ (2) $\Rightarrow$ (1).

(1) $\Rightarrow$ (3): Se $L : K$ é uma extensão normal, então L é o fecho normal de $L : K$, e portanto pelo Lema 5.17, para qualquer $K-$monomorfismo τ temos $\tau(L) \subseteq L$.

Como τ é uma função $K-$linear, definida em um espaço vetorial de dimensão finita L sobre K, e ainda um monomorfismo, segue que $\tau(L)$ tem a mesma dimensão de L, resultando em $\tau(L) = L$ e portanto τ é sobrejetora. Como τ já era monomorfismo, concluímos que τ é um $K-$automorfismo de L.

(3) $\Rightarrow$ (2) Seja N o fecho normal da extensão $L : K$. Por definição, $N : K$ é normal. Além disso, $N : K$ é finita, e por hipótese todo $K-$monomorfismo $\tau : L \to N$ é um $K-$automorfismo de L. Logo tem-se o desejado.

(2) $\Rightarrow$ (1): Suponha que $f(x)$ é um polinômio irredutível sobre $K[x]$, e α é uma raiz de $f(x)$ em L. Então como $N : K$ é uma extensão normal, sabemos que $f(x)$ se decompõe em N. Agora, se β é qualquer raiz de $f(x)$ em N, pela Proposição 5.13 existe um $K-$automorfismo σ de N tal que $\sigma(\alpha) = \beta$. Por hipótese, σ é um $K-$automorfismo de L, assim $\beta = \sigma(\alpha) \in \sigma(L) = L$. Portanto como β é uma raiz qualquer de $f(x)$ e se $\alpha \in L$ então $\beta \in L$, concluímos que $L : K$ é uma extensão normal. □

Teorema 5.19. *Suponhamos que $L : K$ seja uma extensão finita de grau n. Então existem precisamente n $K-$monomorfismos distintos de L no fecho normal N de $L : K$ e portanto, em qualquer extensão normal M de K contendo L.*

Demonstração. A demonstração será feita por indução sobre $[L : K]$.

Se $[L : K] = 1$, pela Proposição 4.44, sabemos que $L = K$. Assim todo $K-$monomorfismo é um $L-$monomorfismo, e como $\tau : L \to N$, concluímos que $\tau = Id$.

Suponha agora que $[L : K] > 1$. Seja $\alpha \in L - K$ e $m(x)$ seu polinômio minimal sobre K. Então $\partial m = [K[\alpha] : K] = r > 1,\ r \leq n$. Como $m(x)$ é um polinômio irredutível sobre um subcorpo de $\mathbb{C}$ com uma raiz na extensão $N : K$, temos que m se decompõe linearmente em N e suas raízes são distintas. Por indução, há precisamente s $K[\alpha]-$monomorfismos distintos $\rho_1, \ldots, \rho_s : L \to N$, em que $s = [L : K[\alpha]] = \dfrac{n}{r}$. Pela Proposição 5.13, existem r $K-$automorfismos distintos $\tau_1, \ldots, \tau_r$ de N tais que $\tau_i(\alpha) = \alpha_i$. As funções $\phi_{ij} = \tau_i\rho_j$ nos dão $rs = n$ $K-$monomorfismos distintos de L em N.

Agora seja $\tau : L \to N$ um $K-$monomorfismo. Então $\tau(\alpha)$ é uma raiz de $m(x)$ em N, portanto $\tau(\alpha) = \alpha_i$ para algum i. A função $\phi = \tau_i^{-1}\tau$ é um $K[\alpha]-$monomorfismo de L em N, pois $\phi(\alpha) = \tau_i^{-1}(\tau(\alpha)) = \tau_i^{-1}(\alpha_i) = \alpha$. Agora, por indução, $\varphi = \rho_j$ para algum j. Portanto $\tau = \tau_i\rho_j = \phi_{ij}$ e o teorema está provado. □

O resultado acima nos fornece a ordem do grupo de Galois de uma extensão normal e finita, resultado de suma importância para nossos estudos.

Corolário 5.20. *Se $L : K$ é uma extensão normal e finita em $\mathbb{C}$, então existem precisamente $[L : K]$ $K-$automorfismos distintos de L. Ou seja, $o(\Gamma(L : K)) = [L : K]$.*

Demonstração. Como $L : K$ é uma extensão normal e finita, segue pelo Teorema 5.19 que existem $n = [L : K]$ $K-$monomorfismos de L em L (já que L é o fecho normal de $L : K$. Mas pelo Teorema 5.18, como $L : K$ é normal, todo $K-$monomorfismo de L em L é um $K-$automorfismo. Portanto $o(\Gamma(L : K)) = [L : K] = n$. □

Teorema 5.21. *Seja $L : K$ uma extensão finita com Grupo de Galois G. Se $L : K$ é normal, então K é o corpo fixo de G.*

Demonstração. Seja K_0 o corpo fixo de G e seja $[L : K] = n$. O Corolário 5.20 nos dá $o(G) = n$. Mas pelo Teorema 5.9 sabemos que $[L : K_0] = o(G) = n$. Porém como $K \subseteq K_0 \subseteq L$ e $[L : K] = [L : K_0] \cdot [K_0 : K] \Rightarrow n = n \cdot [K_0 : K] \Rightarrow [K_0 : K] = 1$ e portanto $K = K_0$. □

Teorema 5.22. *Suponhamos que $K \subseteq L \subseteq M$ e $M : K$ é finita. Então o número de K-monomorfismos distintos de L em M é no máximo $[L : K]$.*

Demonstração. Seja N o fecho normal de $M : K$. Então $N : K$ é finita, e todo $K-$monomorfismo de L em M é também um $K-$monomorfismo de L em N ($M \subseteq N$). Portanto podemos assumir que M é uma extensão normal de K, substituindo M por N.

Argumentaremos agora por indução em $[L : K]$, como na demonstração do Teorema 5.19, exceto pelo fato de podermos deduzir somente que existem s' $K[\alpha]-$monomorfismos de L em N, onde $s' \leq s$ (por indução) e existem r' $K-$automorfismos de N, onde $r' \leq r$ (já que as raízes distintas de m em N podem não ser distintas). O resto da demonstração segue como no Teorema 5.19. □

O próximo teorema atua como uma recíproca do Teorema 5.21.

Teorema 5.23. *Se $L : K$ é uma extensão finita com grupo de Galois G, tal que K é o corpo fixo de G, então $L : K$ é uma extensão normal.*

Demonstração. Sabemos pelo Teorema 5.9 que $[L : K] = o(G) = n$, ou seja, há exatamente n K-automorfismos distintos de L, digamos, $\sigma_1, \ldots, \sigma_n$. Agora, como $L : K$ é finita, existe o fecho normal N de $L : K$. Note que cada σ_i, $i = 1, \ldots, n$ pode ser visto como um K-monomorfismo $\sigma_i : L \to N$, ou seja, obtemos n monomorfismos distintos. Mas, pelo Teorema 5.22, o número de K-monomorfismos de L em N é no máximo n. Logo há exatamente n K-monomorfismos de L em N que são K-automorfismos de L, donde segue pelo item 2 do Teorema 5.18 que $L : K$ é normal. □

Como vimos no início deste capítulo, a correspondência de Galois reverte inclusões. Após estudar os $K-$automorfismos, vemos que se uma extensão é normal e finita, a correspondência de Galois se torna bijetiva (para subcorpos de $\mathbb{C}$).

5.3 A correspondência de Galois

Nesta seção apresentaremos o teorema fundamental de Galois, no qual todas as peças do quebra cabeça são encaixadas.

Considere uma extensão $L : K$ de $\mathbb{C}$ com grupo de Galois G. Seja $\mathcal{F}$ o conjunto dos corpos intermediários, ou seja, o conjunto dos subcorpos M tais que $K \subseteq M \subseteq L$. Seja $\mathcal{G}$ o conjunto de todos os subgrupos H de G. Definimos as seguintes funções,

$$* : \mathcal{F} \to \mathcal{G} \qquad\qquad \dagger : \mathcal{G} \to \mathcal{F}$$

como segue: se $M \in \mathcal{F}$, então M^* é o grupo formado por todos os $M-$automorfismos de L. Se $H \in \mathcal{G}$, então $H^\dagger$ é o corpo fixo de H.

Já observamos que as funções $*$ e $\dagger$ são inclusões reversas, ou seja, $M \subseteq M^{*\dagger}$ e $H \subseteq H^{\dagger *}$. Agora veremos em quais casos a igualdade se mantém.

Lema 5.24. *Suponhamos que $L : K$ seja uma extensão de corpos, M seja um corpo intermediário e τ seja um $K-$automorfismo de L. Então $(\tau(M))^* = \tau M^* \tau^{-1}$.*

Demonstração. Considere $\tau(M)$. Sejam $\gamma \in M^*$ e $x \in \tau(M)$. Então $x = \tau(x_0)$ para algum $x_0 \in M$. Calculando: $(\tau\gamma\tau^{-1})(x) = \tau(\gamma(\tau^{-1}(x))) = \tau(\gamma(x_0)) = \tau(x_0) = x$, portanto $\tau\gamma\tau^{-1} \in (\tau(M))^*$. Logo $\tau M^*\tau^{-1} \subseteq (\tau(M))^*$. Por outro lado, seja $\gamma \in (\tau(M))^*$ e $x \in M$, então $(\tau^{-1}\gamma\tau)(x) = \tau^{-1}(\gamma(\tau(x))) = \tau^{-1}(\tau(x)) = x$, ou seja, $\tau^{-1}\gamma\tau \in M^*$. Assim, $\tau^{-1}(\tau(M))^*\tau \subseteq M^*$, ou ainda, $\tau(M)^* \subseteq \tau M^*\tau^{-1}$. Portanto $(\tau(M))^* = \tau M^*\tau^{-1}$. □

Teorema 5.25. *(Teorema fundamental de Galois) Se $L : K$ é uma extensão normal e finita em $\mathbb{C}$, com grupo de Galois G, e $\mathcal{F}, \mathcal{G}, *$ e $\dagger$ são definidas como acima, então:*

1. *O Grupo de Galois G tem ordem $[L : K]$.*
2. *As funções $*$ e $\dagger$ são mutuamente inversas e geram uma correspondência bijetiva entre $\mathcal{F}$ e $\mathcal{G}$ (revertem tamanho).*
3. *Se M é um corpo intermediário, então $[L : M] = o(M^*)$ e $[M : K] = \dfrac{o(G)}{o(M^*)}$.*
4. *Um corpo intermediário M é uma extensão normal de K se e somente se M^* é subgrupo normal de G.*
5. *Se um corpo intermediário M é uma extensão normal de K, então o grupo de Galois de $M : K$ é isomorfo ao grupo quociente $\dfrac{G}{M^*}$.*

Demonstração. 1. Segue do Corolário 5.20.

2. Seja M um corpo intermediário. Pelo Corolário 4.56, como $L : K$ é normal então $L : M$ também é uma extensão normal. Como $L : M$ é normal, pelo Teorema 5.21, segue que M é o corpo fixo de M^*, ou seja, $M^{*\dagger} = M$. Seja agora $H \in \mathcal{G}$. Sabemos que $H \subseteq H^{\dagger *}$. Como acabamos de provar, temos $H^{\dagger *\dagger} = (H^\dagger)^{*\dagger} = H^\dagger$. Pelo Teorema 5.9, $o(H) = [L : H^\dagger]$. Portanto $o(H) = [L : H^{\dagger *\dagger}]$ e novamente pelo Teorema 5.9 $[L : H^{\dagger *\dagger}] = o(H^{\dagger *})$. Como H e $H^{\dagger *}$ são grupos finitos e $H \subseteq H^{\dagger *}$ devemos ter $H = H^{\dagger *}$. Portanto, se $L : K$ é uma extensão normal e finita, as funções $\dagger$ e $*$ se tornam inversas.

3. Se $L : K$ é normal e M é um corpo intermediário, então $L : M$ é normal e pelo Corolário 5.20, $o(M^*) = [L : M]$. Mas como $[L : K] = [L : M] \cdot [M : K]$ e $[L : K] = \Gamma(L : K) = o(G)$, segue que $o(G) = o(M^*) \cdot [M : K] \Rightarrow [M : K] = \dfrac{o(G)}{o(M^*)}$.

4. Se $M : K$ é uma extensão normal, seja $\tau \in G = \Gamma(L : K) = \{\sigma : L \to L \mid \sigma_{|_K} = Id\}$. Então $\tau_{|_M}$ é um $K-$monomorfismo de M em L, e então um $K-$automorfismo de M pelo Teorema 5.18. Portanto $\tau(M) = M$. Pelo Lema 5.24, $M^* = (\tau(M))^* = \tau M^* \tau^{-1}$. Como τ é qualquer, segue que M^* é um subgrupo normal de G.

   Reciprocamente, suponha que M^* é um subgrupo normal de G. Seja σ qualquer $K-$monomorfismo de M em L. Pelo Teorema 5.12, existe um $K-$automorfismo τ de L tal que $\tau_{|_M} = \sigma$. Agora, como M^* é subgrupo normal de G, temos $\tau M^* \tau^{-1} = M^*$. Portanto, pelo Lema 5.24, segue que $M^* = \tau M^* \tau^{-1} = (\tau(M))^*$. Agora aplicando $\dagger$ temos $M^{*\dagger} = (\tau(M))^{*\dagger} \Rightarrow M = \tau(M)$. Portanto $\sigma(M) = M$ e assim σ é um $K-$automorfismo de M. Pelo Teorema 5.18 concluímos que $M : K$ é normal.

5. Seja G' o grupo de Galois de $M : K$. Podemos definir uma função $\phi : G \to G'$ por $\phi(\tau) = \tau_{|_M}$, $\tau \in G$. Observe que ϕ é um homomorfismo de G em G', e pelo Teorema 5.18, $\tau_{|_M}$ é um $K-$automorfismo de M. Agora, pelo Teorema 5.12, ϕ é sobrejetora, além disso o núcleo de ϕ é $M^* = \Gamma(L : M)$. Assim pelo teorema do homomorfismo para grupos concluímos que $G' = Im(\phi) \simeq \dfrac{G}{Ker(\phi)} \simeq \dfrac{G}{M^*}$.

□

5.4 Exemplos

Para finalizar este capítulo, apresentaremos alguns exemplos, discutindo sobre a teoria estudada até o momento. Uma observação que merece destaque refere-se a forma como os diagramas foram construídos: optamos por manter os diagramas desenhados no mesmo padrão, a fim de facilitar a visualização da relação entre os subgrupos do grupo de Galois e os corpos intermediários.

5.4.1 Exemplo 1

Vamos iniciar com um exemplo mais simples: vamos construir o diagrama das extensões de corpos contidas em $\mathbb{Q}[i, \sqrt{5}]$. Assim, seja $f(x) = x^4 - 4x^2 - 5 = (x^2+1)(x^2-5) = (x+i)(x-i)(x+\sqrt{5})(x-\sqrt{5})$ sobre $\mathbb{Q}$ e seja $\mathbb{Q}[i, \sqrt{5}]$ o corpo de decomposição de $f(x)$ sobre $\mathbb{C}$, já que $\mathbb{Q}[i, \sqrt{5}]$ é o menor corpo que contém todas as raízes de $f(x)$ (observe que mesmo

$f(x)$ não sendo irredutível, podemos calcular seu corpo de decomposição). Pelo Teorema 4.55, sabemos $\mathbb{Q}[i, \sqrt{5}]$ é uma extensão finita e normal. Além disso, vimos no Exemplo 4.48 que $[\mathbb{Q}[i, \sqrt{5}] : \mathbb{Q}] = 4$ e $\mathbb{Q}[i, \sqrt{5}] = \{a_0 + a_1 i + a_2\sqrt{5} + a_3 i\sqrt{5} \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$.

Vamos encontrar os elementos do grupo de Galois de $\mathbb{Q}[i, \sqrt{5}] : \mathbb{Q}$. Sabemos pelo Corolário 4.31 que há um $\mathbb{Q}-$automorfismo σ de $\mathbb{Q}[i, \sqrt{5}]$ tal que $\sigma(i) = i$ e $\sigma(\sqrt{5}) = -\sqrt{5}$ e outro $\tau : \mathbb{Q}[i, \sqrt{5}] \to \mathbb{Q}[i, \sqrt{5}]$ tal que $\tau(i) = -i$ e $\tau(\sqrt{5}) = \sqrt{5}$. Logo encontramos os seguintes automorfismos:

Tabela 2 – $\mathbb{Q}$-automorfismos de $\mathbb{Q}[i, \sqrt{5}]$

Automorfismo	Efeito em $\sqrt{5}$	Efeito em i
Id	$\sqrt{5}$	i
σ	$-\sqrt{5}$	i
τ	$\sqrt{5}$	$-i$
$\sigma\tau$	$-\sqrt{5}$	$-i$

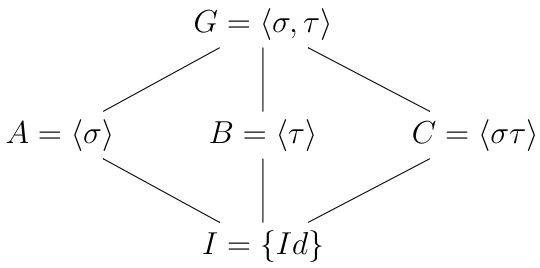
Fonte: Os autores (2021)

Perceba que $\sigma^2 = \tau^2 = (\sigma\tau)^2 = Id$, e $\sigma\tau = \tau\sigma$, portanto o grupo de Galois associado ao polinômio $f(x)$ é $\mathbb{Z}_2 \times \mathbb{Z}_2$. Além disso, qualquer $\mathbb{Q}-$automorfismo de $\mathbb{Q}[i, \sqrt{5}]$ leva i em alguma raiz de $x^2 + 1$, assim $i \mapsto \pm i$. Similarmente, $\sqrt{5}$ é mapeado em $\pm\sqrt{5}$. Todas as possibilidades de combinação destes quatro elementos aparecem na Tabela 2, logo estes são precisamente os $\mathbb{Q}-$automorfismos de $\mathbb{Q}[i, \sqrt{5}]$.

Agora, vamos encontrar os subgrupos de $G = \Gamma(\mathbb{Q}[i, \sqrt{5}] : \mathbb{Q})$. Como $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, sabemos que $o(G) = 4$. Pelo teorema de Lagrange as possíveis ordens dos subgrupos de G são $1, 2$ e 4. Portanto, calculando os subgrupos:

- Ordem 4: $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \simeq \{Id, \sigma\} \times \{Id, \tau\}$;
- Ordem 2:
  - $A = \{Id, \sigma\} \simeq \mathbb{Z}_2$;
  - $B = \{Id, \tau\} \simeq \mathbb{Z}_2$;
  - $C = \{Id, \sigma\tau\} \simeq \mathbb{Z}_2$;
- Ordem 1: $I = \{Id\}$.

Obtemos o seguinte diagrama para $\mathcal{G}$:



Se $x = a_0 + a_1 i + a_2\sqrt{5} + a_3 i\sqrt{5} \in \mathbb{Q}[i, \sqrt{5}]$ (1), vamos encontrar os corpos intermediários:

- $Id : i \to i \qquad \sqrt{5} \to \sqrt{5}$

  Como $Id(x) = x \ \forall \ x \in \mathbb{Q}[i, \sqrt{5}]$, Id fixa $\mathbb{Q}[i, \sqrt{5}]$.

- $\sigma : i \to i \qquad \sqrt{5} \to -\sqrt{5}$

  $$\begin{aligned}\sigma(x) &= a_0 + a_1(i) + a_2(-\sqrt{5}) + a_3(i)(-\sqrt{5}) \\ &= a_0 + a_1 i - a_2\sqrt{5} - a_3 i\sqrt{5}\end{aligned}$$

  Comparando com (1), vamos que x é fixado por σ se e somente se: $a_0 = a_0$, $a_1 = a_1$, $a_2 = -a_2$ e $a_3 = -a_3$. Logo a_0 e a_1 são arbitrários, enquanto que $a_2 = a_3 = 0$. Assim $x = a_0 + a_1 i$ e dessa forma σ fixa $\mathbb{Q}[i]$.

- $\tau : i \to -i \qquad \sqrt{5} \to \sqrt{5}$

  $$\begin{aligned}\tau(x) &= a_0 + a_1(-i) + a_2(\sqrt{5}) + a_3(-i)(\sqrt{5}) \\ &= a_0 - a_1 i + a_2\sqrt{5} - a_3 i\sqrt{5}\end{aligned}$$

  Portanto x é fixado pelo automorfismo τ se $a_0 = a_0$, $a_1 = -a_1$, $a_2 = a_2$ e $a_3 = -a_3$. Portanto a_0 e a_2 são livres, enquanto que $a_1 = a_3 = 0$. Logo $x = a_0 + a_2\sqrt{5}$ e assim τ fixa o corpo $\mathbb{Q}[\sqrt{5}]$.

- $\sigma\tau : i \to -i \qquad \sqrt{5} \to -\sqrt{5}$

  $$\begin{aligned}\sigma(x) &= a_0 + a_1(-i) + a_2(-\sqrt{5}) + a_3(-i)(-\sqrt{5}) \\ &= a_0 - a_1 i - a_2\sqrt{5} + a_3 i\sqrt{5}\end{aligned}$$

  Observe que x é fixado por $\sigma\tau$ se $a_0 = a_0, a_1 = -a_1, a_2 = -a_2$ e $a_3 = a_3$. Dessa forma $x = a_0 + a_3 i\sqrt{5}$ e assim $\sigma\tau$ fixa $\mathbb{Q}[i\sqrt{5}]$.

Por meio das contas que acabamos de fazer, encontramos que:

- ⋆ Id fixa $\mathbb{Q}[i, \sqrt{5}] = \{a_0 + a_1 i + a_2\sqrt{5} + a_3 i\sqrt{5} \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$;
- ⋆ σ fixa $\mathbb{Q}[i] = \{a_0 + a_1 i \mid a_0, a_1 \in \mathbb{Q}\}$;
- ⋆ τ fixa $\mathbb{Q}[\sqrt{5}] = \{a_0 + a_1\sqrt{5} \mid a_0, a_1 \in \mathbb{Q}\}$;

⋆ $\sigma\tau$ fixa $\mathbb{Q}[i\sqrt{5}] = \{a_0 + a_1 i\sqrt{5} \mid a_0, a_1 \in \mathbb{Q}\}$.

Como vimos na Seção 5, a cada subgrupo H de $\Gamma(L : K)$ associamos o conjunto $H^\dagger = \{x \in L \mid \sigma(x) = x \ \forall\ \sigma \in H\}$. Assim, para encontrar o corpo fixo dos subgrupos de $\Gamma(\mathbb{Q}[i, \sqrt{5}] : \mathbb{Q})$, vamos calcular a interseção de todos os corpos que são fixados pelos automorfismos que pertencem aos subgrupos. Dessa forma, encontraremos os corpos intermediários:

∗ $I = \{Id\}$ $\qquad I^\dagger = \mathbb{Q}[i, \sqrt{5}]$;

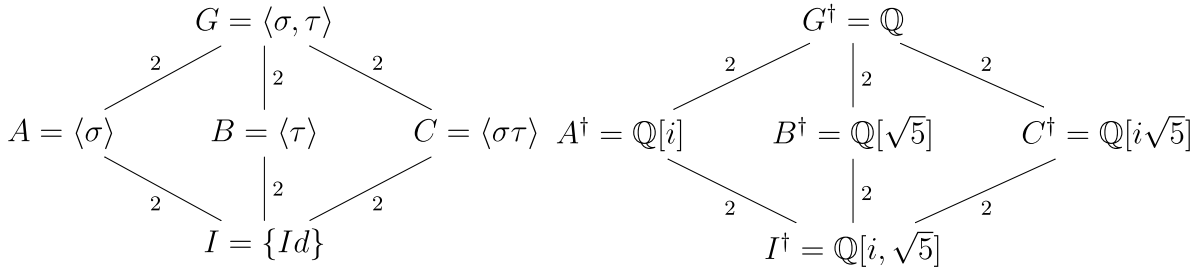
∗ $A = \{Id, \sigma\}$ $\qquad A^\dagger = \mathbb{Q}[i, \sqrt{5}] \cap \mathbb{Q}[i] = \mathbb{Q}[i]$;

∗ $B = \{Id, \tau\}$ $\qquad B^\dagger = \mathbb{Q}[i, \sqrt{5}] \cap \mathbb{Q}[\sqrt{5}] = \mathbb{Q}[\sqrt{5}]$;

∗ $C = \{Id, \sigma\tau\}$ $\qquad C^\dagger = \mathbb{Q}[i, \sqrt{5}] \cap \mathbb{Q}[i\sqrt{5}] = \mathbb{Q}[i\sqrt{5}]$;

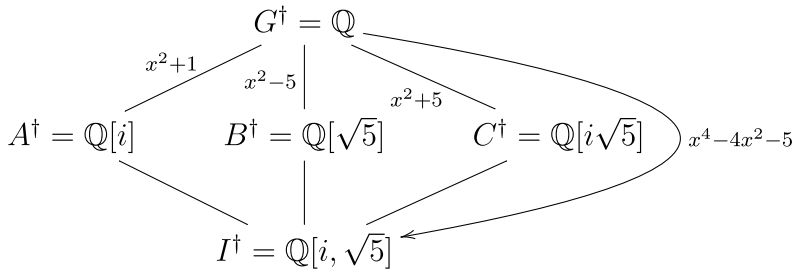
∗ $G = \{Id, \sigma, \tau, \sigma\tau\}$ $\qquad G^\dagger = \mathbb{Q}[i, \sqrt{5}] \cap \mathbb{Q}[i] \cap \mathbb{Q}[\sqrt{5}] \cap \mathbb{Q}[i\sqrt{5}] = \mathbb{Q}$.

Podemos construir o reticulado das extensões de corpos de $\mathcal{F}$, comparando-o com o reticulado de grupos de $\mathcal{G}$:



Podemos calcular os subgrupos normais de $\mathbb{Z}_2 \times \mathbb{Z}_2$. Como $\mathbb{Z}_2$ é abeliano, sabemos que $\mathbb{Z}_2 \times \mathbb{Z}_2$ também é um grupo abeliano e dessa forma todos os seus subgrupos G, A, B, C e I são normais. Pelo teorema fundamental de Galois, $G^\dagger, A^\dagger, B^\dagger, C^\dagger$ e $I^\dagger$ são extensões normais de $\mathbb{Q}$. Como todas essas extensões têm dimensão finita, são corpos de decomposição para polinômios em $\mathbb{Q}[x]$, como segue:

- $I^\dagger = \mathbb{Q}[i, \sqrt{5}]$ é o corpo de decomposição para o polinômio $f(x) = (x^2 + 1)(x^2 - 5) = x^4 - 4x^2 - 5$;
- $A^\dagger = \mathbb{Q}[i]$ é o corpo de decomposição para $f(x) = x^2 + 1$;
- $B^\dagger = \mathbb{Q}[\sqrt{5}]$ é o corpo de decomposição para $f(x) = x^2 - 5$;
- $C^\dagger = \mathbb{Q}[i\sqrt{5}]$ é o corpo de decomposição para $f(x) = x^2 + 5$;
- $G^\dagger = \mathbb{Q}$ é o corpo de decomposição para $f(x) = x$.



5.4.2 Exemplo 2

Agora vamos para um exemplo mais rebuscado, que fala a respeito do grupo de Galois do corpo de decomposição do polinômio $f(x) = x^4 - 2$ sobre $\mathbb{Q}$.

Considere o polinômio $f(x) = x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2}) = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2})$ sobre $\mathbb{Q}$ e seja K o corpo de decomposição para $f(x)$, com $K \subseteq \mathbb{C}$. Podemos fatorar $f(x)$ como $f(x) = (x-\xi)(x+\xi)(x-i\xi)(x+i\xi)$ em que $\xi = \sqrt[4]{2}$. Observe que todas as raízes de $f(x)$ são obtidas através dos elementos i e ξ, portanto $K = \mathbb{Q}[i, \xi]$. Como K é corpo de decomposição, a extensão $\mathbb{Q}[i, \xi]$ é finita e normal. Estamos trabalhando em $\mathbb{C}$, portanto a separabilidade é automática. Agora, encontraremos o grau de $K : \mathbb{Q}$.

Pela Lei da Torre, temos $[\mathbb{Q}[i, \xi] : \mathbb{Q}] = [\mathbb{Q}[i, \xi] : \mathbb{Q}[\xi]] \cdot [\mathbb{Q}[\xi] : \mathbb{Q}]$. Como i é raiz do polinômio $p(x) = x^2 + 1$ e $i \notin \mathbb{Q}[\xi]$, podemos concluir que $p(x)$ é o polinômio minimal de i sobre $\mathbb{Q}[\xi]$, e dessa forma $[\mathbb{Q}[i, \xi] : \mathbb{Q}[\xi]] = 2$. Agora, como ξ é um zero de $f(x)$ sobre $\mathbb{Q}$ e pelo Critério de Eisenstein $f(x)$ é irredutível sobre $\mathbb{Q}$, concluímos que $f(x)$ é o polinômio minimal de ξ sobre $\mathbb{Q}$. Logo $[\mathbb{Q}[\xi]] : \mathbb{Q}] = 4$. Portanto $[\mathbb{Q}[i, \xi] : \mathbb{Q}] = 2 \cdot 4 = 8$.

Como sabemos a dimensão de $\mathbb{Q}[i, \xi]$, vamos encontrar a forma geral dos elementos dessa extensão. Assim, seja $x \in \mathbb{Q}[i, \xi]$. Como $\mathbb{Q}[i, \xi] = \mathbb{Q}[\xi][i]$, $x \in \mathbb{Q}[\xi][i] \Rightarrow x = a + bi$, tal que $a, b \in \mathbb{Q}[\xi]$. Mas como $a, b \in \mathbb{Q}[\xi]$, temos que $a = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3$ e $b = a_4 + a_5\xi + a_6\xi^2 + a_7\xi^3$, e dessa forma $x = a + bi = (a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3) + (a_4 + a_5\xi + a_6\xi^2 + a_7\xi^3)i = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4 i + a_5 i\xi + a_6 i\xi^2 + a_7 i\xi^3$. Logo uma base para a extensão $\mathbb{Q}[i, \xi]$ é $\{1, \xi, \xi^2, \xi^3, i, i\xi, i\xi^2, i\xi^3\}$.

Vamos encontrar os elementos do Grupo de Galois. Sabemos pelo Corolário 4.31 que há um $\mathbb{Q}-$automorfismo σ de $\mathbb{Q}[i, \xi]$ tal que $\sigma(i) = i$ e $\sigma(\xi) = i\xi$, e outro $\mathbb{Q}-$automorfismo τ de $\mathbb{Q}[i, \xi]$ tal que $\tau(i) = -i$ e $\tau(\xi) = \xi$. Vamos compô-los:

Note que $\sigma^4 = \tau^2 = Id$, $\sigma\tau = \tau\sigma^3$, $\sigma^2\tau = \tau\sigma^2$ e $\sigma^3\tau = \tau\sigma$. Além disso, qualquer $\mathbb{Q}-$automorfismo de K leva i em algum zero de $x^2 + 1$, ou seja, $i \mapsto \pm i$. Similarmente, ξ é mapeado em $\xi, -\xi, i\xi$ ou $-i\xi$. Todas as possibilidades de combinação destes números aparecem na Tabela 3, logo estes são precisamente os 8 $\mathbb{Q}-$automorfismos de $\mathbb{Q}[i, \xi]$. Perceba que a quantidade de automorfismos é igual a dimensão de $\mathbb{Q}[i, \xi]$.

A estrutura abstrata do grupo de Galois pode ser encontrada. Se denotarmos por

Tabela 3 – $\mathbb{Q}$-automorfismos de $\mathbb{Q}[i, \xi]$

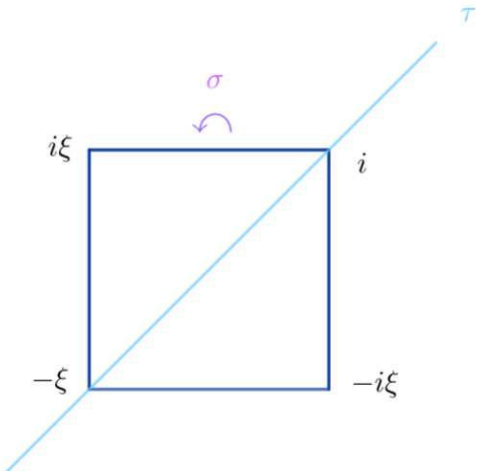
Automorfismo	Efeito em ξ	Efeito em i
Id	ξ	i
σ	$i\xi$	i
σ^2	$-\xi$	i
σ^3	$-i\xi$	i
τ	ξ	$-i$
$\sigma\tau$	$i\xi$	$-i$
$\sigma^2\tau$	$-\xi$	$-i$
$\sigma^3\tau$	$-i\xi$	$-i$

Fonte: Os autores (2021)

G o grupo de Galois, vemos que $G = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = Id, \sigma\tau = \tau\sigma^3 \rangle$, ou seja, como já vimos, G é o grupo diedral de ordem 8, o D_4.

De fato, se denotarmos os vértices do quadrado com as raízes de $x^4 - 2$, vemos que $\sigma = R_{\frac{\pi}{2}}$ e $\tau = R_1$. Ao realizar todas as combinações possíveis e construir o grupo D_4, obteremos exatamente os mesmos automorfismos das Tabela 3.

Figura 6 – O grupo de Galois de $x^4 - 2$ interpretado como simetrias do quadrado



Fonte: Os autores (2021)

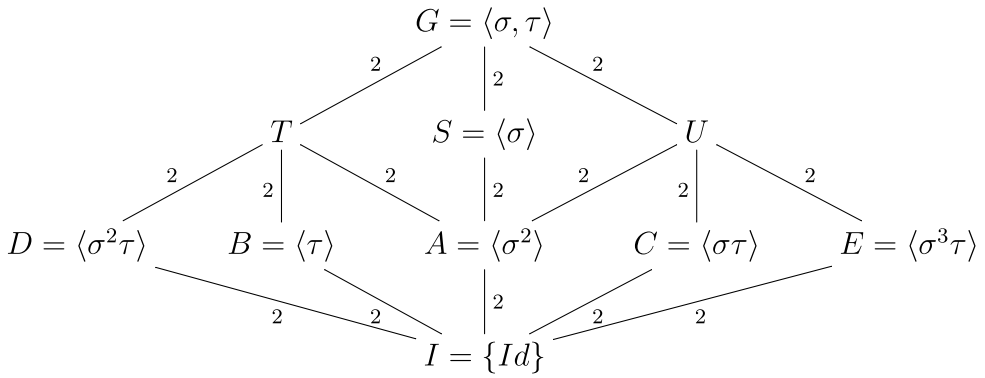
Vamos calcular os subgrupos de D_4. Pelo teorema de Lagrange, sabemos que as possíveis ordens dos subgrupos de D_4 são $1, 2, 4$ e 8. Assim, os subgrupos de G são:

- Ordem 8: $G \simeq D_4$;
- Ordem 4:
  - $S = \{Id, \sigma, \sigma^2, \sigma^3\} \simeq \mathbb{Z}_4$;
  - $T = \{Id, \tau, \sigma^2, \sigma^2\tau\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \simeq \{Id, \sigma^2\} \times \{Id, \tau\}$;

– $U = \{Id, \sigma^2, \sigma\tau, \sigma^3\tau\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \simeq \{Id, \sigma^2\} \times \{Id, \sigma\tau\}$;

- Ordem 2:
  - $A = \{Id, \sigma^2\} \simeq \mathbb{Z}_2$;
  - $B = \{Id, \tau\} \simeq \mathbb{Z}_2$;
  - $C = \{Id, \sigma\tau\} \simeq \mathbb{Z}_2$;
  - $D = \{Id, \sigma^2\tau\} \simeq \mathbb{Z}_2$;
  - $E = \{Id, \sigma^3\tau\} \simeq \mathbb{Z}_2$;
- Ordem 1: $I = \{Id\}$.

Construindo o diagrama dos grupos:



Vamos encontrar os corpos intermediários associados aos subgrupos de G. Sabemos que se $x \in \mathbb{Q}[i, \xi]$, então $x = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4 i + a_5 i\xi + a_6 i\xi^2 + a_7 i\xi^3$ (1). Agora, vamos ver quais subcorpos cada $\mathbb{Q}$-automorfismo fixa:

- Id: $\xi \to \xi \qquad i \to i$

  Como $Id(x) = x \ \forall \ x \in \mathbb{Q}[i, \xi]$, segue que Id fixa o corpo $\mathbb{Q}[i, \xi]$.

- σ: $\xi \to i\xi \qquad i \to i$

$$\begin{aligned} \sigma(x) &= a_0 + a_1 i\xi + a_2(i\xi)^2 + a_3(i\xi)^3 + a_4 i + a_5 i(i\xi) + a_6 i(i\xi)^2 + a_7 i(i\xi)^3 \\ &= a_0 + a_1 i\xi - a_2\xi^2 - a_3 i\xi^3 + a_4 i - a_5\xi - a_6 i\xi^2 + a_7\xi^3 \\ &= a_0 - a_5\xi - a_2\xi^2 + a_7\xi^3 + a_4 i + a_1 i\xi - a_6 i\xi^2 - a_3 i\xi^3 \end{aligned}$$

  Comparando com (1), obtemos que o elemento x é fixado por σ se e somente se: $a_0 = a_0$; $a_1 = -a_5$; $a_2 = -a_2$; $a_3 = a_7$; $a_4 = a_4$; $a_5 = a_1$; $a_6 = -a_6$; $a_7 = -a_3$. Portanto a_0 e a_4 são arbitrários, enquanto que $a_1 = a_5 = 0$, $a_2 = -a_2 = 0$, $a_6 = -a_6 = 0$ e $a_7 = a_3 = 0$. Assim $x = a_0 + a_4 i$, e dessa forma o corpo fixado pelo automorfismo σ é $\mathbb{Q}[i]$.

- τ: $\xi \to \xi \qquad i \to -i$

$$\begin{aligned}\tau(x) &= a_0 + a_1(\xi) + a_2(\xi)^2 + a_3(\xi)^3 + a_4(-i) + a_5(-i)\xi + a_6(-i)(\xi)^2 + a_7(-i)(\xi)^3 \\ &= a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 - a_4 i - a_5 i\xi - a_6 i\xi^2 - a_7 i\xi^3\end{aligned}$$

Portanto x é fixado por τ se e somente se: $a_0 = a_0$; $a_1 = a_1$; $a_2 = a_2$; $a_3 = a_3$; $a_4 = -a_4$; $a_5 = -a_5$; $a_6 = -a_6$; $a_7 = -a_7$. Logo a_0, a_1, a_2 e a_3 são arbitrários, enquanto que $a_4 = a_5 = a_6 = a_7 = 0$. Assim $x = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3$ e dessa forma τ fixa $\mathbb{Q}[\xi] = \mathbb{Q}[\sqrt[4]{2}]$.

- σ^2: $\xi \to -\xi \qquad i \to i$

$$\begin{aligned}\sigma(x) &= a_0 + a_1(-\xi) + a_2(-\xi)^2 + a_3(-\xi)^3 + a_4 i + a_5 i(-\xi) + a_6 i(-\xi)^2 + a_7 i(-\xi)^3 \\ &= a_0 - a_1\xi + a_2\xi^2 - a_3\xi^3 + a_4 i - a_5 i\xi + a_6 i\xi^2 - a_7 i\xi^3\end{aligned}$$

Portanto x é fixado por σ se e somente se: $a_0 = a_0$; $a_1 = -a_1$; $a_2 = a_2$; $a_3 = -a_3$; $a_4 = a_4$; $a_5 = -a_5$; $a_6 = a_6$; $a_7 = -a_7$. Logo a_0, a_2, a_4 e a_6 são livres, enquanto que $a_1 = a_3 = a_5 = a_7 = 0$. Então $x = a_0 + a_2\xi^2 + a_4 i + a_6 i\xi^2 = (a_0 + a_2\xi^2) + (a_4 + a_6\xi^2)i = a + bi$, $a, b \in \mathbb{Q}[\xi^2]$. Logo $x \in \mathbb{Q}[\xi^2][i] = \mathbb{Q}[i, \xi^2]$.

- σ^3: $\xi \to -i\xi \qquad i \to i$

$$\begin{aligned}\sigma^3(x) &= a_0 + a_1(-i\xi) + a_2(-i\xi)^2 + a_3(-i\xi)^3 + a_4 i + a_5 i(-i\xi) + a_6 i(-i\xi)^2 + \\ a_7 i(-i\xi)^3 & \\ &= a_0 - a_1 i\xi - a_2\xi^2 + a_3 i\xi^3 + a_4 i + a_5\xi - a_6 i\xi^2 - a_7\xi^3 \\ &= a_0 + a_5\xi - a_2\xi^2 - a_7\xi^3 + a_4 i - a_1 i\xi - a_6 i\xi^2 + a_3 i\xi^3\end{aligned}$$

Comparando com (1) vemos que x é fixado por σ^3 se: $a_0 = a_0$; $a_1 = a_5$; $a_2 = -a_2$; $a_3 = -a_7$; $a_4 = a_4$; $a_5 = -a_1$; $a_6 = -a_6$; $a_7 = a_3$. Então a_0 e a_4 são arbitrários e $a_1 = a_5 = 0$, $a_2 = 0$, $a_3 = a_7 = 0$ e $a_6 = 0$. Assim $x = a_0 + a_4 i$ e forma σ^3 fixa $\mathbb{Q}[i]$.

- $\sigma\tau$: $\xi \to i\xi \qquad i \to -i$

$$\begin{aligned}\sigma^3(x) &= a_0 + a_1(i\xi) + a_2(i\xi)^2 + a_3(i\xi)^3 + a_4(-i) + a_5(-i)(i\xi) + a_6(-i)(i\xi)^2 \\ +a_7(-i)(i\xi)^3 & \\ &= a_0 + a_1 i\xi - a_2\xi^2 - a_3 i\xi^3 - a_4 i + a_5\xi + a_6 i\xi^2 - a_7\xi^3 \\ &= a_0 + a_5\xi - a_2\xi^2 - a_7\xi^3 - a_4 i + a_1 i\xi + a_6 i\xi^2 - a_3 i\xi^3\end{aligned}$$

Assim x é fixado por $\sigma\tau$ se: $a_0 = a_0$; $a_1 = a_5$; $a_2 = -a_2$; $a_3 = -a_7$; $a_4 = -a_4$; $a_5 = a_1$; $a_6 = a_6$; $a_7 = -a_3$. Então a_0 e a_6 são quaisquer, $a_2 = a_4 = 0$, $a_1 = a_5$ e $a_3 = -a_7$, o que nos dá:

$$\begin{aligned}x &= a_0 + a_1\xi + a_3\xi^3 + a_1 i\xi + a_6 i\xi^2 - a_3 i\xi^3 \\ &= a_0 + a_1(\xi + i\xi) + a_3(\xi^3 - i\xi^3) + a_6 i\xi^2 \\ &= a_0 + a_1(\xi + i\xi) + a_6 i\xi^2 + a_3(1 - i)\xi^3 \\ &= a_0 + a_1[(1 + i)\xi] + \tfrac{a_6}{2}[(1 + i)\xi]^2 - \tfrac{a_3}{2}[(1 + i)\xi]^3\end{aligned}$$

Portanto $\sigma\tau$ fixa o corpo $\mathbb{Q}[(1 + i)\xi]$.

- $\sigma^2\tau$: $\xi \to -\xi \qquad i \to -i$

$$\sigma^2\tau(x) = a_0+a_1(-\xi)+a_2(-\xi)^2+a_3(-\xi)^3+a_4(-i)+a_5(-i)(-\xi)+a_6(-i)(-\xi)^2+a_7(-i)(-\xi)^3$$
$$= a_0 - a_1\xi + a_2\xi^2 - a_3\xi^3 - a_4 i + a_5 i\xi - a_6 i\xi^2 + a_7 i\xi^3$$

Portanto a_0, a_2, a_5 e a_7 são livres e $a_1 = a_3 = a_4 = a_6 = 0$. Logo $x = a_0+a_2\xi^2+a_5 i\xi+a_7 i\xi^3 = (a_0+a_5 i\xi)+(a_2+a_7 i\xi)\xi^2 = a+b\xi^2$ tais que $a, b \in \mathbb{Q}[i\xi]$. Assim o corpo fixo por τ é $\mathbb{Q}[i\xi][\xi^2] = \mathbb{Q}[i\xi]$, já que $\xi^2 \in \mathbb{Q}[i\xi]$ ($\xi^2 = (i\xi)^2 \cdot (-1) \in \mathbb{Q}[i\xi]$).

- $\sigma^3\tau$: $\xi \to -i\xi \qquad i \to -i$

$$\sigma^3\tau(x) = a_0 + a_1(-i\xi) + a_2(-i\xi)^2 + a_3(-i\xi)^3 + a_4(-i) + a_5(-i)(-i\xi) + a_6(-i)(-i\xi)^2 + a_7(-i)(-i\xi)^3$$
$$= a_0 - a_1 i\xi - a_2\xi^2 + a_3 i\xi^3 - a_4 i - a_5\xi + a_6 i\xi^2 + a_7\xi^3$$
$$= a_0 - a_5\xi - a_2\xi^2 + a_7\xi^3 - a_4 i - a_1 i\xi + a_6 i\xi^2 + a_3 i\xi^3$$

Comparando com (1) : $a_0 = a_0$; $a_1 = -a_5$; $a_2 = -a_2$; $a_3 = a_7$; $a_4 = -a_4$; $a_5 = -a_1$; $a_6 = a_6$; $a_7 = a_3$. Portanto a_0 e a_6 são livres, $a_5 = -a_1$, $a_3 = a_7$ e $= a_2 = a_4 = 0$. Logo:

$$\begin{aligned} x &= a_0 + a_1\xi + a_3\xi^3 - a_1 i\xi + a_6 i\xi^2 + a_3 i\xi^3 \\ &= a_0 + a_1(\xi - i\xi) + a_3(\xi^3 + i\xi^3) + a_6 i\xi^2 \\ &= a_0 + a_1[(1-i)\xi] + a_6 i\xi^2 + a_3(1+i)\xi^3 \\ &= a_0 + a_1[(1-i)\xi] - \tfrac{a_6}{2}[(1-i)\xi]^2 - \tfrac{a_3}{2}[(1-i)\xi]^3 \end{aligned}$$

Portanto o corpo fixado por $\sigma^3\tau$ é $\mathbb{Q}[(1-i)\xi]$.

Assim, sabemos que:

⋆ $\mathbb{Q}[i] = \{a_0 + a_1 i \mid a_0, a_1 \in \mathbb{Q}\}$;

⋆ $\mathbb{Q}[i\xi^2] = \{a_0 + a_1 i\xi^2 \mid a_0, a_1 \in \mathbb{Q}\}$;

⋆ $\mathbb{Q}[\xi^2] = \{a_0 + a_1\xi^2 \mid a_0, a_1 \in \mathbb{Q}\}$;

⋆ $\mathbb{Q}[\xi] = \{a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$;

⋆ $\mathbb{Q}[i, \xi^2] = \{a_0 + a_1\xi^2 + a_2 i + a_3 i\xi^2 \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$;

⋆ $\mathbb{Q}[i\xi] = \{a_0 + a_1 i\xi + a_2\xi^2 + a_3 i\xi^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$;

⋆ $\mathbb{Q}[(1+i)\xi] = \{a_0 + a_1(1+i)\xi + a_2 i\xi^2 + a_3(1-i)\xi^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$;

⋆ $\mathbb{Q}[(1-i)\xi] = \{a_0 + a_1(1-i)\xi + a_2 i\xi^2 + a_3(1+i)\xi^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$;

⋆ $\mathbb{Q}[i, \xi] = \{a_0+a_1\xi+a_2\xi^2+a_3\xi^3+a_4 i+a_5 i\xi+a_6 i\xi^2+a_7 i\xi^3 \mid a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 \in \mathbb{Q}\}$;

E calculamos que:

- Id fixa $\mathbb{Q}[i,\xi]$:
- σ fixa $\mathbb{Q}[i]$;
- τ fixa $\mathbb{Q}[\xi]$;
- σ^2 fixa $\mathbb{Q}[i,\xi^2]$;
- σ^3 fixa $\mathbb{Q}[i]$:
- $\sigma\tau$ fixa $\mathbb{Q}[(1+i)\xi]$;
- $\sigma^2\tau$ fixa $\mathbb{Q}[i\xi]$;
- $\sigma^3\tau$ fixa $\mathbb{Q}[(1-i)\xi]$.

Agora vamos encontrar o corpo fixo de cada um dos subgrupos de Galois:

$*$ $G = \langle \sigma, \tau \rangle$ $\qquad G^\dagger = \mathbb{Q}$;

$*$ $T = \{Id, \tau, \sigma^2, \sigma^2\tau\}$ $\qquad T^\dagger = \mathbb{Q}[i,\xi] \cap \mathbb{Q}[\xi] \cap \mathbb{Q}[i,\xi^2] \cap \mathbb{Q}[i\xi] = \mathbb{Q}[\xi^2]$;

$*$ $S = \{Id, \sigma, \sigma^2, \sigma^3\}$ $\qquad S^\dagger = \mathbb{Q}[i,\xi] \cap \mathbb{Q}[i] \cap \mathbb{Q}[i,\xi^2] \cap \mathbb{Q}[i] = \mathbb{Q}[i]$;

$*$ $U = \{Id, \sigma^2, \sigma\tau, \sigma^3\tau\}$ $\qquad U^\dagger = \mathbb{Q}[i,\xi] \cap \mathbb{Q}[i,\xi^2] \cap \mathbb{Q}[(1+i)\xi] \cap \mathbb{Q}[(1-i)\xi] = \mathbb{Q}[i\xi^2]$;

$*$ $A = \{Id, \sigma^2\}$ $\qquad A^\dagger = \mathbb{Q}[i,\xi] \cap \mathbb{Q}[i,\xi^2] = \mathbb{Q}[i,\xi^2]$;

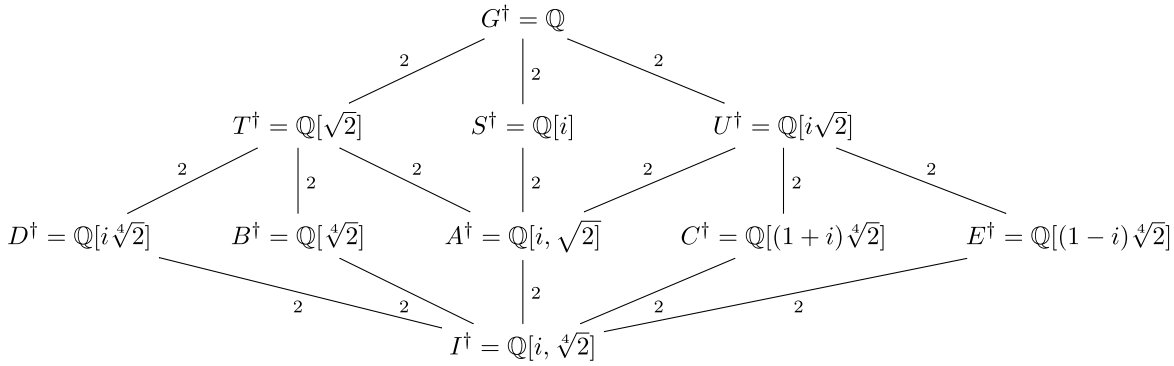
$*$ $B = \{Id, \tau\}$ $\qquad B^\dagger = \mathbb{Q}[i,\xi] \cap \mathbb{Q}[\xi] = \mathbb{Q}[\xi]$;

$*$ $C = \{Id, \sigma\tau\}$ $\qquad C^\dagger = \mathbb{Q}[i,\xi] \cap \mathbb{Q}[(1+i)\xi] = \mathbb{Q}[(1+i)\xi]$;

$*$ $D = \{Id, \sigma^2\tau\}$ $\qquad D^\dagger = \mathbb{Q}[i,\xi] \cap \mathbb{Q}[i\xi] = \mathbb{Q}[i\xi]$;

$*$ $E = \{Id, \sigma^3\tau\}$ $\qquad E^\dagger = \mathbb{Q}[i,\xi] \cap \mathbb{Q}[(1-i)\xi] = \mathbb{Q}[(1-i)\xi]$.

Vamos construir o reticulado dos corpos, substituindo $\xi = \sqrt[4]{2}$ para facilitar a visualização:



Ao calcular os subgrupos normais de G, encontramos que G, T, S, U, A e I são subgrupos normais. Pelo teorema fundamental de Galois, $G^\dagger$, $T^\dagger$, $S^\dagger$, $U^\dagger$, $A^\dagger$ e $I^\dagger$ devem ser as únicas extensões normais de $\mathbb{Q}$, que estão contidas em $\mathbb{Q}[i,\xi]$.

Como estas extensões são finitas e normais, são os corpos de decomposição de $\mathbb{Q}$ para os seguintes polinômios:

- $G^\dagger = \mathbb{Q}$ $\quad p(x) = x;$
- $T^\dagger = \mathbb{Q}[\sqrt{2}]$ $\quad p(x) = x^2 - 2;$
- $S^\dagger = \mathbb{Q}[i]$ $\quad p(x) = x^2 + 1;$
- $U^\dagger = \mathbb{Q}[i\sqrt{2}]$ $\quad p(x) = x^2 + 2;$
- $A^\dagger = \mathbb{Q}[i, \sqrt{2}]$ $\quad p(x) = x^4 - x^2 - 2;$
- $I^\dagger = \mathbb{Q}[i, \sqrt[4]{2}]$ $\quad p(x) = x^4 - 2.$

Por outro lado, observe que a extensão $B^\dagger : \mathbb{Q}$ não é uma extensão normal, uma vez que $x^4 - 2$ tem uma raiz em $B^\dagger$ ($\xi = \sqrt[4]{2}$) mas não se fatora linearmente em $B^\dagger$. Observe que só podemos decompor $x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x^2 + \sqrt{2})$ em $B^\dagger : \mathbb{Q}$. Similarmente, $C^\dagger$, $D^\dagger$ e $E^\dagger$ não são extensões normais.

De acordo com o teorema fundamental de Galois, o grupo de Galois de $A^\dagger : \mathbb{Q}$ é isomorfo ao grupo quociente $\dfrac{G}{A}$. Agora, como $\dfrac{G}{A} = \{A, \sigma A, \tau A, \sigma\tau A\}$ é isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$, calcularemos diretamente o grupo de Galois de $A^\dagger : \mathbb{Q}$. Como $A^\dagger = \mathbb{Q}[i, \sqrt{2}]$, há 4 $\mathbb{Q}-$automorfismos:

Tabela 4 – $\mathbb{Q}$-automorfismos de $\mathbb{Q}[i, \sqrt{2}]$

Automorfismo	Efeito em $\sqrt{2}$	Efeito em i
Id	$\sqrt{2}$	i
α	$-\sqrt{2}$	i
β	$\sqrt{2}$	$-i$
$\alpha\beta$	$-\sqrt{2}$	$-i$

Fonte: Os autores (2021)

Note que $\alpha^2 = \beta^2 = Id$ e $\alpha\beta = \beta\alpha$, como em $\mathbb{Z}_2 \times \mathbb{Z}_2$. Além disso, não devemos confundir estes automorfismos com os automorfismos encontrados na Tabela 3. Perceba que estes automorfismos tem como domínio e imagem o conjunto $\mathbb{Q}[i, \sqrt{2}]$, enquanto que os automorfismos descritos na Tabela 3 tem como domínio e imagem o conjunto $\mathbb{Q}[i, \sqrt[4]{2}]$. É interessante ver a aplicação do Item 5 do teorema fundamental de Galois, pois através dele podemos encontrar a estrutura do grupo de Galois de uma extensão menor, conhecendo o Grupo de Galois de uma extensão maior que a contém.

5.4.3 Exemplo 3

Neste exemplo, calcularemos o grupo de Galois associado a extensão $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$. Pela lei da torre, $[\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}] : \mathbb{Q}[\sqrt{2}, \sqrt{3}]] \cdot [\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}[\sqrt{2}]] \cdot [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}]$. O polinômio minimal de $\sqrt{5}$ sobre $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ é $x^2 - 5$, já que $\sqrt{5} \notin \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Assim $[\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}] : \mathbb{Q}[\sqrt{2}, \sqrt{3}]] = 2$. Da mesma forma, $\sqrt{3}$ é algébrico sobre $\mathbb{Q}[\sqrt{2}]$, e como $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$, seu polinômio minimal é $x^2 - 3$, portanto

$[\mathbb{Q}[\sqrt{2},\sqrt{3}] : \mathbb{Q}[\sqrt{2}]] = 2$. Por fim, sabemos pelo Exemplo 4.41 que $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$. Portanto $[\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}] : \mathbb{Q}] = 2 \cdot 2 \cdot 2 = 8$.

Podemos identificar os elementos dessa extensão: se $x \in \mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]$ então $x = a + b\sqrt{5}$, com $a, b \in \mathbb{Q}[\sqrt{2},\sqrt{3}]$. Mas se $y \in \mathbb{Q}[\sqrt{2},\sqrt{3}] = \mathbb{Q}[\sqrt{2}][\sqrt{3}]$, $y = c + d\sqrt{3}$, com $c, d \in \mathbb{Q}[\sqrt{2}]$. Logo $x = a + b\sqrt{5} = (a' + b'\sqrt{3}) + (a'' + b''\sqrt{3})\sqrt{5}$ com $a', b', a'', b'' \in \mathbb{Q}[\sqrt{2}]$, o que nos dá $a' = a_1 + a_2\sqrt{2}$, $b' = a_3 + a_4\sqrt{2}$, $a'' = a_5 + a_6\sqrt{2}$ e $b'' = a_7 + a_8\sqrt{2}$. Assim $x = [(a_1 + a_2\sqrt{2}) + (a_3 + a_4\sqrt{2})\sqrt{3}] + [(a_5 + a_6\sqrt{2}) + (a_7 + a_8\sqrt{2})\sqrt{3}]\sqrt{5} = a_1 + a_2\sqrt{2} + a_3\sqrt{3} + a_4\sqrt{2}\cdot\sqrt{3} + a_5\sqrt{5} + a_6\sqrt{2}\cdot\sqrt{5} + a_7\sqrt{3}\cdot\sqrt{5} + a_8\sqrt{2}\cdot\sqrt{3}\cdot\sqrt{5} = a_1 + a_2\sqrt{2} + a_3\sqrt{3} + a_4\sqrt{6} + a_5\sqrt{5} + a_6\sqrt{10} + a_7\sqrt{15} + a_8\sqrt{30}$. Portanto uma base para $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]$ é $\{1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}\}$.

Vamos encontrar o grupo de Galois associado à extensão $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}] : \mathbb{Q}$. Já sabemos que há três $\mathbb{Q}$-automorfismos de $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]$ (que permutam as raízes dos polinômios). Assim, há um $\mathbb{Q}$-automorfismo σ tal que $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = \sqrt{3}$ e $\sigma(\sqrt{5}) = \sqrt{5}$; há um $\mathbb{Q}$-automorfismo τ tal que $\tau(\sqrt{2}) = \sqrt{2}$, $\tau(\sqrt{3}) = -\sqrt{3}$ e $\sigma(\sqrt{5}) = \sqrt{5}$ e há um $\mathbb{Q}$-automorfismo ρ tal que $\rho(\sqrt{2}) = \sqrt{2}$, $\rho(\sqrt{3}) = \sqrt{3}$ e $\rho(\sqrt{5}) = -\sqrt{5}$. Esses automorfismos comutam e geram os demais $\mathbb{Q}$-automorfismos de $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]$, como podemos observar na Tabela 5.

Como $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]$ é o corpo de decomposição do polinômio $(x^2-2)(x^2-3)(x^2-5) = x^6 - 10x^4 + 31x^2 - 30$, pelo Teorema 4.55, $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]$ é uma extensão finita e normal. Assim, pelo Corolário 5.20 há exatamente $[\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}] : \mathbb{Q}]$ automorfismos. Como sabemos que a dimensão de $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}] = 8$, os automorfismos apresentados na Tabela 5 são todos os $\mathbb{Q}-$automorfismos de $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]$ (observe neste caso que o grau do polinômio é diferente do grau da extensão pois não calculamos o polinômio minimal referente a apenas um elemento, para que a extensão fosse simples).

Agora, vamos encontrar a estrutura abstrata do grupo de Galois associado à extensão $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]$. Podemos observar que $(\sigma)^2 = (\tau)^2 = (\rho)^2 = Id$, além disso $\sigma\tau = \tau\sigma$, $\sigma\rho = \rho\sigma$ e $\tau\rho = \rho\tau$. Portanto $G = \Gamma(\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}] : \mathbb{Q}) = \langle\sigma,\tau,\rho\rangle = \{Id,\sigma\} \times \{Id,\tau\} \times \{Id,\rho\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Vamos determinar os subgrupos de G:

- Ordem 8: $G = \langle\sigma,\tau,\rho\rangle = \{Id,\sigma\} \times \{Id,\tau\} \times \{Id,\rho\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$;
- Ordem 4:
  - $S = \{Id,\sigma,\tau,\sigma\tau\} = \langle\sigma,\tau\rangle = \{Id,\sigma\} \times \{Id,\tau\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$;
  - $T = \{Id,\sigma,\rho,\sigma\rho\} = \langle\sigma,\rho\rangle = \{Id,\sigma\} \times \{Id,\rho\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$;
  - $U = \{Id,\tau,\rho,\tau\rho\} = \langle\tau,\rho\rangle = \{Id,\tau\} \times \{Id,\rho\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$;
  - $V = \{Id,\sigma,\tau\rho,\sigma\tau\rho\} = \langle\sigma,\tau\rho\rangle = \{Id,\sigma\} \times \{Id,\tau\rho\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$;

Tabela 5 – $\mathbb{Q}$-automorfismos de $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$

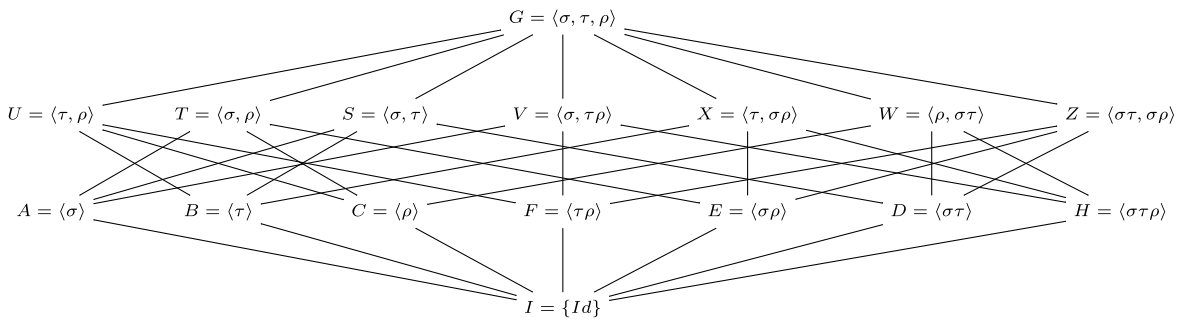
Automorfismo	Efeito em $\sqrt{2}$	Efeito em $\sqrt{3}$	Efeito em $\sqrt{5}$
Id	$\sqrt{2}$	$\sqrt{3}$	$\sqrt{5}$
σ	$-\sqrt{2}$	$\sqrt{3}$	$\sqrt{5}$
τ	$\sqrt{2}$	$-\sqrt{3}$	$\sqrt{5}$
ρ	$\sqrt{2}$	$\sqrt{3}$	$-\sqrt{5}$
$\sigma\tau$	$-\sqrt{2}$	$-\sqrt{3}$	$\sqrt{5}$
$\sigma\rho$	$-\sqrt{2}$	$\sqrt{3}$	$-\sqrt{5}$
$\tau\rho$	$\sqrt{2}$	$-\sqrt{3}$	$-\sqrt{5}$
$\sigma\tau\rho$	$-\sqrt{2}$	$-\sqrt{3}$	$-\sqrt{5}$

Fonte: Os autores (2021)

  - $X = \{Id, \tau, \sigma\rho, \sigma\tau\rho\} = \langle \tau, \sigma\rho \rangle = \{Id, \tau\} \times \{Id, \sigma\rho\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$;
  - $W = \{Id, \rho, \sigma\tau, \sigma\tau\rho\} = \langle \rho, \sigma\tau \rangle = \{Id, \rho\} \times \{Id, \sigma\tau\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$;
  - $Z = \{Id, \sigma\tau, \sigma\rho, \tau\rho\} = \langle \sigma\tau, \sigma\rho \rangle = \{Id, \sigma\tau\} \times \{Id, \sigma\rho\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$;

- Ordem 2:
  - $A = \{Id, \sigma\} = \langle \sigma \rangle \simeq \mathbb{Z}_2$;
  - $B = \{Id, \tau\} = \langle \tau \rangle \simeq \mathbb{Z}_2$;
  - $C = \{Id, \rho\} = \langle \rho \rangle \simeq \mathbb{Z}_2$;
  - $D = \{Id, \sigma\tau\} = \langle \sigma\tau \rangle \simeq \mathbb{Z}_2$;
  - $E = \{Id, \sigma\rho\} = \langle \sigma\rho \rangle \simeq \mathbb{Z}_2$;
  - $F = \{Id, \tau\rho\} = \langle \tau\rho \rangle \simeq \mathbb{Z}_2$;
  - $H = \{Id, \sigma\tau\rho\} = \langle \sigma\tau\rho \rangle \simeq \mathbb{Z}_2$;
- Ordem 1: $I = \{Id\}$.

Construindo o diagrama dos subgrupos de G:



Vamos calcular os corpos intermediários, identificando cada automorfismo que fixa os subcorpos de $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$.

Já vimos que uma base de $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]$ é $\{1,\sqrt{2},\sqrt{3},\sqrt{5},\sqrt{6},\sqrt{10},\sqrt{15},\sqrt{30}\}$. Logo se $x \in \mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]$ então $x = a_0 + a_1\sqrt{2} + a_3\sqrt{3} + a_4\sqrt{5} + a_5\sqrt{6} + a_6\sqrt{10} + a_7\sqrt{15} + a_7\sqrt{30}$, com $a_i \in \mathbb{Q}$, $i = 0,\ldots,7$.

Neste exemplo faremos a construção dos corpos intermediários de uma maneira diferente em relação aos exemplos anteriores. Primeiramente, vamos identificar todos os subcorpos de $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]$ e depois veremos quais automorfismos fixam cada um dos subcorpos. O objetivo através desse encaminhamento é evitar contas exageradas, já que neste exemplo é mais fácil ver quais são os corpos fixos.

Como vimos anteriormente, há 7 subgrupos de ordem 2 e 7 subgrupos de ordem 4, portanto há 7 extensões de dimensão 4 e 7 extensões de dimensão 2 entre $\mathbb{Q}$ e $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]$. Observe que para os outros subgrupos triviais $I = \{Id\}$ e $G = \langle\sigma,\tau,\rho\rangle$ já sabemos os corpos fixos: I fixa o corpo $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]$ e G fixa o corpo $\mathbb{Q}$.

Vamos começar encontrando as extensões de grau 2.

Já vimos anteriormente que $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a,b \in \mathbb{Q}\}$ é corpo e $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]$. Como a extensão $\mathbb{Q}[\sqrt{2}] : \mathbb{Q}$ tem grau 2, é uma das extensões procuradas. As demais extensões são $\mathbb{Q}[\sqrt{3}], \mathbb{Q}[\sqrt{5}], \mathbb{Q}[\sqrt{6}], \mathbb{Q}[\sqrt{10}], \mathbb{Q}[\sqrt{15}]$ e $\mathbb{Q}[\sqrt{30}]$. Portanto as extensões de grau 2 são:

- $\mathbb{Q}[\sqrt{2}] = \{a_0 + a_1\sqrt{2} \mid a_0, a_1 \in \mathbb{Q}\}$;
- $\mathbb{Q}[\sqrt{3}] = \{a_0 + a_1\sqrt{3} \mid a_0, a_1 \in \mathbb{Q}\}$;
- $\mathbb{Q}[\sqrt{5}] = \{a_0 + a_1\sqrt{5} \mid a_0, a_1 \in \mathbb{Q}\}$;
- $\mathbb{Q}[\sqrt{6}] = \{a_0 + a_1\sqrt{6} \mid a_0, a_1 \in \mathbb{Q}\}$;
- $\mathbb{Q}[\sqrt{10}] = \{a_0 + a_1\sqrt{10} \mid a_0, a_1 \in \mathbb{Q}\}$;
- $\mathbb{Q}[\sqrt{15}] = \{a_0 + a_1\sqrt{15} \mid a_0, a_1 \in \mathbb{Q}\}$;
- $\mathbb{Q}[\sqrt{30}] = \{a_0 + a_1\sqrt{30} \mid a_0, a_1 \in \mathbb{Q}\}$;

Além disso, há 7 extensões de grau 4, que são formadas pelas adjunções de elementos da base nas extensões acima (a menos de repetições). Por exemplo, ao adjuntar $\sqrt{3}$ na extensão $\mathbb{Q}[\sqrt{2}]$, obtemos a extensão $\mathbb{Q}[\sqrt{2},\sqrt{3}] = \{a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6} \mid a_0,a_1,a_2,a_3 \in \mathbb{Q}\}$. Observe que ao adjuntar $\sqrt{3}$ à extensão $\mathbb{Q}[\sqrt{6}]$ obtemos a mesma extensão que $\mathbb{Q}[\sqrt{2},\sqrt{3}]$. Após calcular as extensões diferentes, encontramos os corpos:

- $\mathbb{Q}[\sqrt{2},\sqrt{3}] = \{a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6} \mid a_0,a_1,a_2,a_3 \in \mathbb{Q}\}$;
- $\mathbb{Q}[\sqrt{2},\sqrt{5}] = \{a_0 + a_1\sqrt{2} + a_2\sqrt{5} + a_3\sqrt{10} \mid a_0,a_1,a_2,a_3 \in \mathbb{Q}\}$;

⋆ $\mathbb{Q}[\sqrt{3},\sqrt{5}] = \{a_0 + a_1\sqrt{3} + a_2\sqrt{5} + a_3\sqrt{15} \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$;

⋆ $\mathbb{Q}[\sqrt{5},\sqrt{6}] = \{a_0 + a_1\sqrt{5} + a_2\sqrt{6} + a_3\sqrt{30} \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$;

⋆ $\mathbb{Q}[\sqrt{3},\sqrt{10}] = \{a_0 + a_1\sqrt{3} + a_2\sqrt{10} + a_3\sqrt{30} \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$;

⋆ $\mathbb{Q}[\sqrt{2},\sqrt{15}] = \{a_0 + a_1\sqrt{2} + a_2\sqrt{15} + a_3\sqrt{30} \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$;

⋆ $\mathbb{Q}[\sqrt{6},\sqrt{10},\sqrt{15}] = \{a_0 + a_1\sqrt{6} + a_2\sqrt{10} + a_3\sqrt{15} \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$;

Agora que encontramos todas as extensões, vamos calcular o Grupo de Galois de cada extensão. Para isso, vamos aplicar os automorfismos da Tabela 5 no elemento $x = a_0 + a_1\sqrt{2} + a_3\sqrt{3} + a_4\sqrt{5} + a_5\sqrt{6} + a_6\sqrt{10} + a_7\sqrt{15} + a_7\sqrt{30}$:

- $Id(x) = x$;
- $\sigma(x) = a_0 - a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{5} - a_4\sqrt{6} - a_5\sqrt{10} + a_6\sqrt{15} - a_7\sqrt{30}$;
- $\tau(x) = a_0 + a_1\sqrt{2} - a_2\sqrt{3} + a_3\sqrt{5} - a_4\sqrt{6} + a_5\sqrt{10} - a_6\sqrt{15} - a_7\sqrt{30}$;
- $\rho(x) = a_0 + a_1\sqrt{2} + a_2\sqrt{3} - a_3\sqrt{5} + a_4\sqrt{6} - a_5\sqrt{10} - a_6\sqrt{15} - a_7\sqrt{30}$;
- $\sigma\tau(x) = a_0 - a_1\sqrt{2} - a_2\sqrt{3} + a_3\sqrt{5} + a_4\sqrt{6} - a_5\sqrt{10} - a_6\sqrt{15} + a_7\sqrt{30}$;
- $\sigma\rho(x) = a_0 - a_1\sqrt{2} + a_2\sqrt{3} - a_3\sqrt{5} - a_4\sqrt{6} + a_5\sqrt{10} - a_6\sqrt{15} + a_7\sqrt{30}$;
- $\tau\rho(x) = a_0 + a_1\sqrt{2} - a_2\sqrt{3} - a_3\sqrt{5} - a_4\sqrt{6} - a_5\sqrt{10} + a_6\sqrt{15} + a_7\sqrt{30}$;
- $\sigma\tau\rho(x) = a_0 - a_1\sqrt{2} - a_2\sqrt{3} - a_3\sqrt{5} + a_4\sqrt{6} + a_5\sqrt{10} + a_6\sqrt{15} + a_7\sqrt{30}$;

Observe que:

∗ Os $\mathbb{Q}$-automorfismos que fixam os elementos de $\mathbb{Q}[\sqrt{2}]$ (a_0 e $a_1\sqrt{2}$) são Id, τ, ρ e $\tau\rho$. Logo o subgrupo associado à extensão $\mathbb{Q}[\sqrt{2}]$ é $U = \langle\tau, \rho\rangle$.

∗ Os $\mathbb{Q}$-automorfismos que fixam os elementos a_0 e $a_2\sqrt{3}$ são $Id, \sigma, \rho, \sigma\rho$. Logo $\Gamma(\mathbb{Q}[\sqrt{3}] : \mathbb{Q}) = T = \langle\sigma, \rho\rangle$.

∗ Os $\mathbb{Q}$-automorfismos que fixam os elementos a_0 e $a_3\sqrt{5}$ são $Id, \sigma, \tau, \sigma\tau$. Logo $\Gamma(\mathbb{Q}[\sqrt{5}] : \mathbb{Q}) = S = \langle\sigma, \tau\rangle$.

∗ Os $\mathbb{Q}$-automorfismos que fixam os elementos a_0 e $a_4\sqrt{6}$ são $Id, \rho, \sigma\tau, \sigma\tau\rho$. Logo $\Gamma(\mathbb{Q}[\sqrt{6}] : \mathbb{Q}) = W = \langle\rho, \sigma\tau\rangle$.

∗ Os $\mathbb{Q}$-automorfismos que fixam os elementos a_0 e $a_5\sqrt{10}$ são $Id, \sigma\rho, \tau, \sigma\tau\rho$. Logo $\Gamma(\mathbb{Q}[\sqrt{10}] : \mathbb{Q}) = X = \langle\tau, \sigma\rho\rangle$.

* Os $\mathbb{Q}$-automorfismos que fixam os elementos a_0 e $a_6\sqrt{15}$ são $Id, \sigma, \tau\rho, \sigma\tau\rho$. Logo $\Gamma(\mathbb{Q}[\sqrt{15}] : \mathbb{Q}) = V = \langle \sigma, \tau\rho \rangle$.

* Os $\mathbb{Q}$-automorfismos que fixam os elementos a_0 e $a_7\sqrt{30}$ são $Id, \sigma\tau, \sigma\rho, \tau\rho$. Logo $\Gamma(\mathbb{Q}[\sqrt{30}] : \mathbb{Q}) = Z = \langle \sigma\tau, \sigma\rho \rangle$.

* Os $\mathbb{Q}$-automorfismos que fixam os elementos de $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ são Id, ρ. Logo $\Gamma(\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}) = C = \langle \rho \rangle$.

* Os $\mathbb{Q}$-automorfismos que fixam os elementos $a_0 + a_1\sqrt{2} + a_3\sqrt{5} + a_5\sqrt{10}$ são Id, τ. Logo $\Gamma(\mathbb{Q}[\sqrt{2}, \sqrt{5}] : \mathbb{Q}) = B = \langle \tau \rangle$.

* Os $\mathbb{Q}$-automorfismos que fixam os elementos $a_0 + a_2\sqrt{3} + a_3\sqrt{5} + a_6\sqrt{15}$ são Id, σ. Logo $\Gamma(\mathbb{Q}[\sqrt{3}, \sqrt{5}] : \mathbb{Q}) = A = \langle \sigma \rangle$.

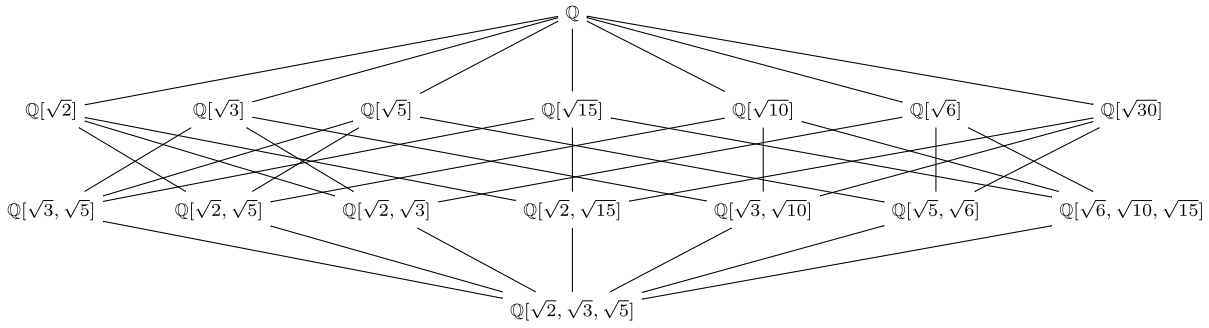
* Os $\mathbb{Q}$-automorfismos que fixam os elementos $a_0 + a_3\sqrt{5} + a_4\sqrt{6} + a_7\sqrt{30}$ são $Id, \sigma\tau$. Logo $\Gamma(\mathbb{Q}[\sqrt{5}, \sqrt{6}] : \mathbb{Q}) = D = \langle \sigma\tau \rangle$.

* Os $\mathbb{Q}$-automorfismos que fixam os elementos $a_0 + a_2\sqrt{3} + a_5\sqrt{10} + a_7\sqrt{30}$ são $Id, \sigma\rho$. Logo $\Gamma(\mathbb{Q}[\sqrt{3}, \sqrt{10}] : \mathbb{Q}) = E = \langle \sigma\rho \rangle$.

* Os $\mathbb{Q}$-automorfismos que fixam os elementos $a_0 + a_1\sqrt{2} + a_6\sqrt{15} + a_7\sqrt{30}$ são $Id, \tau\rho$. Logo $\Gamma(\mathbb{Q}[\sqrt{2}, \sqrt{15}] : \mathbb{Q}) = F = \langle \tau\rho \rangle$.

* Os $\mathbb{Q}$-automorfismos que fixam os elementos $a_0 + a_4\sqrt{6} + a_5\sqrt{10} + a_6\sqrt{15}$ são $Id, \sigma\tau\rho$. Logo $\Gamma(\mathbb{Q}[\sqrt{6}, \sqrt{10}, \sqrt{15}] : \mathbb{Q}) = H = \langle \sigma\tau\rho \rangle$.

Portanto, podemos construir o reticulado dos subcorpos intermediários de $\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$:



5.4.4 Exemplo 4

A construção dos números complexos como estudamos hoje levou alguns séculos até ser consolidada. No primeiros milênios da história da matemática, os matemáticos ainda não compreendiam o que raízes de números negativos representavam, e equações da forma $x^2 + 1 = 0$ eram tidas como impossíveis de resolver.

A partir do século XVI, com o desenvolvimento da fórmula resolutiva para equações cúbicas, os matemáticos começaram a investigar e compreender melhor como os números complexos se comportavam. Nesse contexto, iniciou-se o estudo das raízes n-ésimas de um número complexo, ou seja, dado um número complexo z, quais valores ω pode assumir para que $\omega^n = z$?

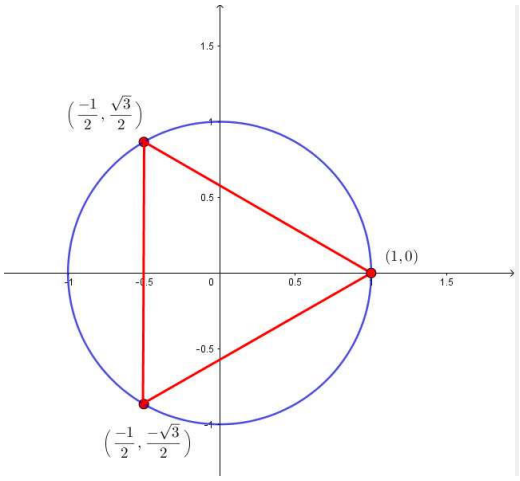
Em especial, quais os valores de ω para que $\omega^n = 1$? Neste caso, dizemos que ω é uma **raiz da unidade**. Utilizando a fórmula de De Moivre, encontramos que as raízes da unidade são da forma

$$\omega_k = \cos\frac{2\pi k}{n} + i\,\text{sen}\,\frac{2\pi k}{n} \qquad k = 0, \ldots, n-1.$$

Essas raízes tem uma propriedade muito bonita. Elas dividem a circunferência unitária em n partes iguais, sendo $\omega_0 = 1$. Assim, se $n \geq 3$, as raízes n-ésimas da unidade são vértices de um polígono regular de n lados inscrito em uma circunferência unitária com centro na origem.

Exemplo 5.26. *Se $n = 3$, as raízes cúbicas da unidade são $\omega_0 = 1, \omega_1 = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$ e $\omega_2 = -\frac{1}{2} - \frac{i\sqrt{3}}{2}$.*

Figura 7 – Triângulo equilátero inscrito em uma circunferência unitária com centro na origem, formado pelas raízes cúbicas da unidade



Fonte: Os autores (2021)

Vamos explorar mais este exemplo. A fim de facilitar a compreensão, chamaremos $\omega_1 = u$. Observe que $u^2 = \left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right)^2 = -\frac{1}{2} - \frac{i\sqrt{3}}{2} = \omega_2$. Além disso, $\omega_2^2 = \left(-\frac{1}{2} - \frac{i\sqrt{3}}{2}\right)^2 = -\frac{1}{2} + \frac{i\sqrt{3}}{2} = u$. Ou seja, $(\omega_1)^2 = u^2 = \omega_2$ e $\omega_2^2 = (u^2)^2 = u^4 = u = \omega_1$. Assim, encontramos que $\omega_1 \cdot \omega_2 = 1$, o que nos dá $\omega_1^{-1} = u^{-1} = \omega_2 = u^2$ e $\omega_2^{-1} = (u^2)^{-1} = u = \omega_1$.

Então u e u^2 são inversos com respeito a multiplicação. Observe que um ciclo vai se formando: $\omega_0 = 1 \cdot u = u$, $\omega_1 \cdot u = u \cdot u = u^2 = \omega_2$ e $\omega_2 \cdot u = u^2 \cdot u = u^3 = 1$. Assim, as três raízes cúbicas da unidade formam um grupo cíclico, de ordem 3, gerado por u.

Resumindo, as raízes cúbicas da unidade são $1, u$ e u^2, em que $u = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$. Algumas relações que encontramos são:

$$u^2 = -u - 1,\ u^4 = u,\ u^{-1} = u^2,\ (u^2)^{-1} = u \tag{5.1}$$

Elas formam um grupo cíclico, gerado por u. Observe também que $-u - 1 = -\left(-\frac{1}{2} + \frac{i\sqrt{3}}{2} \right) - 1 = \frac{1}{2} - \frac{i\sqrt{3}}{2} - 1 = -\frac{1}{2} - \frac{i\sqrt{3}}{2} = u^2$. Logo, u é raiz do polinômio $x^2 + x + 1$.

Proposição 5.27. *Seja z um número complexo não nulo, $\omega \in \mathbb{C}$ um raiz n-ésima de z e $\zeta_n = \cos\frac{2\pi}{n} + i\,\mathrm{sen}\,\frac{2\pi}{n}$. Então as raízes de z são $\omega \cdot \zeta_n^k$, $k = 1, \ldots, n$.*

Demonstração. A demonstração pode ser encontrada em [REZENDE, 2017], p. 38. □

Observe que as potências de ζ_n fornecem todas as raízes n-ésimas da unidade, que representaremos por $U_n(\mathbb{C}) = \{\zeta_n^m \mid m \in \mathbb{Z}\}$.

Dizemos que uma raiz n-ésima da unidade ω é **primitiva** se $U_n(\mathbb{C}) = \{\omega^m \mid m \in \mathbb{Z}\}$. Em outras palavras, é possível encontrar todas as demais raízes n-ésimas a partir de ω. Observe também que $U_n(\mathbb{C})$ é um grupo multiplicativo, cujo gerador é uma raiz n-ésima da unidade ω.

Definição 5.28. *Seja ζ_n um raiz n-ésima primitiva da unidade. Um **corpo ciclotômico** L é uma extensão de $\mathbb{Q}$ gerada por ζ_n, ou seja, $L = \mathbb{Q}[\zeta_n]$.*

Em especial, o corpo L é o corpo de decomposição do polinômio $x^n - 1$ sobre $\mathbb{Q}$.

Definição 5.29. *Dado um inteiro positivo n, o n-ésimo **polinômio ciclotômico** é o polinômio mônico cujas raízes são simples e são n-ésimas primitivas da unidade, isto é, o polinômio*

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n, \\ mdc(k,n)=1}} (x - \zeta_n^k)$$

em que ζ_n é uma raiz n-ésima primitiva da unidade.

Assim $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$, $\Phi_4(x) = x^2 + 1$, $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, etc. Observe que o grau de $\Phi_n(x)$ é $\phi(n)$, em que ϕ é a função totiente ou função de Euler.[1]

[1] O número $\phi(n)$ representa a quantidade de números menores que n que são inversíveis (mod n). Se p for um número primo, teremos $\phi(p) = p - 1$.

Um fato curioso (que pode ser provado) é que $x^n - 1 = \prod_{d|n} \Phi_d(x)$. Por exemplo, $x^4 - 1 = \prod_{d|4} \Phi_d(x) = \Phi_1(x) \cdot \Phi_2(x) \cdot \Phi_4(x) = (x-1) \cdot (x+1) \cdot (x^2+1)$.

Além disso, se p é primo, temos $\Phi_p(x) = \dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$. Com exceção do 1, todas as demais raízes de $x^p - 1$ são primitivas.

Vale destacar que para todo $n \geq 1$, o polinômio ciclotômico $\Phi_n(x)$ é irredutível sobre $\mathbb{Q}$.

Teorema 5.30. *Seja K um corpo de característica 0, e seja L o corpo de decomposição do polinômio $x^n - 1$ sobre K. Então $\Gamma(L : K)$ é isomorfo ao grupo multiplicativo R_n formado pelas classes $\overline{r} \pmod n$ tal que $mdc(r, n) = 1$.*

Demonstração. A demonstração pode ser encontrada em [HOWIE, 2006], p.138. □

Exemplo 5.31. *O grupo de Galois do polinômio $f(x) = x^8 - 1$ sobre $\mathbb{Q}$ é isomorfo ao grupo multiplicativo $R_8 = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$.*

Neste exemplo, uma raiz 8-ésima primitiva da unidade é $\omega = \dfrac{\sqrt{2}}{2} + \dfrac{\sqrt{2}i}{2}$. O corpo de decomposição $Gal(x^8 - 1, \mathbb{Q})$ é $\mathbb{Q}[\omega]$. Assim, os elementos do grupo de Galois atuam da seguinte forma: $Id : \omega \to \omega$, $\sigma : \omega \to \omega^3$, $\tau : \omega \to \omega^5$ e $\rho : \omega \to \omega^7$.

Logo $\Gamma(\mathbb{Q}[\omega] : \mathbb{Q}) = R_8 = \{Id, \sigma, \tau, \rho\}$ é isomorfo ao grupo de Klein ou $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Corolário 5.32. *Seja K um corpo de característica 0 e seja L o corpo de decomposição sobre K do polinômio $x^p - 1$, em que p é primo. Então $\Gamma(L : K)$ é cíclico.*[2]

Demonstração. A demonstração pode ser encontrada em [HOWIE, 2006], p.139. □

Quando p é primo, o polinômio $x^p - 1$ pode ser fatorado da forma $x^p - 1 = \Phi_1(x) \cdot \Phi_p(x) = (x-1)(x^{p-1} + x^{p-2} + \ldots + x + 1)$. Assim, com exceção do 1, todas as demais raízes de $x^p - 1$ são primitivas. Os elementos do grupo de Galois irão permutar tais raízes, logo o grupo de Galois de $x^p - 1$ sobre $\mathbb{Q}$ será $\mathbb{Z}_p^*$, que é um grupo cíclico. Se ζ é uma raiz primitiva de $x^p - 1$, os elementos do grupo de Galois serão: $Id : \zeta \to \zeta$, $\sigma : \zeta \to \zeta^2$, $\sigma^2 : \zeta \to \zeta^4$, etc.

Vamos apresentar um exemplo mais detalhado. Seja $L = Gal(x^{11} - 1, \mathbb{Q})$ o corpo de decomposição do polinômio $x^{11} - 1$. As 11 raízes de $x^{11} - 1$ são 1 e $u = \cos\dfrac{2\pi}{11} + i \operatorname{sen}\dfrac{2\pi}{11}, u^2, u^3, \ldots, u^{10}$. Assim, o corpo de decomposição será $L = \mathbb{Q}[u]$. Como $x^{11} - 1 = (x-1)(x^{10} + x^9 + \ldots + x + 1)$, e $x^{10} + x^9 + \ldots + x + 1$ é irredutível sobre $\mathbb{Q}$, temos $[\mathbb{Q}[u] : \mathbb{Q}] = 10$.

Vamos considerar o $\mathbb{Q}$-automorfismo $\sigma : u \to u^2$. Podemos encontrar todos os demais $\mathbb{Q}$-automorfismos, que podem ser observados na Tabela 6:

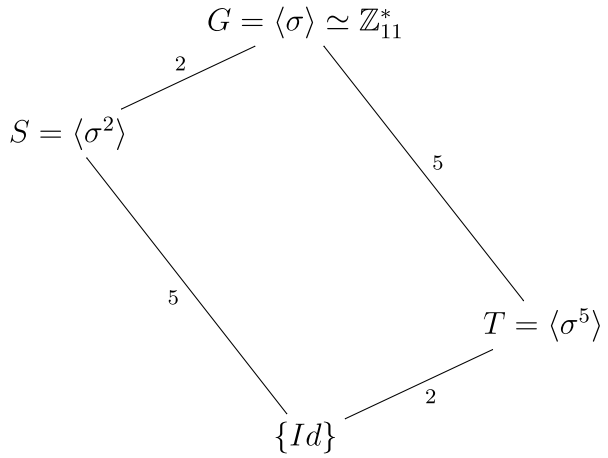
[2] Como $\Gamma(L : K)$ é cíclico, decorre que $\Gamma(L : K)$ é abeliano.

Tabela 6 – $\mathbb{Q}$-automorfismos de $\mathbb{Q}[u]$, em que u é uma raiz 11-ésima primitiva da unidade

Automorfismo	Efeito em u
Id	u
σ	u^2
σ^2	u^4
σ^3	u^8
σ^4	u^5
σ^5	u^{10}
σ^6	u^9
σ^7	u^7
σ^8	u^3
σ^9	u^6
$\sigma^{10} = Id$	u

Fonte: Os autores (2021)

Observe que o grupo de Galois G associado a extensão $\mathbb{Q}[u] : \mathbb{Q}$ é isomorfo ao grupo multiplicativo $\mathbb{Z}_{11}^*$. Os subgrupos de G são $\{Id\}$, $S = \langle\sigma^2\rangle = \{Id, \sigma^2, \sigma^4, \sigma^6, \sigma^8\}$, $T = \langle\sigma^5\rangle = \{Id, \sigma^5\}$ e G, que podem ser observados no diagrama abaixo:



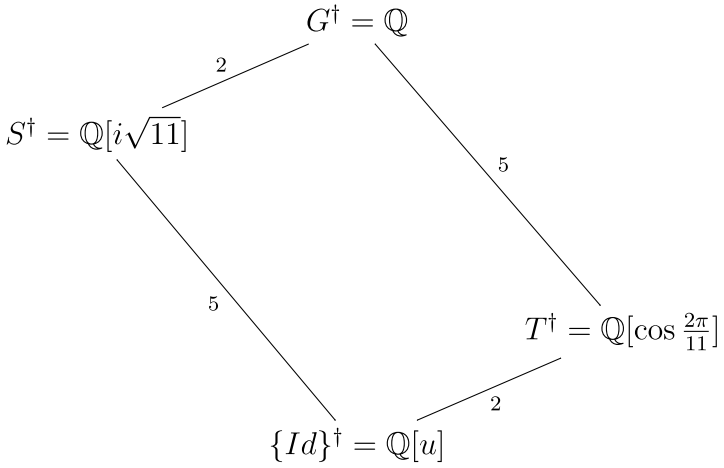
Agora, vamos calcular os corpos intermediários da extensão $\mathbb{Q}[u] : \mathbb{Q}$. Como essa extensão é normal, temos $\{Id\}^\dagger = \mathbb{Q}[u]$ e $G^\dagger = \mathbb{Q}$.

Para calcular o corpo fixo associado ao grupo $S = \langle\sigma^2\rangle$, vamos ver quais elementos são fixos pelo automorfismo σ^2. Como $\sigma^2(u) = u^4$, $\sigma^2(u^4) = \sigma^4(u) = u^5$, $\sigma^2(u^5) = \sigma^6(u) = u^9$, $\sigma^2(u^9) = \sigma^8(u) = u^3$ e $\sigma^2(u^3) = \sigma^{10} = u$, segue que $\sigma^2(u + u^3 + u^4 + u^5 + u^9) = u + u^3 + u^4 + u^5 + u^9$, ou seja, σ^2 fixa o elemento $u + u^3 + u^4 + u^5 + u^9$. Se considerarmos $w = u + u^3 + u^4 + u^5 + u^9$, temos $\mathbb{Q}[w] \subseteq S^\dagger$. Além disso, $\overline{w} = \overline{u + u^3 + u^4 + u^5 + u^9} = \overline{u} + \overline{u^3} + \overline{u^4} + \overline{u^5} + \overline{u^9} = u^2 + u^6 + u^7 + u^8 + u^{10}$ e $\sigma^2(\overline{w}) = \overline{w}$, assim S também fixa $\overline{w}$.

Seja $f_w(x)$ o polinômio minimal de w. Como $[\mathbb{Q}[w] : \mathbb{Q}] = 2$, pela Proposição 4.45, encontramos que $f_w(x)$ tem grau 2. Como as raízes de f_w são w e $\overline{w}$, temos $f_w(x) =$

$(x-w)(x-\overline{w}) = x^2+x+3$.[3] Observe que as raízes de f_w são $\dfrac{-1\pm\sqrt{-11}}{2}$. Assim, f_w é irredutível sobre $\mathbb{Q}$ e $\mathbb{Q}[w] = \mathbb{Q}[i\sqrt{11}]$. Como $[\mathbb{Q}[i\sqrt{11}] : \mathbb{Q}] = [S^\dagger : \mathbb{Q}] = 2$, concluímos que $S^\dagger = \mathbb{Q}[i\sqrt{11}]$.

Agora, vamos calcular o corpo fixo de $T = \langle\sigma^5\rangle$. Como $\sigma^5(u) = u^{10}$ e $\sigma^5(u^{10}) = \sigma^{10}(u) = u$, segue que $\sigma^5(u+u^{10}) = u+u^{10}$. Além disso, $\sigma^5(u^2+u^9) = u^2+u^9$, $\sigma^5(u^3+u^8) = u^3+u^8$, $\sigma^5(u^4+u^7) = u^4+u^7$ e $\sigma^5(u^5+u^6) = u^5+u^6$. Dessa forma, T fixa os elementos $u+u^{10}$, u^2+u^9, u^3+u^8, u^4+u^7 e u^5+u^6. Seja $f_t(x)$ o polinômio minimal de $u+u^{10}$, que tem grau 5. Como $u+u^{10}$, u^2+u^9, u^3+u^8, u^4+u^7 e u^5+u^6 são fixados pelos elementos de T, podemos supor que as outras raízes de f_t são u^2+u^9, u^3+u^8, u^4+u^7 e u^5+u^6. Assim, $f_t(x) = (x-(u+u^{10}))\cdot(x-(u^2+u^9))\cdot(x-(u^3+u^8))\cdot(x-(u^4+u^7))\cdot(x-(u^5+u^6)) = x^5+x^4-4x^3-3x^2+3x+1$. Observe que f_t é irredutível sobre $\mathbb{Q}$. Como $[\mathbb{Q}[u+u^{10}] : \mathbb{Q}] = [T^\dagger : \mathbb{Q}] = 5$, temos que $T^\dagger = \mathbb{Q}[u+u^{10}]$. Como $u = \cos\dfrac{2\pi}{11} + i\,\mathrm{sen}\,\dfrac{2\pi}{11}$ e $u^{10} = \overline{u} = \cos\dfrac{2\pi}{11} - i\,\mathrm{sen}\,\dfrac{2\pi}{11}$, $u+u^{10} = u+\overline{u} = 2\cos\dfrac{2\pi}{11}$. Portanto o corpo intermediário associado ao grupo T é $\mathbb{Q}[2\cos\dfrac{2\pi}{11}] = \mathbb{Q}[\cos\dfrac{2\pi}{11}]$.



Observe que as extensões intermediárias são normais, visto que G é abeliano. Assim, $S^\dagger$ é o corpo de decomposição do polinômio x^2+11 e $T^\dagger$ é o corpo de decomposição do polinômio $f(x) = x^5 + \dfrac{x^4}{2} - x^3 - \dfrac{3x^2}{8} + \dfrac{3x}{16} + \dfrac{1}{32}$. Em especial, as raízes de $f(x)$ são $\cos\dfrac{2\pi}{11}$, $\cos\dfrac{4\pi}{11}$, $\cos\dfrac{6\pi}{11}$, $\cos\dfrac{8\pi}{11}$ e $\cos\dfrac{10\pi}{11}$.

5.4.5 Exemplo 5

Vamos estudar o polinômio $f(x) = x^3-2$ sobre $\mathbb{Q}$. Sabemos que $\alpha = \sqrt[3]{2}$ é uma raiz de $f(x)$, no entanto $\alpha \notin \mathbb{Q}$. Assim, considere a extensão $\mathbb{Q}[\alpha]$. Como $f(x)$ é o polinômio minimal de α sobre $\mathbb{Q}$, $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$. Além disso, $\mathbb{Q}[\alpha] = \{a_0+a_1\alpha+a_2\alpha^2 \mid a_0,a_1,a_2 \in \mathbb{Q}\}$ e $f(x) = x^3-2$ se fatora como $f(x) = (x-\alpha)(x^2+\alpha x+\alpha^2)$. Perceba que $p(x) = x^2+\alpha x+\alpha^2$

[3] Para encontrar este resultado, usamos $u^{11} = 1$ e $u^{10}+u^9+u^8+u^7+u^6+u^5+u^4+u^3+u^2+u = -1$.

possui raízes complexas, que são αu e αu^2, em que $u = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$ denota a raiz cúbica da unidade.

Observe que $u \notin \mathbb{Q}[\alpha]$, assim podemos construir uma nova extensão, $\mathbb{Q}[\alpha][u] = \mathbb{Q}[\alpha, u]$. Como $[\mathbb{Q}[\alpha, u] : \mathbb{Q}] = [\mathbb{Q}[\alpha, u] : \mathbb{Q}[\alpha]] \cdot [\mathbb{Q}[\alpha] : \mathbb{Q}]$, e $p(x)$ é irredutível sobre $\mathbb{Q}[\alpha]$, temos que $[\mathbb{Q}[\alpha, u] : \mathbb{Q}] = 2 \cdot 3 = 6$.

Já vimos que as raízes de $f(x)$ são α, αu e αu^2, que estão todas em $\mathbb{Q}[\alpha, u]$, portanto $\mathbb{Q}[\alpha, u]$ é o corpo de decomposição de $f(x)$ (veja que é o menor, pois qualquer outro corpo que contém α, αu e αu^2 necessariamente contém $\{\alpha, u\}$ e dessa forma contém $\mathbb{Q}[\alpha, u]$). Além disso, os elementos de $\mathbb{Q}[\alpha, u]$ são da forma $a + bu$, com $a, b \in \mathbb{Q}[\alpha]$. Se $a = a_0 + a_1\alpha + a_2\alpha^2$ e $b = a_3 + a_4\alpha + a_5\alpha^2$, então $x = a_0 + a_1\alpha + a_2\alpha^2 + (a_3 + a_4\alpha + a_5\alpha^2)u = a_0 + a_1\alpha + a_2 + a_3u + a_4\alpha u + a_5\alpha^2 u$. Assim, uma base para a extensão $\mathbb{Q}[\alpha, u]$ em $\mathbb{Q}$ é $\{1, \alpha, \alpha^2, u, \alpha u, \alpha^2 u\}$.

Agora, vamos encontrar o grupo de Galois de $\mathbb{Q}[\alpha, u]$ sobre $\mathbb{Q}$. Vamos apresentar duas maneiras de fazer essa construção: permutar os elementos que foram adjuntados com as raízes e permutar as raízes entre si (poderíamos ter apresentado as duas formas nos exemplos anteriores, mas acreditamos que é mais adequado neste exemplo pois temos menos elementos para permutar).

Primeira maneira: Seja $\gamma \in \Gamma(\mathbb{Q}[\alpha, u] : \mathbb{Q})$ um $\mathbb{Q}$-automorfismo qualquer. Como γ atua no elementos α e u?

Observe que $\alpha^3 = 2$, assim $\gamma(\alpha^3) = \gamma(2)$. Como γ é um automorfismo que fixa $\mathbb{Q}$, encontramos que $(\gamma(\alpha))^3 = 2$, ou seja, $\gamma(\alpha)$ é raiz do polinômio $f(x) = x^3 - 2$. Logo $\gamma(\alpha) = \alpha, \alpha u$ ou αu^2.

Agora, como u e u^2 são raízes do polinômio $p(x) = x^2 + x + 1$, observe que $\gamma(u^2) + \gamma(u) + \gamma(1) = \gamma(0) \Rightarrow [\gamma(u)]^2 + \gamma(u) + 1 = 0$, portanto $\gamma(u)$ também é raiz de $p(x)$, e dessa forma $\gamma(u) = u$ ou u^2. Assim obtemos todos os $\mathbb{Q}$-automorfismos, que podem ser gerados através de dois $\mathbb{Q}$-automorfismos σ e τ, como pode ser visto na Tabela 7:

Tabela 7 – $\mathbb{Q}$-automorfismos de $\mathbb{Q}[\alpha, u]$

Automorfismo	Efeito em α	Efeito em u
Id	α	u
σ	αu	u
σ^2	αu^2	u
τ	α	u^2
$\sigma\tau$	αu	u^2
$\sigma^2\tau$	αu^2	u^2

Fonte: Os autores (2021)

Podemos observar que $\sigma^3 = Id$, $\tau^2 = Id$, $\sigma\tau = \tau\sigma^2$ e $\sigma^2\tau = \tau\sigma$. Portanto $G = \Gamma(\mathbb{Q}[\alpha, u] : \mathbb{Q}) \simeq S_3$.

Como G é isomorfo ao S_3, podemos permutar as raízes de $x^3 - 2$ e assim obteremos os mesmos automorfismos, nos mostrando uma segunda maneira de encontrá-los.

Segunda maneira: Permutando as raízes de $f(x) = x^3 - 2$, como pode ser observado na Tabela 8.

Observe que os automorfismos são iguais, exceto pela maneira que foram encontrados. Como $\mathbb{Q}[\alpha, u]$ é um corpo de decomposição, é uma extensão finita e normal. Assim, encontramos todos os elementos do grupo de Galois, já que pelo Corolário 5.20, $o(\Gamma(\mathbb{Q}[\alpha, u] : \mathbb{Q})) = [\mathbb{Q}[\alpha, u] : \mathbb{Q}] = 6$.

Tabela 8 – $\mathbb{Q}$-automorfismos de $\mathbb{Q}[\alpha, u]$

Automorfismo	Efeito em α	Efeito em αu	Efeito em αu^2
Id	α	αu	αu^2
σ	αu	αu^2	α
σ^2	αu^2	α	αu
τ	α	αu^2	αu
$\sigma\tau$	αu	α	αu^2
$\sigma^2\tau$	αu^2	αu	α

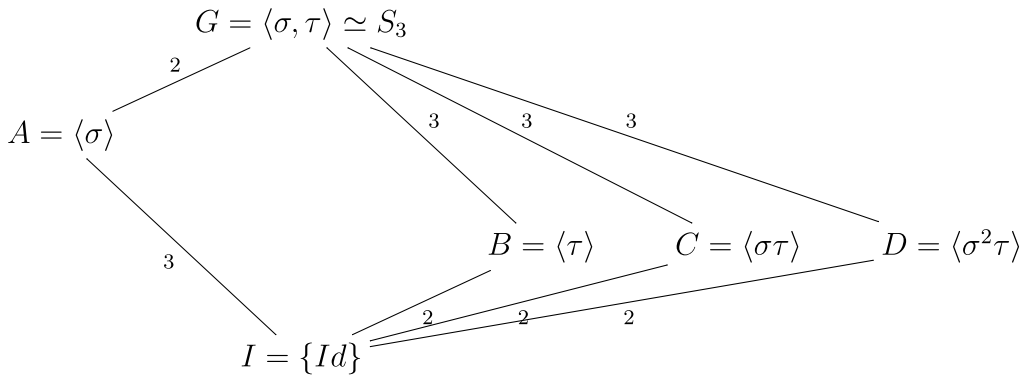
Fonte: Os autores (2021)

Pela construção acima, é fácil identificar os automorfismos como elementos do grupo S_3. Vejamos, σ atua da seguinte forma: $\alpha \mapsto \alpha u$, $\alpha u \mapsto \alpha u^2$ e $\alpha u^2 \mapsto \alpha$. Se denotarmos os elementos $\alpha, \alpha u$ e αu^2 por $1, 2$ e 3, respectivamente, teremos que σ atua como $1 \to 2$, $2 \to 3$ e $3 \to 1$. Assim σ pode ser identificado como a permutação (123). Da mesma forma obtemos $\sigma^2 = (132), \tau = (23), \sigma\tau = (12)$ e $\sigma^2\tau = (13)$.

Agora, vamos determinar os subgrupos de $G = \Gamma(\mathbb{Q}[\alpha, u] : \mathbb{Q})$:

- Ordem 6: $G \simeq S_3$;
- Ordem 3: $A = \{Id, \sigma, \sigma^2\} = \langle\sigma\rangle$;
- Ordem 2:
  - $B = \{Id, \tau\} = \langle\tau\rangle$;
  - $C = \{Id, \sigma\tau\} = \langle\sigma\tau\rangle$;
  - $D = \{Id, \sigma^2\tau\} = \langle\sigma^2\tau\rangle$;
- Ordem 1: $I = \{Id\}$.

Podemos construir o reticulado dos subgrupos de $G = \Gamma(\mathbb{Q}[\alpha, u] : \mathbb{Q})$:



Agora, vamos determinar o corpo fixo dos subgrupos de G. Para realizar tais contas, precisamos relembrar que $u^3 = 1$, $\alpha^3 = 2$ e $u^2 = -u - 1$. Dado $x \in \mathbb{Q}[\alpha, u]$, com $x = a_0 + a_1\alpha + a_2\alpha^2 + a_3u + a_4\alpha u + a_5\alpha^2 u$, temos:

- $Id(x) = x$, portanto Id fixa $\mathbb{Q}[\alpha, u]$;

- σ: $\alpha \to \alpha u$ $\quad u \to u$

$$\begin{aligned} \sigma(x) &= a_0 + a_1(\alpha u) + a_2(\alpha u)^2 + a_3u + a_4(\alpha u)u + a_5(\alpha u)^2 u \\ &= a_0 + a_1\alpha u + a_2\alpha^2(-u-1) + a_3u + a_4\alpha(-u-1) + a_5\alpha^2 \\ &= a_0 + a_1\alpha u - a_2\alpha^2 u - a_2\alpha^2 + a_3u - a_4\alpha u - a_4\alpha + a_5\alpha^2 \\ &= a_0 - a_4\alpha + (a_5 - a_2)\alpha^2 + a_3u + (a_1 - a_4)\alpha u - a_2\alpha^2 u \end{aligned}$$

  Assim $a_0 = a_0$, $a_1 = -a_4$, $a_2 = a_5 - a_2$, $a_3 = a_3$, $a_4 = a_1 - a_4$ e $a_5 = -a_2$. Logo $a_1 = a_2 = a_4 = a_5 = 0$. Dessa forma σ fixa $x = a_0 + a_3u$. Portanto σ fixa $\mathbb{Q}[u]$.

- σ^2: $\alpha \to \alpha u^2$ $\quad u \to u$

$$\begin{aligned} \sigma^2(x) &= a_0 + a_1(\alpha u^2) + a_2(\alpha u^2)^2 + a_3u + a_4(\alpha u^2)u + a_5(\alpha u^2)^2 u \\ &= a_0 + a_1\alpha(-u-1) + a_2\alpha^2 u + a_3u + a_4\alpha + a_5\alpha^2(-u-1) \\ &= a_0 - a_1\alpha u - a_1\alpha + a_2\alpha^2 u + a_3u + a_4\alpha - a_5\alpha^2 u - a_5\alpha^2 \\ &= a_0 + (-a_1 + a_4)\alpha - a_5\alpha^2 + a_3u - a_1\alpha u + (a_2 - a_5)\alpha^2 u \end{aligned}$$

  Portanto $a_0 = a_0$, $a_1 = -a_1 + a_4$, $a_2 = -a_5$, $a_3 = a_3$, $a_4 = -a_1$ e $a_5 = a_2 - a_5$. Logo $a_1 = a_2 = a_4 = a_5 = 0$. Assim σ fixa $x = a_0 + a_3u$. Dessa forma concluímos que σ fixa $\mathbb{Q}[u]$.

- τ: $\alpha \to \alpha$ $\quad u \to u^2$

$$\begin{aligned} \tau(x) &= a_0 + a_1\alpha + a_2\alpha^2 + a_3u^2 + a_4(\alpha)u^2 + a_5(\alpha)^2 u^2 \\ &= a_0 + a_1\alpha + a_2\alpha^2 + a_3(-u-1) + a_4\alpha(-u-1) + a_5\alpha^2(-u-1) \\ &= a_0 + a_1\alpha + a_2\alpha^2 - a_3u - a_3 - a_4\alpha u - a_4\alpha - a_5\alpha^2 u - a_5\alpha^2 \\ &= (a_0 - a_3) + (a_1 - a_4)\alpha + (a_2 - a_5)\alpha^2 - a_3u - a_4\alpha u - a_5\alpha^2 u \end{aligned}$$

  Assim, para que x seja fixado por τ precisamos ter $a_0 = a_0 - a_3$, $a_1 = a_1 - a_4$, $a_2 = a_2 - a_5$, $a_3 = -a_3$, $a_4 = -a_4$ e $a_5 = -a_5$, donde obtemos $a_3 = a_4 = a_5 = 0$, e

assim a_0, a_1 e a_2 são livres. Logo τ fixa $x = a_0 + a_1\alpha + a_2\alpha^2$ e assim τ fixa o corpo $\mathbb{Q}[\alpha]$.

- $\sigma\tau$: $\alpha \to \alpha u$ $\quad u \to u^2$

$$\begin{aligned}\sigma\tau(x) &= a_0 + a_1(\alpha u) + a_2(\alpha u)^2 + a_3u^2 + a_4(\alpha u)u^2 + a_5(\alpha u)^2u^2\\ &= a_0 + a_1\alpha u + a_2\alpha^2(-u-1) + a_3(-u-1) + a_4\alpha + a_5\alpha^2 u\\ &= a_0 + a_1\alpha u - a_2\alpha^2 u - a_2\alpha^2 - a_3u - a_3 + a_4\alpha + a_5\alpha^2 u\\ &= (a_0 - a_3) + a_4\alpha - a_2\alpha^2 - a_3u + a_1\alpha u + (a_5 - a_2)\alpha^2 u\end{aligned}$$

Portanto $a_0 = a_0 - a_3$, $a_1 = a_4$, $a_2 = -a_2$, $a_3 = -a_3$, $a_4 = a_1$ e $a_5 = a_5 - a_2$. Observe que $a_2 = a_3 = 0$, dessa forma a_0 e a_5 são arbitrários e $a_1 = a_4$. Assim $x = a_0 + a_1\alpha + a_1\alpha u + a_5\alpha^2 u = a_0 + a_1(\alpha + \alpha u) + a_5\alpha^2 u$, o que nos dá $x = a_0 - a_1(\alpha^2 u)^2 + a_5(\alpha^2 u)$. Portanto $\sigma\tau$ fixa $\mathbb{Q}[\alpha^2 u] = \mathbb{Q}[\alpha u^2]$.

- $\sigma^2\tau$: $\alpha \to \alpha u^2$ $\quad u \to u^2$

$$\begin{aligned}\sigma^2\tau(x) &= a_0 + a_1(\alpha u^2) + a_2(\alpha u^2)^2 + a_3u^2 + a_4(\alpha u^2)u^2 + a_5(\alpha u^2)^2u^2\\ &= a_0 + a_1\alpha(-u-1) + a_2\alpha^2 u + a_3(-u-1) + a_4\alpha u + a_5\alpha^2\\ &= a_0 - a_1\alpha u - a_1\alpha + a_2\alpha^2 u - a_3u - a_3 + a_4\alpha u + a_5\alpha^2\\ &= (a_0 - a_3) - a_1\alpha + a_5\alpha^2 - a_3u + (-a_1 + a_4)\alpha u + a_2\alpha^2 u\end{aligned}$$

Logo $a_0 = a_0 - a_3$, $a_1 = -a_1$, $a_2 = a_5$, $a_3 = -a_3$, $a_4 = -a_1 + a_4$ e $a_5 = a_2$. Observe que $a_3 = a_1 = 0$, assim a_0 e a_4 são livres e $a_2 = a_5$. Logo $x = a_0 + a_2\alpha^2 + a_4\alpha u + a_2\alpha^2 u = a_0 + a_2(\alpha^2 + \alpha^2 u) + a_4\alpha u = a_0 + a_2\alpha^2(1+u) + a_4\alpha u = a_0 - \alpha^2 u^2 + a_4\alpha u = a_0 - a_2(\alpha u)^2 + a_4\alpha u$. Portanto $\sigma^2\tau$ fixa $\mathbb{Q}[\alpha u]$.

Assim:

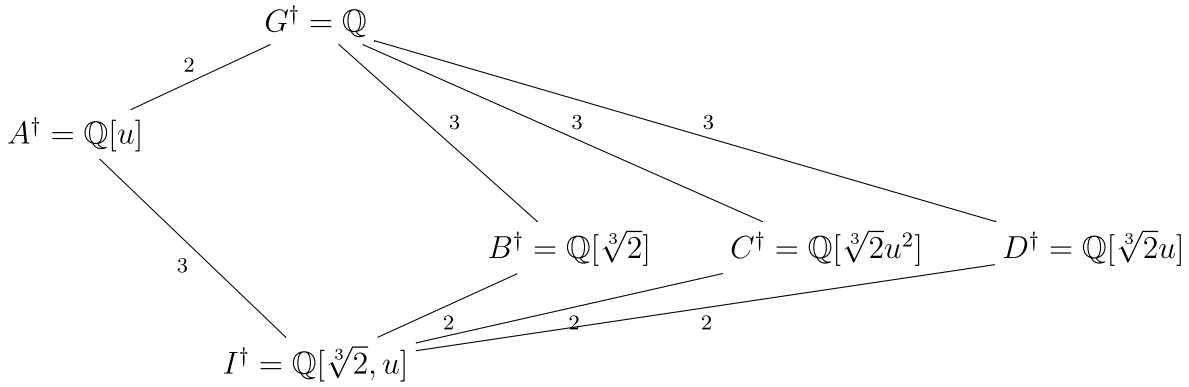
- Id fixa $\mathbb{Q}[\alpha, u] = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3u + a_4\alpha u + a_5\alpha^2 u \mid a_0, a_1, a_2, a_3, a_4, a_5 \in \mathbb{Q}\}$;
- σ fixa $\mathbb{Q}[u] = \{a_0 + a_1u \mid a_0, a_1 \in \mathbb{Q}\}$;
- σ^2 fixa $\mathbb{Q}[u] = \{a_0 + a_1u \mid a_0, a_1 \in \mathbb{Q}\}$;
- τ fixa $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_0, a_1, a_2 \in \mathbb{Q}\}$;
- $\sigma\tau$ fixa $\mathbb{Q}[\alpha u^2] = \{a_0 + a_1\alpha^2 u + a_2\alpha u^2 \mid a_0, a_1, a_2 \in \mathbb{Q}\}$;
- $\sigma^2\tau$ fixa $\mathbb{Q}[\alpha u] = \{a_0 + a_1\alpha u + a_2\alpha^2 u^2 \mid a_0, a_1, a_2 \in \mathbb{Q}\}$;

Portanto:

* $G = \langle\sigma, \tau\rangle \simeq S_3$ $\qquad$ $G^\dagger = \mathbb{Q}$;
* $A = \{Id, \sigma, \sigma^2\}$ $\qquad$ $A^\dagger = \mathbb{Q}[\alpha, u] \cap \mathbb{Q}[u] \cap \mathbb{Q}[u] = \mathbb{Q}[u]$;

* $B = \{Id, \tau\}$ $\qquad B^\dagger = \mathbb{Q}[\alpha, u] \cap \mathbb{Q}[\alpha] = \mathbb{Q}[\alpha];$
* $C = \{Id, \sigma\tau\}$ $\qquad C^\dagger = \mathbb{Q}[\alpha, u] \cap \mathbb{Q}[\alpha u^2] = \mathbb{Q}[\alpha u^2];$
* $D = \{Id, \sigma^2\tau\}$ $\qquad D^\dagger = \mathbb{Q}[\alpha, u] \cap \mathbb{Q}[\alpha u] = \mathbb{Q}[\alpha u];$
* $I = \{Id\}$ $\qquad I^\dagger = \mathbb{Q}[\alpha, u].$

Construindo o reticulado dos subcorpos de $\mathbb{Q}[\alpha, u]$:



Ao calcular os subgrupos normais de G, encontramos que os únicos subgrupos normais são G, A e I. Assim pelo teorema fundamental de Galois, as únicas extensões normais são $G^\dagger, A^\dagger$ e $I^\dagger$, que são os corpos de decomposição dos polinômios $x, x^2 + x + 1$ e $x^3 - 2$, respectivamente.

Observe que $B^\dagger$ confirma o teorema: como $\alpha \in B^\dagger$, α é raiz do polinômio $f(x) = x^3 - 2$ e $f(x)$ é irredutível sobre $\mathbb{Q}$, concluímos que $f(x)$ é o polinômio minimal de α, mas se $B^\dagger : \mathbb{Q}$ fosse uma extensão normal, $B^\dagger$ seria o corpo de decomposição de $f(x)$, o que é falso.

5.4.6 Exemplo 6

Finalizaremos os exemplos com mais um polinômio interessante para ser estudado, que é o polinômio $f(x) = x^5 - 2 \in \mathbb{Q}[x]$.

Seja $L = Gal(x^5 - 2, \mathbb{Q})$ o corpo de decomposição do polinômio $f(x) = x^5 - 2$. Pela Proposição 5.27, as cinco raízes de $f(x)$ são $\sqrt[5]{2}$, $\sqrt[5]{2}u$, $\sqrt[5]{2}u^2$, $\sqrt[5]{2}u^3$ e $\sqrt[5]{2}u^4$, em que $u = \cos\dfrac{2\pi}{5} + i\,\text{sen}\,\dfrac{2\pi}{5}$ é a raiz quinta da unidade. Temos assim $L = \mathbb{Q}[\sqrt[5]{2}, u]$.

A partir de agora, vamos denotar $\sqrt[5]{2} = \beta$ a fim de facilitar a escrita.

Sabemos que u é raiz do polinômio irredutível $x^4 + x^3 + x^2 + x + 1$, assim $[\mathbb{Q}[\beta, u] : \mathbb{Q}[\beta]] = 4$. Além disso, como $x^5 - 2$ é o polinômio minimal de β, temos $[\mathbb{Q}[\beta] : \mathbb{Q}] = 5$. Logo $[\mathbb{Q}[\beta, u] : \mathbb{Q}] = [\mathbb{Q}[\beta, u] : \mathbb{Q}[\beta]] \cdot [\mathbb{Q}[\beta] : \mathbb{Q}] = 4 \cdot 5 = 20$. Uma base para $\mathbb{Q}[\beta, u]$ visto como $\mathbb{Q}$-espaço vetorial é $B = \{1, \beta, \beta^2, \beta^3, \beta^4, u, \beta u, \beta^2 u, \beta^3 u, \beta^4 u, u^2, \beta u^2, \beta^2 u^2, \beta^3 u^2, \beta^4 u^2, u^3, \beta u^3,$

$\beta^2u^3, \beta^3u^3, \beta^4u^3\}$.

Vamos calcular os $\mathbb{Q}$-automorfismos de L. Como $\mathbb{Q}[\beta] \simeq \mathbb{Q}[\beta u]$, (já que são raízes do mesmo polinômio), vamos definir um $\mathbb{Q}$-automorfismo σ de L por $\sigma(\beta) = \beta u$ e $\sigma(u) = u$. Da mesma forma, como u e u^2 são raízes do mesmo polinômio, vamos definir um $\mathbb{Q}$-automorfismo τ de L por $\tau(\beta) = \beta$ e $\tau(u) = u^2$. Assim, $\sigma^5 = Id$ e $\tau^4 = Id$, onde Id é o homomorfismo identidade. Compondo tais automorfismos, obtemos todos os elementos do grupo de Galois, como pode ser observado na Tabela 9.

Assim, o grupo de Galois do polinômio $f(x)$ é $G = \langle \sigma, \tau \rangle = \{\sigma^i\tau^j \mid 0 \leq i \leq 4, 0 \leq j \leq 3\}$ é um grupo de ordem 20, isomorfo ao grupo de Frobenius $\mathbb{F}_{20}$. Observe que $\tau\sigma = \sigma^2\tau$.

De forma geral, um grupo finito G é dito **grupo de Frobenius** se G contém um subgrupo H próprio diferente de $\{e\}$ tal que $H \cap gHg^{-1} = \{e\}\ \forall\ g \in G - H$. Alguns exemplos são S_3 e D_n para n ímpar. No nosso exemplo, o grupo de Galois será o grupo de Frobenius $\mathbb{F}_{20}$, que é subgrupo de S_5, tem ordem 20 e é gerado pelas permutações (12345) e (2354).

Vamos calcular a ordem dos elementos:

- Elementos de ordem 2: $\tau^2, \sigma\tau^2, \sigma^2\tau^2, \sigma^3\tau^2$ e $\sigma^4\tau^2$.
- Elementos de ordem 4: $\tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau, \sigma^4\tau, \tau^3, \sigma\tau^3, \sigma^2\tau^3, \sigma^3\tau^3$ e $\sigma^4\tau^3$.
- Elementos de ordem 5: $\alpha, \alpha^2, \alpha^3$ e α^4.

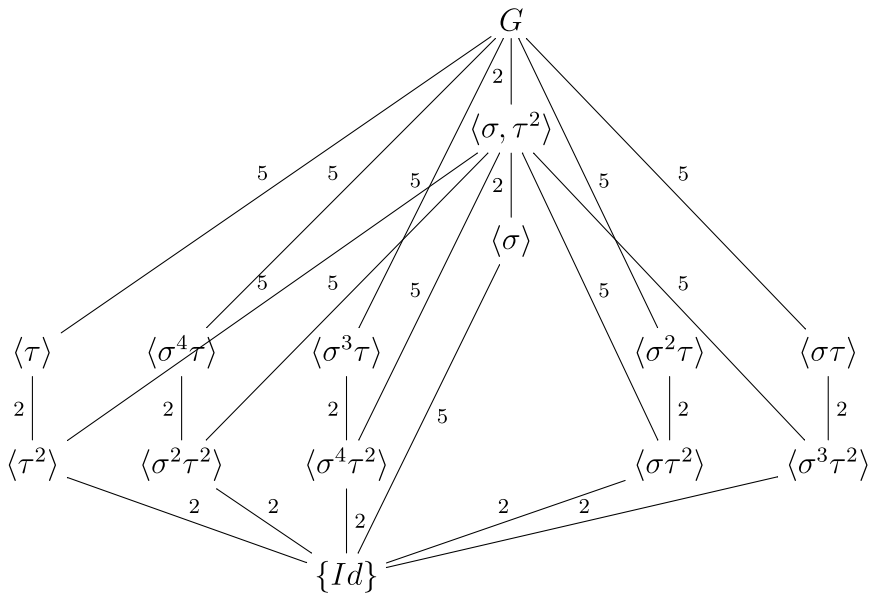
Agora,vamos calcular os subgrupos de $G \simeq \mathbb{F}_{20}$ utilizando geradores:

- $I = \langle Id \rangle = \{Id\}$;
- $A = \langle \tau^2 \rangle = \{Id, \tau^2\} \simeq \mathbb{Z}_2$;
- $B = \langle \sigma\tau^2 \rangle = \{Id, \sigma\tau^2\} \simeq \mathbb{Z}_2$;
- $S = \langle \tau \rangle = \{Id, \tau, \tau^2, \tau^3\} \simeq \mathbb{Z}_4$;
- $T = \langle \sigma\tau \rangle = \{Id, \sigma\tau, \sigma^3\tau^2, \sigma^2\tau^3\} \simeq \mathbb{Z}_4$;
- $U = \langle \sigma^2\tau \rangle = \{Id, \sigma^2\tau, \sigma\tau^2, \sigma^4\tau^3\} \simeq \mathbb{Z}_4$;
- $C = \langle \sigma^2\tau^2 \rangle = \{Id, \sigma^2\tau^2\} \simeq \mathbb{Z}_2$;
- $D = \langle \sigma^3\tau^2 \rangle = \{Id, \sigma^3\tau^2\} \simeq \mathbb{Z}_2$;
- $E = \langle \sigma^4\tau^2 \rangle = \{Id, \sigma^4\tau^2\} \simeq \mathbb{Z}_2$;
- $V = \langle \sigma^3\tau \rangle = \{Id, \sigma^3\tau, \sigma^4\tau^2, \sigma\tau^3\} \simeq \mathbb{Z}_4$;
- $W = \langle \sigma^4\tau \rangle = \{Id, \sigma^4\tau, \sigma^2\tau^2, \sigma^3\tau^3\} \simeq \mathbb{Z}_4$
- $X = \langle \sigma \rangle = \{Id, \sigma, \sigma^2, \sigma^3, \sigma^4\} \simeq \mathbb{Z}_5$;
- $Z = \langle \sigma, \tau^2 \rangle = \{Id, \sigma, \sigma^2, \sigma^3, \sigma^4, \tau^2, \sigma\tau^2, \sigma^2\tau^2, \sigma^3\tau^2, \sigma^4\tau^2\} \simeq D_5$;
- $G = \langle \sigma, \tau \rangle \simeq \mathbb{F}_{20}$.

Tabela 9 – $\mathbb{Q}$-automorfismos de $\mathbb{Q}[\beta, u]$

Automorfismo	Efeito em β	Efeito em u
Id	β	u
σ	βu	u
σ^2	βu^2	u
σ^3	βu^3	u
σ^4	βu^4	u
τ	β	u^2
$\sigma\tau$	βu	u^2
$\sigma^2\tau$	βu^2	u^2
$\sigma^3\tau$	βu^3	u^2
$\sigma^4\tau$	βu^4	u^2
τ^2	β	u^4
$\sigma\tau^2$	βu	u^4
$\sigma^2\tau^2$	βu^2	u^4
$\sigma^3\tau^2$	βu^3	u^4
$\sigma^4\tau^2$	βu^4	u^4
τ^3	β	u^3
$\sigma\tau^3$	βu	u^3
$\sigma^2\tau^3$	βu^2	u^3
$\sigma^3\tau^3$	βu^3	u^3
$\sigma^4\tau^3$	βu^4	u^3

Fonte: Os autores (2021)



Agora, vamos determinar os corpos intermediários da extensão $L : \mathbb{Q}$, onde $L = Gal(x^5 - 2, \mathbb{Q})$. Os subgrupos normais de G são $\{Id\}$, $\langle\sigma\rangle \simeq \mathbb{Z}_5$, $\langle\sigma, \tau^2\rangle \simeq D_5$ e G. Assim, $I^\dagger = L$ e $G^\dagger = \mathbb{Q}$.

Como $\tau(\beta) = \beta$, segue que $\mathbb{Q}[\beta] \subseteq \langle\tau\rangle^\dagger$. Mas então $\langle\tau\rangle \subseteq \langle\tau\rangle^{\dagger *} \subseteq \mathbb{Q}[\beta]^*$. Perceba que $[\mathbb{Q}[\beta] : \mathbb{Q}] = 5$ e $[\mathbb{Q}[u] : \mathbb{Q}] = 4$. Como $\mathbb{Q}[\beta]$ é um corpo intermediário, pelo Teorema

Fundamental de Galois, temos $o(\mathbb{Q}[\beta]^*) = [L : \mathbb{Q}[\beta]] = 4$. Como $o(\langle\tau\rangle) = 4$, segue que $\langle\tau\rangle = \langle\tau\rangle^{\dagger *} = \mathbb{Q}[\beta]^*$, assim $S^\dagger = \langle\tau\rangle^\dagger = \mathbb{Q}[\beta]$. Da mesma forma concluímos que $X^\dagger = \mathbb{Q}[u]$.

Além disso, observe que:

- $\sigma(u) = u$;
- $\tau(\beta) = \beta$;
- $\sigma^4\tau(\beta u) = \beta u$;
- $\sigma^3\tau(\beta u^2) = \beta u^2$;
- $\sigma^2\tau(\beta u^3) = \beta u^3$;
- $\sigma\tau(\beta u^4) = \beta u^4$.

Como $\beta, \beta u, \beta u^2, \beta u^3$ e βu^4 são raízes do polinômio $x^5 - 2$, pelo Corolário 4.31, segue que os corpos $\mathbb{Q}[\beta]$, $\mathbb{Q}[\beta u]$, $\mathbb{Q}[\beta u^2]$, $\mathbb{Q}[\beta u^3]$ e $\mathbb{Q}[\beta u^4]$ são isomorfos, assim todos são fixos por subgrupos de ordem 4.

Como $\sigma^4\tau(\beta u) = \beta u$, $\sigma^3\tau(\beta u^2) = \beta u^2$, $\sigma^2\tau(\beta u^3) = \beta u^3$ e $\sigma\tau(\beta u^4) = \beta u^4$, concluímos que $W^\dagger = \mathbb{Q}[\beta u]$, $V^\dagger = \mathbb{Q}[\beta u^2]$, $U^\dagger = \mathbb{Q}[\beta u^3]$ e $T^\dagger = \mathbb{Q}[\beta u^4]$.

Agora, vamos determinar o corpo fixo do subgrupo $Z = \langle\sigma, \tau^2\rangle$. Como $\tau^2(u) = u^4$ e $\tau^2(u^4) = u$, temos $\tau^2(u + u^4) = u + u^4$, ou seja, τ^2 fixa $u + u^4$. Da mesma forma, como $\sigma(u) = u$, σ também fixa $u + u^4$. Além disso, $\tau^2(u^2 + u^3) = u^2 + u^3$ e $\sigma(u^2 + u^3) = u^2 + u^3$, logo $u^2 + u^3$ também é fixado pelos automorfismos de Z.

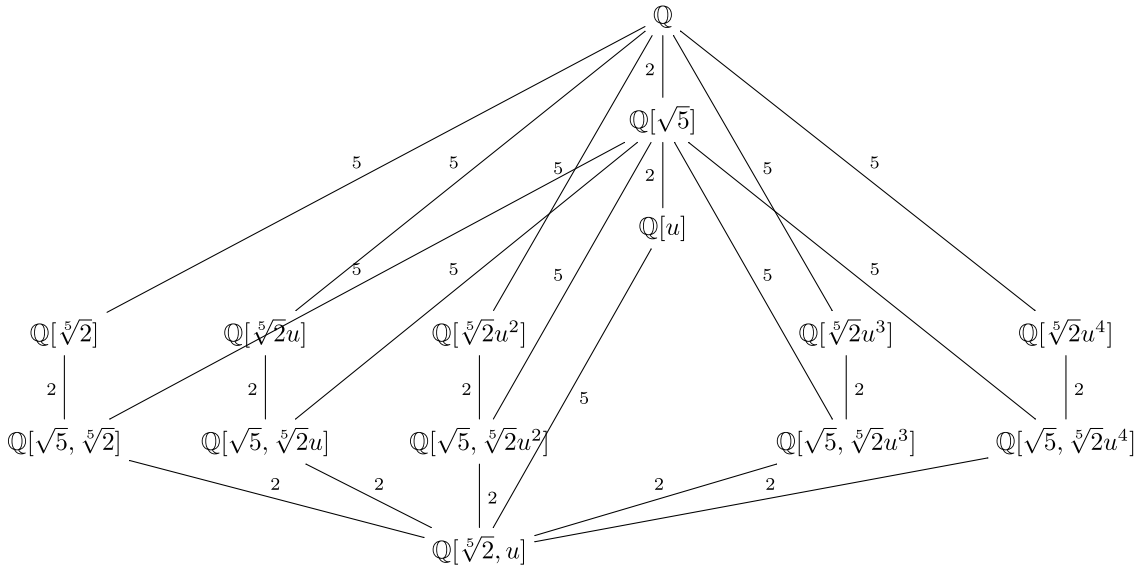
Seja $m_{u+u^4}(x)$ o polinômio minimal associado ao elemento $u + u^4$, que possui grau 2. Como $u^2 + u^3$ também é fixo por Z, $u^2 + u^3$ deve ser a outra raiz de $m_{u+u^4}(x)$. Assim:

$$m_{u+u^4}(x) = (x - (u + u^4))(x - (u^2 + u^3)) = x^2 - (u + u^2 + u^3 + u^4)x + (u + u^2 + u^3 + u^4)$$

Sabemos que u é raiz do polinômio $f(x) = x^4+x^3+x^2+x+1$, logo $u+u^2+u^3+u^4 = -1$, donde segue $m_{u+u^4}(x) = x^2 + x - 1$. Como as raízes de $m_{u+u^4}(x)$ são $\dfrac{-1 \pm \sqrt{5}}{2}$, obtemos que $\mathbb{Q}[u + u^4] = \mathbb{Q}[\sqrt{5}]$. Como $[\mathbb{Q}[\sqrt{5}] : \mathbb{Q}] = [Z^\dagger : \mathbb{Q}] = 2$, concluímos que $Z^\dagger = \mathbb{Q}[\sqrt{5}]$.

Agora resta encontrar os corpos fixos pelos subgrupos de ordem 2. Seja $A = \langle\tau^2\rangle$. Temos $A \subseteq Z$ e $A \subseteq S$, assim $Z^\dagger \subseteq A^\dagger$ e $S^\dagger \subseteq A^\dagger$, ou seja, $\mathbb{Q}[\sqrt{5}] \subseteq A^\dagger$ e $\mathbb{Q}[\beta] \subseteq A^\dagger$, logo $\mathbb{Q}[\sqrt{5}, \beta] \subseteq A^\dagger$. Como $[\mathbb{Q}[\sqrt{5}, \beta] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{5}, \beta] : \mathbb{Q}[\beta]] \cdot [\mathbb{Q}[\beta] : \mathbb{Q}] = 2 \cdot 5 = 10$ e $[A^\dagger : \mathbb{Q}] = 10$, segue que $A^\dagger = \mathbb{Q}[\sqrt{5}, \beta]$. Da mesma forma, encontramos os demais corpos fixos: $C^\dagger = \mathbb{Q}[\sqrt{5}, \beta u]$, $E^\dagger = \mathbb{Q}[\sqrt{5}, \beta u^2]$, $B^\dagger = \mathbb{Q}[\sqrt{5}, \beta u^3]$ e $D^\dagger = \mathbb{Q}[\sqrt{5}, \beta u^4]$.

Para finalizar este capítulo, apresentamos o diagrama dos corpos intermediários:


$\mathbb{Q}$
$\mathbb{Q}[\sqrt{5}]$
$\mathbb{Q}[u]$
$\mathbb{Q}[\sqrt[5]{2}]$
$\mathbb{Q}[\sqrt[5]{2}u]$
$\mathbb{Q}[\sqrt[5]{2}u^2]$
$\mathbb{Q}[\sqrt[5]{2}u^3]$
$\mathbb{Q}[\sqrt[5]{2}u^4]$
$\mathbb{Q}[\sqrt{5}, \sqrt[5]{2}]$
$\mathbb{Q}[\sqrt{5}, \sqrt[5]{2}u]$
$\mathbb{Q}[\sqrt{5}, \sqrt[5]{2}u^2]$
$\mathbb{Q}[\sqrt{5}, \sqrt[5]{2}u^3]$
$\mathbb{Q}[\sqrt{5}, \sqrt[5]{2}u^4]$
$\mathbb{Q}[\sqrt[5]{2}, u]$
2
5

6 Solubilidade e cálculo do grupo de Galois de polinômios

Para finalizar nosso trabalho, neste capítulo apresentaremos a relação entre a solubilidade das equações polinomiais, relacionadas à solubilidade dos grupos de Galois. Também apresentaremos critérios que permitem classificar o grupo de Galois de um polinômio de grau menor ou igual a 5, apenas conhecendo seus coeficientes e algumas ferramentas auxiliares. Devido ao objetivo deste capítulo, algumas demonstrações serão omitidas.

6.1 Solução por radicais

Nesta seção apresentaremos a relação entre os grupos solúveis e as equações polinomiais solúveis por radicais, justificando o porquê de não ser possível encontrar uma equação que forneça as raízes de um polinômio de grau 5 utilizando apenas radicais. Estamos quase chegando no fim desta aventura.

6.1.1 Grupos solúveis

Nesta subseção vamos apresentar algumas definições e resultados pertinentes a teoria de grupos, em especial, grupos simples e solúveis. Tais tópicos são necessários para a compreensão da insolubilidade de algumas equações quínticas.

Definição 6.1. *Um grupo G é dito* ***solúvel*** *se este tem uma sequência finita de subgrupos*

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_n = G$$

tais que:

i) G_i *é subgrupo normal de* G_{i+1}*, ou seja,* $G_i \lhd G_{i+1}, \quad \forall\, i = 0, \ldots, n-1$*;*

ii) $\dfrac{G_{i+1}}{G_i}$ *é abeliano* [1]*,* $\quad \forall\, i = 0, \ldots, n-1.$

Observe que não vale a transitividade: $G_i \lhd G_{i+1} \lhd G_{i+2}$ não implica que $G_i \lhd G_{i+2}$.

Exemplo 6.2. *Todo grupo abeliano G é solúvel, basta considerar a sequência $\{e\} \lhd G$.*

Com efeito, $\{e\}$ é subgrupo normal de G e $\dfrac{G}{\{e\}} \simeq G$ é abeliano.

[1] Observe que o grupo $\dfrac{G_{i+1}}{G_i}$ está bem definido, visto que $G_i \lhd G_{i+1}$.

Exemplo 6.3. *O grupo simétrico S_3 de ordem 6 é solúvel, pois possui um subgrupo cíclico A_3 de ordem 3, gerado pela permutação (123), cujo quociente $\frac{S_3}{A_3}$ é cíclico de ordem 2.*[2]

Basta ver no exemplo acima que a sequência $\{e\} \subseteq A_3 \subseteq S_3$ satisfaz as condições *i)* e *ii)*. Outros exemplos de grupos solúveis são:

- $D_4 = \langle \sigma, \tau \rangle$, com a sequência $\{e\} \subseteq A \subseteq S \subseteq D_4$, em que $A = \langle \sigma^2 \rangle \simeq \mathbb{Z}_2$ e $S = \langle \sigma \rangle \simeq \mathbb{Z}_4$;

  Neste caso temos $\{e\} \lhd A$, $A \lhd S$ e $S \lhd D_4$, além disso $\frac{A}{\{e\}} \simeq A$ é cíclico, $\frac{S}{A} \simeq \mathbb{Z}_2$ é cíclico e $\frac{D_4}{S} \simeq \mathbb{Z}_2$ é cíclico, portanto os quocientes são abelianos e consequentemente D_4 é solúvel.

- S_4, com a sequência $\{e\} \subseteq V \subseteq A_4 \subseteq S_4$, em que V é o grupo de Klein.

  Temos $\{e\} \lhd V$, $V \lhd A_4$ e $A_4 \lhd S_4$. Além disso, $\frac{V}{\{e\}} \simeq V$ é abeliano, $\frac{A_4}{V} \simeq \mathbb{Z}_3$ e $\frac{S_4}{A_4} \simeq \mathbb{Z}_2$ são cíclicos. Portanto os quocientes são abelianos, e assim S_4 é solúvel.

Teorema 6.4. *Seja G um grupo, H um subgrupo de G e N um subgrupo normal de G.*

i) Se G é solúvel, então H é solúvel.

ii) Se G é solúvel, então $\frac{G}{N}$ é solúvel.

iii) Se N e $\frac{G}{N}$ são solúveis, então G é solúvel.

Demonstração. A demonstração pode ser encontrada em [STEWART I, 2015], p. 145. □

Definição 6.5. *Um grupo G é **simples** se seus únicos subgrupos normais são $\{e\}$ e G.*

Exemplo 6.6. *Todo grupo cíclico $\mathbb{Z}_p$ com p primo é simples, já que não possui outros subgrupos normais além dos triviais. Estes grupos também são abelianos, portanto, solúveis. Em especial, eles são os únicos grupos simples solúveis.*

O próximo resultado generaliza este exemplo:

Teorema 6.7. *Um grupo solúvel é simples se e somente se é cíclico de ordem prima.*

Demonstração. Suponha que G é um grupo solúvel simples, assim existe uma sequência $\{e\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$, no qual assumimos $G_i \neq G_{i+1}$. Dessa forma, G_{n-1} é subgrupo normal de G. Mas como G é simples, G só possui subgrupos normais triviais, logo $G_{n-1} = \{e\}$ e assim $\frac{G_n}{G_{n-1}} = \frac{G}{\{e\}} = G$ é abeliano. Como G é abeliano, todo subgrupo de G é normal, mas G é simples, logo G não possui subgrupos normais próprios. Assim,

[2] Em especial, todo grupo cíclico é abeliano.

dado um elemento $g \in G$ teremos $\langle g \rangle = G$, então G deve ser cíclico com ordem prima. Por outro lado, se G é cíclico com ordem prima, G é abeliano e não possui subgrupos não triviais, logo G é solúvel e simples. □

Teorema 6.8. *Se $n \geq 5$, o grupo alternado A_n de grau n é simples.*

Demonstração. Ver [STEWART I, 2015], p. 147. □

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

Corolário 6.9. *O grupo simétrico S_n de grau n não é solúvel para $n \geq 5$.*

Demonstração. Suponha por absurdo que S_n é solúvel para $n \geq 5$. Assim, pelo Item i) do Teorema 6.4 temos que A_n é solúvel. Se $n \geq 5$, vimos no Teorema 6.8 que A_n é simples. Logo, se $n \geq 5$, A_n é um subgrupo simples e solúvel. Pelo Teorema 6.7, segue que A_5 é cíclico de ordem prima. Mas sabemos que se $n \geq 5$, a ordem de A_5 é $$\frac{n!}{2} = \frac{n \cdot (n-1) \cdot \ldots \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{2} = n \cdot (n-1) \cdot \ldots \cdot 5 \cdot 4 \cdot 3 \cdot 1 = 2 \cdot [n \cdot (n-1) \cdot \ldots \cdot 5 \cdot 2 \cdot 3 \cdot 1]$$ que é par. Absurdo. □

6.1.2 Extensões radicais

Nesta seção, apresentaremos um rigor maior na definição de solução por radicais. Iniciaremos explicando informalmente o que é uma extensão radical. Por exemplo, considere $x = \sqrt[3]{11} \cdot \sqrt[5]{\frac{7+\sqrt{3}}{2}} + \sqrt[4]{1+\sqrt[3]{4}}$. Para encontrarmos uma extensão de $\mathbb{Q}$ que contém x, precisaremos adjuntar os elementos $\alpha = \sqrt[3]{11}$, $\beta = \sqrt{3}$, $\gamma = \sqrt[5]{\frac{7+\beta}{2}}$, $\delta = \sqrt[3]{4}$ e $\epsilon = \sqrt[4]{1+\delta}$. De maneira formal, temos a seguinte definição:

Definição 6.10. *Uma extensão $L : K$ em $\mathbb{C}$ é radical se $L = K[\alpha_1, \ldots, \alpha_n]$ onde para cada $j = 1, \ldots, n$ existe um inteiro n_j tal que $\alpha_j^{n_j} \in K[\alpha_1, \ldots, \alpha_{j-1}]$, $j \geq 2$. Dizemos que os elementos α_j formam uma sequência radical para $L : K$. O grau radical do radical α_j é n_j.*

Exemplo 6.11. *A expressão anterior $x = \sqrt[3]{11} \cdot \sqrt[5]{\frac{7+\sqrt{3}}{2}} + \sqrt[4]{1+\sqrt[3]{4}}$ está contida em uma extensão radical da forma $\mathbb{Q}[\alpha, \beta, \gamma, \delta, \epsilon]$ em que $\alpha^3 = 11$, $\beta^2 = 3$, $\gamma^5 = \frac{7+\beta}{2}$, $\delta^3 = 4$ e $\epsilon^4 = 1 + \delta$.*

Perceba que qualquer expressão radical está contida em uma extensão radical.

Observação 6.12. *Toda extensão radical é finita.*

Observação 6.13. *Nem toda extensão radical é normal. Por exemplo, $\mathbb{Q}[\sqrt[3]{2}]$ é uma extensão radical, porém já vimos no Exemplo 5.16 que $\mathbb{Q}[\sqrt[3]{2}]$ não é normal.*

Observação 6.14. *Podemos tomar os graus $n_j's$ como primos, mesmo que seja necessário aumentar a sequência de subcorpos. Por exemplo, considere $\alpha = \sqrt[6]{5} = \sqrt[3]{\sqrt{5}}$. Sejam $\beta = \sqrt{5}$ e $\gamma = \sqrt[3]{\beta}$. Temos $\alpha^6 \in \mathbb{Q}$, $\beta^2 \in \mathbb{Q}$ e $\gamma^3 \in \mathbb{Q}[\beta]$. Assim $\alpha \in \mathbb{Q}[\alpha]$ ou $\alpha \in \mathbb{Q}[\beta, \gamma]$, que são extensões radicais.*

Um polinômio é considerado solúvel por radicais se todas as suas raízes são expressões radicais sobre o corpo base. Assim, temos a seguinte definição:

Definição 6.15. *Seja $f(x)$ um polinômio sobre um corpo K de $\mathbb{C}$ e seja $Gal(f, K)$ o corpo de decomposição de $f(x)$ sobre K. Dizemos que $f(x)$ é **solúvel por radicais** se existe um corpo M contendo $Gal(f, K)$ tal que $M : K$ seja uma extensão radical.*

Observe que $f(x)$ é solúvel por radicais somente se existe tal corpo M. Além disso, a extensão $Gal(f, K) : K$ não precisa ser radical. De fato, queremos que tudo no corpo de decomposição $Gal(f, K)$ seja expresso por radicais, mas não adianta esperar que tudo expresso pelos mesmos radicais esteja no corpo de decomposição.

De fato, considere o polinômio $f(x) = x^3 + x^2 - 2x - 1$. Pelo Teorema 3.45, vamos verificar se o polinômio $\overline{f}(x) = x^3 + x^2 + 1$ é irredutível sobre $\mathbb{Z}_2[x]$. De fato, como $\overline{f}$ não possui raízes em $\mathbb{Z}_2$, concluímos que $f(x)$ é irredutível sobre $\mathbb{Z}$ e consequentemente sobre $\mathbb{Q}$. Agora, vamos mostrar que $Gal(f, \mathbb{Q}) : \mathbb{Q}$ não é radical.

As raízes de $f(x)$ são $\alpha_1 = 2\cos\dfrac{2\pi}{7}$, $\alpha_2 = 2\cos\dfrac{4\pi}{7}$ e $\alpha_3 = 2\cos\dfrac{8\pi}{7}$. Observe que as raízes de $f(x)$ são reais, logo $Gal(f, \mathbb{Q}) \subseteq \mathbb{R}$. Além disso, $\alpha_2 = \alpha_1^2 - 2$ e $\alpha_3 = -\alpha_1^2 - \alpha_1 + 1$, assim as raízes α_2 e α_3 podem ser obtidas por meio de α_1, ou seja, $Gal(f, \mathbb{Q}) = \mathbb{Q}[\alpha_1]$.

Agora, suponha que $\mathbb{Q}[\alpha_1] : \mathbb{Q}$ é uma extensão radical. Então existe $n \in \mathbb{N}$ tal que $\alpha_1^n \in \mathbb{Q}$. Ou seja, α_1 é raiz do polinômio $x^n - \alpha_1^n \in \mathbb{Q}[x]$. Como $f(x)$ é mônico e irredutível, $f(x)$ é o polinômio minimal associado a α_1, logo $f(x)$ divide $x^n - \alpha_1^n$.

Sabemos pela Proposição 5.27 que as raízes n-ésimas de α_1^n são $\alpha_1 \cdot \zeta_n^k$, $k = 1, \ldots, n$, em que $\zeta_n = \cos\dfrac{2\pi}{n} + i\,\text{sen}\,\dfrac{2\pi}{n}$. Ou seja, as raízes do polinômio $x^n - \alpha_1^n$ são da forma $\alpha_1 \cdot \zeta_n^k$, $k = 1, \ldots, n$. Mas como $f(x)$ divide $x^n - \alpha_1^n$, as demais raízes de $f(x)$ são da forma $\alpha_1 \cdot \zeta_n^k \in \mathbb{C}$ (observe que só teríamos $\zeta_n^k \in \mathbb{R}$ se $\text{sen}\,\frac{2\pi}{n} = 0$, o que implica que $n = 1$ ou $n = 2$, mas como $\partial f = 3$, $n \geq 3$). Porém vimos que as raízes de $f(x)$ são números reais. Absurdo. Portanto $Gal(f, \mathbb{Q}) : \mathbb{Q}$ não é uma extensão radical.

Com o auxílio do *software Wolfram Alpha*, encontramos que as raízes de $f(x)$ expressas por radicais são da forma:

$$\alpha_1 = \frac{1}{3}\left(-1 + \frac{7^{\frac{2}{3}}}{\sqrt[3]{\dfrac{1+3i\sqrt{3}}{2}}} + \sqrt[3]{\frac{7(1+3i\sqrt{3})}{2}}\right)$$

$$\alpha_2 = -\frac{1}{3} - \frac{7^{\frac{2}{3}}(1-i\sqrt{3})}{3\sqrt[3]{4(1+3i\sqrt{3})}} - \frac{1}{6}(1+i\sqrt{3})\sqrt[3]{\frac{7(1+3i\sqrt{3})}{2}}$$

$$\alpha_3 = -\frac{1}{3} - \frac{7^{\frac{2}{3}}(1+i\sqrt{3})}{3\sqrt[3]{4(1+3i\sqrt{3})}} - \frac{1}{6}(1-i\sqrt{3})\sqrt[3]{\frac{7(1+3i\sqrt{3})}{2}}$$

Considere $M = \mathbb{Q}[\alpha, \beta, \gamma, \delta]$, em que $\alpha^2 = -3$, $\beta^3 = 2$, $\gamma^3 = 1 + 3\alpha$ e $\delta^3 = 7$. Observe que M é uma extensão radical que contém $Gal(f, \mathbb{Q})$. Assim $f(x)$ é solúvel por radicais, embora seu corpo de decomposição não seja uma extensão radical.

Além disso, queremos que todos as raízes de $f(x)$ sejam expressas por radicais. É possível que algumas raízes sejam expressas por radicais enquanto outras não (basta tomar o produto de dois polinômios, um solúvel e o outro não). Entretanto se um polinômio irredutível $f(x)$ tem uma raiz expressa por radicais, então todas as suas raízes devem ser expressas, basta lembrar que $K[\alpha] \simeq K[\beta]$, onde α e β são as raízes de $f(x)$.

Lema 6.16. *Se $L : K$ é uma extensão radical em $\mathbb{C}$ e M é o fecho normal de $L : K$, então $M : K$ é radical.*

Demonstração. Seja $L = K[\alpha_1, \ldots, \alpha_n]$ uma extensão radical com $\alpha_i^{n_i} \in K[\alpha_1, \ldots, \alpha_{i-1}]$. Seja $f_i(x)$ o polinômio minimal de α_i sobre K. Então $M \supseteq L$ é o corpo de decomposição de $f_1(x) \cdot \ldots \cdot f_n(x) = \prod_{i=1}^{n} f_i(x)$. Se β_{ij} é outra raiz de $f_i(x)$, temos $\beta_{ij} \in M$, e pelo Corolário 4.31, existe um isomorfismo $\sigma : K[\alpha_i] \to K[\beta_{ij}]$ que pode ser estendido a um K-automorfismo $\tau : M \to M$ pela Proposição 5.13. Como α_i é radical sobre K, β_{ij} também é, portanto concluímos que $M : K$ é radical. □

Lema 6.17. *Seja K um subcorpo de $\mathbb{C}$ em que $x^n - 1$ se divide. Sejam $a \in K$ e L o corpo de decomposição de $x^n - a \in K[x]$. Então o grupo de Galois de $L : K$ é abeliano.*

Demonstração. Seja α uma raiz qualquer de $x^n - a$. Como $x^n - 1$ se decompõe em K, a raiz geral de $x^n - a$ é αu, onde u é uma raiz de $x^n - 1$ em K. Como $u \in K$, temos $L = K[\alpha]$, assim qualquer $K-$automorfismo de L é determinado por seu efeito em α. Dados dois K-automorfismos $\sigma : \alpha \to \alpha u$ e $\tau : \alpha \to \alpha\xi$, onde u, ξ são raízes n-ésimas da unidade, temos $(\sigma \circ \tau)(\alpha) = \sigma(\tau(\alpha)) = \sigma(\alpha\xi) = \sigma(\alpha) \cdot \xi = (\alpha u)\xi = \tau(\alpha u) = \tau(\sigma(\alpha)) = (\tau \circ \sigma)(\alpha)$. Portanto o grupo de Galois de $L : K$ é abeliano. □

Este resultado é bem interessante, pois generaliza o Exemplo 5.4.4. Só devemos tomar cuidado com o corpo base, que deve conter uma raiz n-ésima primitiva da unidade. Além disso, este resultado é importante para os demais resultados que virão a seguir.

Lema 6.18. *Se K é um subcorpo de $\mathbb{C}$ e $L : K$ é normal e radical, então $\Gamma(L : K)$ é solúvel.*

Demonstração. Suponha que $L = K[\alpha_1, \ldots, \alpha_n]$ com $\alpha_i^{n_i} \in K[\alpha_1, \ldots, \alpha_{i-1}]$. Como vimos na Observação 6.14, como $L : K$ é radical, podemos refinar $K[\alpha_1, \ldots, \alpha_n]$ a fim de tomar

todos os índices $n_i's$ primos. Portanto vamos assumir que todos os índices n_i, $i = 1, \ldots, n$ são primos. Em particular, existe um primo p tal que $\alpha_1^p \in K$. Além disso, a demonstração será feita por indução sobre n.

Se $n = 0$, então $L = K$, assim $\Gamma(L : K) = \{Id\}$ é solúvel.

Se $\alpha_1 \in K$, então $L = K[\alpha_2, \ldots, \alpha_n]$ e $\Gamma(L : K)$ é solúvel por indução. Podemos assumir então que $\alpha_1 \notin K$. Seja $f(x)$ o polinômio minimal de α_1 sobre K. Como $\alpha_1^p \in K$, α_1 é raiz do polinômio $x^p - \alpha_1^p$. Assim $f(x)$ divide $x^p - \alpha_1^p$.

Como $\alpha_1 \notin K$, $f(x)$ tem no mínimo grau 2. Seja $\beta \in L$ uma outra raiz de $f(x)$ diferente de α_1. Consequentemente β também é raiz de $x^p - \alpha_1^p$, assim $\beta^p = \alpha_1^p$. Considere $\epsilon = \frac{\alpha_1}{\beta}$. Então $\epsilon^p = 1$ e $\epsilon \neq 1$ é raiz do polinômio $x^p - 1$. Assim, $M = K[\epsilon]$ é o corpo de decomposição do polinômio $x^p - 1$, logo $M : K$ é normal e $\Gamma(M : K)$ é abeliano.

Agora, considere a cadeia de subcorpos $K \subseteq M \subseteq M[\alpha_1] \subseteq L$. Observe que $L : K$ é finita e normal, logo $L : M$ também é, e assim o teorema fundamental de Galois se aplica à $L : K$ e à $L : M$.

Como $x^p - 1$ se decompõe linearmente em M e $\alpha_1^p \in M$, o Lema 6.17 nos dá que $\Gamma(M[\alpha_1] : M)$ é abeliano. Aplicamos o teorema fundamental de Galois para deduzir que $\Gamma(M[\alpha_1] : M) \simeq \dfrac{\Gamma(L : M)}{\Gamma(L : M[\alpha_1])}$.

Agora, $L = M[\alpha_1][\alpha_2, \ldots, \alpha_n]$, e assim $L : M[\alpha_1]$ é uma extensão normal e radical. Por indução, $\Gamma(L : M[\alpha_1])$ é solúvel. Portanto, pelo Teorema 6.4, $\Gamma(L : M)$ é solúvel. Já observamos que $M : K$ é normal e que $\Gamma(M : K)$ é abeliano. Assim, pelo Teorema Fundamental de Galois $\Gamma(M : K) \simeq \dfrac{\Gamma(L : K)}{\Gamma(L : M)}$. Por fim, como $\Gamma(L : M)$ é solúvel, segue pelo Teorema 6.4 que $\Gamma(L : K)$ é solúvel, como queríamos. □

Teorema 6.19. *Se K é subcorpo de $\mathbb{C}$ e $K \subseteq L \subseteq M$ onde $M : K$ é uma extensão radical, então o grupo de Galois de $L : K$ é solúvel.*

Demonstração. Seja K_0 o corpo fixo de $\Gamma(L : K)$ e $N : M$ o fecho normal de $M : K_0$. Assim $K \subseteq K_0 \subseteq L \subseteq M \subseteq N$. Como $M : K_0$ é radical, temos pelo Lema 6.16 que $N : K_0$ é uma extensão normal radical. Assim, pelo Lema 6.18 segue que $\Gamma(N : K_0)$ é solúvel. Pelo Teorema 5.23 encontramos que $L : K_0$ é uma extensão normal. Assim, pela correspondência de Galois, segue:

$$\Gamma(L : K_0) \simeq \frac{\Gamma(N : K_0)}{\Gamma(N : L)}$$

O Teorema 6.4 implica que $\Gamma(L : K_0)$ é solúvel. Mas $\Gamma(L : K) = \Gamma(L : K_0)$, assim concluímos que $\Gamma(L : K)$ é solúvel. □

Teorema 6.20. *Seja K um corpo de característica zero e seja $L : K$ uma extensão normal finita com grupo de Galois solúvel. Então existe uma extensão R de L tal que $R : K$ é radical.*

Demonstração. A demonstração pode ser encontrada em [STEWART I, 2015], p. 199.

□

O próximo resultado é o mais importante desta seção:

Teorema 6.21. *Se $f(x)$ é um polinômio sobre um corpo $K \subseteq \mathbb{C}$, $f(x)$ é solúvel por radicais se e somente se o grupo de Galois de $f(x)$ é solúvel.*

Demonstração. Seja $Gal(f, K)$ o corpo de decomposição de $f(x)$ sobre $K \subseteq \mathbb{C}$ e suponha que $f(x)$ é solúvel por radicais. Como $f(x)$ é solúvel por radicais, existe uma extensão $M : K$ radical, com $Gal(f, K) \subseteq M$. Assim, pelo Teorema 6.19 segue que o grupo de Galois de $Gal(f, K) : K$ é solúvel, ou seja, o grupo de Galois associado a $f(x)$ sobre K é solúvel.

Por outro lado, se o grupo $\Gamma(Gal(f, K) : K)$ é solúvel, pelo Teorema 6.20, como $Gal(f, K)$ é uma extensão normal e finita, existe uma extensão R de $Gal(f, K)$ tal que $R : K$ é radical. Portanto $f(x)$ é solúvel por radicais. □

Agora, temos condições de determinar quando um polinômio será solúvel por radicais. Para terminar essa seção, apresentaremos um último resultado:

Teorema 6.22. *Sejam p um primo e $f(x)$ um polinômio irredutível de grau p sobre $\mathbb{Q}$. Suponha que $f(x)$ tenha precisamente duas raízes imaginárias em $\mathbb{C}$. Então o grupo de Galois de $f(x)$ sobre $\mathbb{Q}$ é isomorfo ao grupo simétrico S_p.*

Demonstração. A demonstração pode ser encontrada em [STEWART I, 2015], p. 159.

□

Exemplo 6.23. *O polinômio $x^5 - 6x + 3$ sobre $\mathbb{Q}$ não é solúvel por radicais.*

De fato, o polinômio $f(x) = x^5 - 6x + 3$ possui três raízes reais e duas complexas, donde segue pelo Teorema 6.22 que o grupo de Galois de $f(x)$ é S_5, que não é solúvel.

Na próxima seção, apresentaremos alguns resultados que permitem determinar o grupo de Galois de qualquer polinômio com grau menor ou igual a 5, facilitando a compreensão da insolubilidade de algumas equações quínticas.

6.2 Classificando os Grupos de Galois

Finalizaremos este trabalho apresentando resultados que permitem classificar o grupo de Galois de um polinômio irredutível de grau $2, 3, 4$ ou 5. Estes resultados são muito lindos e fecham com chave de ouro nosso trabalho. As demonstrações serão ocultadas pois estamos mais interessados nas aplicações dos teoremas. Além disso, ao longo desta seção consideraremos $charK = 0$.

Definição 6.24. *Seja K um corpo e seja $f(x) \in K[x]$. Sejam $\alpha_1, \alpha_2, \ldots, \alpha_n$ as raízes de $f(x)$ em $Gal(f, K)$, e seja $\Delta = \prod_{i<j}(\alpha_i - \alpha_j) \in Gal(f, K)$. Então o discriminante de $f(x)$ é o elemento $D = \Delta^2 = \prod_{i<j}(\alpha_i - \alpha_j)^2$.*

Definição 6.25. *Se L é uma extensão algébrica de K e $\alpha \in L$, então o discriminante de α é definido como o discriminante do polinômio minimal $m_\alpha(x)$.*

A partir das definições acima, podemos enunciar o seguinte lema:

Lema 6.26. *Sejam $f(x) \in K[x]$ um polinômio irredutível e $Gal(f, K)$ o corpo de decomposição de $f(x)$ em $K[x]$. Então:*

i) $\sigma \in \Gamma(Gal(f, K) : K)$ é uma permutação par se e somente se $\sigma(\Delta) = \Delta = \sqrt{\Delta^2}$;

ii) $\sigma \in \Gamma(Gal(f, K) : K)$ é uma permutação ímpar se e somente se $\sigma(\Delta) = -\Delta$;

Além disso, $D = \Delta^2 \in K$. Assim, temos o seguinte resultado:

Corolário 6.27. *Seja $f(x) \in K[x]$ um polinômio irredutível com n raízes, cujo discriminante é Δ^2 . Então $\Gamma(Gal(f, K) : K)$ é um subgrupo de A_n se e somente se $\Delta \in K$.*

6.2.1 Polinômios de grau 2

Seja $f(x) = x^2 + bx + c$ um polinômio irredutível sobre um corpo K. Sabemos, pela fórmula resolutiva de equações do 2º grau, que as raízes desse polinômio podem ser expressas por $\alpha_1 = \dfrac{-b + \sqrt{b^2 - 4c}}{2}$ e $\alpha_2 = \dfrac{-b - \sqrt{b^2 - 4c}}{2}$. Assim, podemos calcular o discriminante:

$$\begin{aligned} D = \Delta^2 &= \prod_{i<j} (\alpha_i - \alpha_j)^2 \\ &= (\alpha_1 - \alpha_2)^2 \\ &= \left(\frac{-b + \sqrt{b^2 - 4c}}{2} - \left(\frac{-b - \sqrt{b^2 - 4c}}{2} \right) \right)^2 \\ &= \left(\frac{-b + \sqrt{b^2 - 4c} + b + \sqrt{b^2 - 4c}}{2} \right)^2 \\ &= \left(\sqrt{b^2 - 4c} \right)^2 \\ &= b^2 - 4c \end{aligned}$$

Observe que encontramos o famoso discriminante estudado durante o ensino fundamental (só não possui o coeficiente a pois $f(x)$ é mônico).

O corpo de decomposição de $f(x)$ em K será $K[\alpha_1, \alpha_2] = K\left[\dfrac{-b + \sqrt{\Delta^2}}{2}, \dfrac{-b + \sqrt{\Delta^2}}{2}\right]$. Porém, como $b \in K$, $\frac{-b}{2} \in K$, e assim $Gal(f, K) = K\left[\sqrt{\Delta^2}, -\sqrt{\Delta^2}\right] = K[\sqrt{\Delta^2}] = K[\Delta]$.

Exemplo 6.28. *Seja $f(x) = x^2 + 1 \in \mathbb{R}[x]$. Temos $\Delta^2 = b^2 - 4c = 0^2 - 4 \cdot 1 = -4$. Portanto $Gal(f, \mathbb{R}) = \mathbb{R}[\Delta] = \mathbb{R}[\sqrt{-4}] = \mathbb{R}[2i] = \mathbb{R}[i] \simeq \mathbb{C}$.*

Proposição 6.29. *Sejam $f(x) \in K[x]$ um polinômio de grau 2 e Δ^2 seu discriminante. Se G é o Grupo de Galois de $Gal(f, K) : K$, então $G \leq S_2$. Em especial,*

i) Se $\sqrt{\Delta^2} = \Delta \in K$*, então* $G = \{Id\}$*;*

ii) Se $\sqrt{\Delta^2} = \Delta \notin K$ *então* $G = S_2$*.*

Exemplo 6.30. *Seja* $f(x) = x^2 - 2x - 3 \in \mathbb{Q}[x]$*. Observe que* $\Delta = \sqrt{(-2)^2 - 4 \cdot (-3)} = \sqrt{16} = 4 \in \mathbb{Q}$*. Portanto* $G = \{Id\}$*. Perceba que neste caso as raízes de* $f(x)$ *são* $\alpha_1 = -1$ *e* $\alpha_2 = 3$*, que são números racionais, assim* $Gal(f, \mathbb{Q}) = \mathbb{Q}$ *e por isso* $G = \{Id\}$*, já que o único* $\mathbb{Q}-$*automorfismo de* $\mathbb{Q}$ *é a* Id*.*

Exemplo 6.31. *Considere* $f(x) = x^2 - 2 \in \mathbb{Q}[x]$*.*

Temos $Gal(f, \mathbb{Q}) = \mathbb{Q}[\sqrt{\Delta^2}] = \mathbb{Q}[\sqrt{0^2 - 4 \cdot (-2)}] = \mathbb{Q}[\sqrt{8}] = \mathbb{Q}[2\sqrt{2}] = \mathbb{Q}[\sqrt{2}]$*. Como* $\Delta = \sqrt{8} \notin \mathbb{Q}$*, o grupo de Galois associado à extensão* $\mathbb{Q}[\sqrt{2}] : \mathbb{Q}$ *é* S_2*. Perceba que já tínhamos encontrado este resultado no Exemplo 5.4.3, visto que* $S_2 \simeq \mathbb{Z}_2$*.*

Observe que no Exemplo 6.30 temos o caso trivial. Dado $f(x) \in K[x]$ e L o corpo de decomposição de $f(x)$ sobre K, o grupo de Galois é $\Gamma(L : K) = \{Id\}$ se e somente as raízes de $f(x)$ estão em K. Portanto, a partir de agora não vamos mais nos interessar em calcular quando $\Gamma(L : K)$ é $\{Id\}$, ou seja, vamos analisar apenas os casos em que $f(x)$ é irredutível sobre K.

Sabemos que o grupo de Galois de um polinômio $f(x) \in K[x]$ de grau n é um subgrupo de S_n. Ou seja, o grupo de Galois $\Gamma(f, K)$ irá permutar as raízes da equação $f(x) = 0$. Se nós reordenarmos as raízes de $f(x)$, o novo grupo de Galois $\Gamma'(f, K)$ irá mudar para um conjugado do grupo $\Gamma(f, K)$, ou seja, existe $\rho \in \Gamma(f, K)$ tal que $\Gamma'(f, K) = \rho\Gamma(f, K)\rho^{-1}$. Assim, estaremos interessados apenas em calcular as classes de conjugação de $\Gamma(f, K)$. Conforme o grau do polinômio $f(x)$ aumenta, o número de classes de conjugação também irá aumentar consideravelmente. Mas no caso em que $f(x)$ é irredutível sobre K, o grupo de Galois $\Gamma(f, K)$ irá agir transitivamente sobre as raízes de $f(x)$, o que reduz a lista de possíveis subgrupos rapidamente. A seguir apresentamos algumas definições e teoremas importantes para a compreensão deste parágrafo.

Definição 6.32. *Seja* G *um grupo e* X *um conjunto. Uma* ***ação*** *de* G *em* X *é definida como um homomorfismo* $\phi : G \to P(X)$*, no qual* $P(X)$ *é o conjunto das permutações dos elementos de* X*.*

Neste caso, dado $\alpha \in X$ e $g \in G$, representamos a ação de g em α por α^g.

Definição 6.33. *Seja* G *agindo no conjunto* X*. Sejam* $\alpha, \beta \in X$*. Vamos definir a relação* $\sim$ *da seguinte forma:* $\alpha \sim \beta$ *se e somente se existe* $g \in G$ *tal que* $\beta = \alpha^g$*. Essa relação é de equivalência, e assim as classes de conjugação são definidas como as* ***órbitas*** *de* G *sobre* X*.*

Definição 6.34. *Uma ação de um grupo* G *sobre um conjunto* X *é chamada* ***transitiva*** *se houver uma única órbita sobre a ação, isto é, para quaisquer* $\alpha, \beta \in X$*, existe* $\rho \in G$ *tal que* $\alpha^\rho = \beta$*.*

Teorema 6.35. *Seja $f(x)$ um polinômio sobre o corpo K. Então o grupo de Galois G age transitivamente no conjunto de todas as raízes de $f(x)$ se e somente se $f(x)$ é irredutível sobre K.*

Teorema 6.36. *Seja K um corpo e $f(x)$ um polinômio irredutível de grau n sobre K. Então o grupo de Galois G de $f(x)$ é um subgrupo transitivo de S_n cuja ordem é divisível por n.*

Observe que os dois teoremas acima são muito importantes e auxiliam na determinação dos possíveis grupos de Galois. Assim, para que G seja grupo de Galois de um polinômio irredutível $f(x)$ de grau n, G deve ser um grupo transitivo cuja ordem é múltipla de n.

6.2.2 Polinômios de grau 3

Já sabemos que um polinômio irredutível de grau 3 tem grupo de Galois isomorfo a um subgrupo de S_3. Além disso, pelo Teorema 6.36, a ordem do Grupo de Galois será divisível por 3, portanto as únicas possibilidades para o grupo de Galois de um polinômio irredutível de grau 3 são os subgrupos transitivos A_3 (gerado pela permutação (123)) e S_3 (gerado pelas permutações (123) e (12)). Vamos verificar em quais casos cada um ocorre, mas antes precisaremos de alguns resultados auxiliares, que nos ajudarão no cálculo do discriminante.

Lema 6.37. *Seja $f(x) \in K[x]$ um polinômio irredutível da forma $f(x) = x^3 + bx^2 + cx + d$. O polinômio $f(x)$ pode ser reescrito da forma $y^3 + py + q$, substituindo $x = y - \dfrac{b}{3}$, com $p = \dfrac{-b^2}{3} + c$ e $q = \dfrac{2b^3}{27} - \dfrac{bc}{3} + d$.*

Observação 6.38. *O discriminante do polinômio $f(x) = x^3 + bx^2 + cx + d$ é igual ao discriminante do polinômio $y^3 + py + q$.*

Proposição 6.39. *Seja $f(x) = x^3 + bx^2 + cx + d \in K[x]$ um polinômio irredutível e $y^3 + py + q$ sua forma reduzida. Então o discriminante de $f(x)$ pode ser facilmente calculado por $D = \Delta^2 = -4p^3 - 27q^2$.*

Veja que a substituição que fizemos nos fornece uma equação muito importante que facilita o cálculo do discriminante.

Exemplo 6.40. *Considere $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$. Vamos encontrar sua forma reduzida.*

Temos $b = 1, c = -2$ e $d = -1$. Portanto $p = \dfrac{-b^2}{3} + c = \dfrac{-1}{3} - 2 = \dfrac{-7}{3}$ e $q = \dfrac{2b^3}{27} - \dfrac{bc}{3} + d = \dfrac{2}{27} - \left(\dfrac{-2}{3}\right) - 1 = \dfrac{-7}{27}$. Assim $f(x)$ pode ser reescrito como $y^3 - \dfrac{7}{3}y - \dfrac{7}{27}$ e seu discriminante será $\Delta^2 = -4 \cdot \left(\dfrac{-7}{3}\right)^3 - 27 \cdot \left(\dfrac{-7}{27}\right)^2 = -4 \cdot \left(\dfrac{-343}{27}\right) - 27 \cdot \left(\dfrac{49}{729}\right) = \dfrac{1372}{27} - \dfrac{49}{27} = 49$.

Exemplo 6.41. *Já sabemos que $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ é irredutível, além disso, já está na forma reduzida. Assim, fica mais fácil calcular o seu discriminante, como podemos ver:* $\Delta^2 = \prod_{i<j}(\alpha_i - \alpha_j)^2 = -4 \cdot 0^3 - 27 \cdot (-2)^2 = -108$.

Teorema 6.42. *Seja $f(x) \in K[x]$ um polinômio irredutível de grau 3. Se $\alpha_1, \alpha_2, \alpha_3$ são as raízes de $f(x)$, o corpo de decomposição de $f(x)$ será $K[\alpha_1, \alpha_2, \alpha_3] = K[\alpha_1, \Delta]$.*

Exemplo 6.43. *Obtemos no Exemplo 6.41 que o discriminante do polinômio $f(x) = x^3 - 2$ é $\Delta^2 = -108$. Pelo Teorema 6.42, podemos encontrar seu corpo de decomposição. Assim, como uma das raízes de $f(x)$ é $\sqrt[3]{2}$, temos $Gal(f, \mathbb{Q}) = \mathbb{Q}[\alpha_1, \Delta] = \mathbb{Q}[\sqrt[3]{2}, \sqrt{-108}] = \mathbb{Q}[\sqrt[3]{2}, i\sqrt{3}]$. Observe que é o mesmo resultado que obtemos no Exemplo 5.4.5, pois a raiz cúbica da unidade $u = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ pode ser obtida por meio da adjunção do elemento $i\sqrt{3}$.*

Teorema 6.44. *Sejam $f(x) \in K[x]$ um polinômio irredutível de grau 3 e $L = Gal(f, K)$ seu corpo de decomposição. Assim:*

i) Se $\Delta \in K$ então $\Gamma(L : K) \simeq A_3$;

ii) Se $\Delta \notin K$ então $\Gamma(L : K) \simeq S_3$.

Quando $\Delta \in K$, o corpo de decomposição de um polinômio $f(x) \in K[x]$ com raízes $\alpha_1, \alpha_2, \alpha_3$ será $K[\alpha_1, \Delta] = K[\alpha_1]$. Portanto, o grupo de Galois de $f(x)$ irá permutar as raízes, ou seja, os automorfismos serão da forma

$$Id = \begin{cases} \alpha_1 \to \alpha_1 \\ \alpha_2 \to \alpha_2 \\ \alpha_3 \to \alpha_3 \end{cases} \qquad \sigma = \begin{cases} \alpha_1 \to \alpha_2 \\ \alpha_2 \to \alpha_3 \\ \alpha_3 \to \alpha_1 \end{cases} \qquad \sigma^2 = \begin{cases} \alpha_1 \to \alpha_3 \\ \alpha_2 \to \alpha_1 \\ \alpha_3 \to \alpha_2 \end{cases}$$

visto que os corpos $K[\alpha_1], K[\alpha_2]$ e $K[\alpha_3]$ são isomorfos (pois são raízes do mesmo polinômio irredutível). Observe que estas permutações são iguais as permutações $\{Id, (123), 132)\} = A_3$.

Exemplo 6.45. *Considere o polinômio $f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$, cujo discriminante é $\Delta^2 = -4 \cdot (-3)^3 - 27 \cdot 1^2 = 108 - 27 = 81$. Como $\Delta = \sqrt{81} = 9 \in \mathbb{Q}$, concluímos que o grupo de Galois de $f(x)$ é A_3. Em especial, as raízes de $f(x)$ são $\alpha_1 = 2\cos\left(\frac{2\pi}{9}\right)$, $\alpha_2 = 2\cos\left(\frac{8\pi}{9}\right)$ e $\alpha_3 = 2\cos\left(\frac{14\pi}{9}\right)$.*

Exemplo 6.46. *No Exemplo 6.40 vimos que $\Delta = \sqrt{\Delta^2} = \sqrt{49} = 7 \in \mathbb{Q}$, portanto o polinômio $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$ possui grupo de Galois isomorfo ao A_3.*

Lembra-se quando comentamos que o corpo de decomposição de $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$ não é uma extensão radical? Pois bem, havíamos calculado que o corpo de decomposição de $f(x)$ era $\mathbb{Q}[\alpha_1]$, onde $\alpha_1 = 2\cos\frac{2\pi}{7}$, assim $[\mathbb{Q}[\alpha_1] : \mathbb{Q}] = 3$. Pelo teorema

fundamental de Galois, o grupo de Galois tem ordem 3, e como é subgrupo de S_3, a única possibilidade é A_3, indo de acordo com o que obtemos no Exemplo 6.46.

Exemplo 6.47. *No Exemplo 6.41 calculamos $\Delta^2 = -108$, portanto $\Delta = \sqrt{-108} \notin \mathbb{Q}$. Dessa forma, o grupo de Galois do polinômio $x^3 - 2$ sobre $\mathbb{Q}$ será S_3, confirmando o que havíamos calculado no Exemplo 5.4.5. Observe que ao estudar o grupo de Galois de $x^3 - 2$ sobre $\mathbb{Q}[u]$, encontramos que $\sqrt{\Delta^2} = \sqrt{-108} = 6i\sqrt{3}$, que pertence a $\mathbb{Q}[i\sqrt{3}] \simeq \mathbb{Q}[u]$. Portanto, neste caso, o grupo de Galois de $x^3 - 2$ sobre $\mathbb{Q}[u]$ é A_3, confirmando o que vimos no Exemplo 6.41.*

6.2.3 Polinômios de grau 4

Sejam $f(x) = x^4 + ax^3 + bx^2 + cx + d$ um polinômio irredutível sobre K e $\alpha_1, \alpha_2, \alpha_3$ e α_4 suas raízes. Se considerarmos $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$, $\beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$ e $\beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$, o polinômio $r(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3)$ será chamado *cúbica resolvente de $f(x)$*. Por métodos computacionais obtemos $r(x) = x^3 - bx^2 + (ac - 4d)x + 4bd - a^2d - c^2 \in K[x]$. Assim como nos polinômios de grau 3, $f(x)$ e $r(x)$ estão intimamente ligados, a começar pelo fato de seus discriminantes serem iguais. Além disso, como a cúbica resolvente é um polinômio de grau 3, já sabemos calcular o discriminante pela Proposição 6.39. Além disso, os subgrupos transitivos de S_4 são:

- O subgrupo de Klein V, gerado pelas permutações (12)(34) e (13)(24) isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$;
- O subgrupo cíclico C_4 (consequentemente abeliano) de ordem 4, gerado por pela permutação (1234) e isomorfo a $\mathbb{Z}_4$;
- O subgrupo D_4, grupo de simetrias do quadrado, que foi apresentado no Exemplo 3.10 e é gerado pelas permutações (1234) e (24).
- O subgrupo alternado A_4, gerado pelas permutações (123) e (234).
- S_4, gerado por (1234) e (12).

Teorema 6.48. *Sejam $f(x) \in K[x]$ um polinômio irredutível de grau 4, $r(x)$ sua cúbica resolvente com corpo de decomposição E e Δ^2 o discriminante de $f(x)$. Então, se G denota o grupo de Galois de $f(x)$ sobre K, temos:*

i) $G \simeq V$ se e somente se $r(x)$ se divide em fatores lineares sobre K;

ii) $G \simeq C_4$ se e somente $r(x)$ tem uma única raiz $t \in K$ e $h(x) = (x^2 - tx + d)(x^2 + ax + (b - t))$ se divide sobre E;

iii) $G = D_4$ se e só se $r(x)$ tem uma única raiz $t \in K$ e $h(x)$ não se divide sobre E;

iv) $G = A_4$ se e somente se $r(x)$ é irredutível sobre K e $\Delta \in K$;

v) $G = S_4$ se e somente se $r(x)$ é irredutível sobre K e $\Delta \notin K$.

Tabela 10 – Critérios para calcular o grupo de Galois de um polinômio irredutível de grau 4

$\Delta = \sqrt{\Delta^2} \in K$?	Cúbica resolvente $r(x) \in K[x]$	$h(x)$ se divide em E?	Grupo de Galois
Sim	Redutível: todas as raízes $\in K$	———	V
Não	Redutível: uma única raiz $\in K$	Sim	C_4
Não	Redutível: uma única raiz $\in K$	Não	D_4
Sim	Irredutível	———	A_4
Não	Irredutível	———	S_4

Fonte: Os autores (2021)

Tabela 11 – Polinômios irredutíveis de grau 4 com diferentes grupos de Galois sobre $\mathbb{Q}$

$f(x) \in \mathbb{Q}[x]$	$r(x) \in \mathbb{Q}[x]$	Δ^2	$h(x)$: Se fatora em E?	Gr. de Galois
$x^4+4x^3+6x^2+4x+2$	$x(x-2)(x-4)$	16^2	———	V
$x^4+x^3+x^2+x+1$	$(x-2)(x^2+x-1)$	125	$(x^2-2x+1)(x^2+x-1)$: Sim	C_4
x^4-2	$x(x^2+8)$	-2048	$x^2(x^2-2)$: Não	D_4
x^4-7x^2-3x+1	$x^3+7x^2-4x-37$	183^2	———	A_4
x^4-x^3+1	x^3-4x-1	229	———	S_4
x^4+x+1	x^3-4x-1	229	———	S_4
$x^4+8x+12$	$x^3-48x-64$	576^2	———	A_4
$x^4-4x^3+4x^2+6$	$x(x^2-4x-24)$	64512	$(x^2+6)(x^2-4x+4)$: Não	D_4
$x^4-x^3+x^2-x+1$	$(x-2)(x^2+x-1)$	125	$(x^2-2x+1)(x^2-x-1)$: Sim	C_4
x^4+1	$x(x-2)(x+2)$	16^2	———	V

Fonte: Os autores (2021)

Na Tabela 10 apresentamos os critérios de forma resumida. Também apresentamos alguns exemplos, como pode ser observado na Tabela 11.

6.2.4 Polinômios de grau 5

Assim como para polinômios de grau 4, também precisamos de um polinômio resolvente, que auxiliará no cálculo do grupo de Galois. Dado um polinômio de grau 5 irredutível da forma $f(x) = x^5 - c_1x^4 + c_2x^3 - c_3x^2 + c_4x - c_5 \in \mathbb{Q}[x]$, a sexta resolvente $r_f(x) \in \mathbb{Q}[x]$ será dada pela expressão

$$r_f(x) = (x^3 + B_2x^2 + B_4x + B_6)^2 - 2^{10} \cdot \Delta^2 x$$

em que Δ^2 é o discriminante de $f(x)$, $B_2 = 8c_1c_3 - 3c_2^2 - 20c_4$, $B_4 = 3c_2^4 - 16c_1c_2^2c_3 + 16c_1^2c_3^2 + 16c_2c_3^2 + 16c_1^2c_2c_4 - 8c_2^2c_4 - 112c_1c_3c_4 + 240c_4^2 - 64c_1^3c_5 + 240c_1c_2c_5 - 400c_3c_5$ e $B_6 = 8c_1c_2^4c_3 - c_2^6 - 16c_1^2c_2^2c_3^2 - 16c_2^3c_3^2 + 64c_1c_2c_3^3 - 64c_3^4 - 16c_1^2c_2^3c_4 + 28c_2^4c_4 + 64c_1^3c_2c_3c_4 - 112c_1c_2^2c_3c_4 - 128c_1^2c_3^2c_4 + 224c_2c_3^2c_4 - 64c_1^4c_4^2 + 224c_1^2c_2c_4^2 - 176c_2^2c_4^2 - 64c_1c_3c_4^2 + 320c_4^3 + 48c_1c_2^3c_5 - 192c_1^2c_2c_3c_5 - 80c_2^2c_3c_5 + 640c_1c_3^2c_5 + 384c_1^3c_4c_5 - 640c_1c_2c_4c_5 - 1600c_3c_4c_5 - 1600c_1^2c_5^2 + 4000c_2c_5^2$.

Na Tabela 12 apresentamos alguns polinômios de grau 5 juntamente com as suas respectivas sextas resolventes.[3]

[3] O cálculo da sexta resolvente e do discriminante foram realizados com o auxílio de *softwares* matemáticos, como *Wolfram Alpha* e *Maxima*.

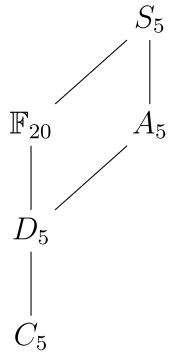
Tabela 12 – Exemplos de polinômios irredutíveis $f(x)$ de grau 5 e seus respectivos polinômios resolventes

$f(x) \in \mathbb{Q}[x]$	$r_f(x) \in \mathbb{Q}[x]$
$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$	$(x^3 - 132x^2 + 3872x)^2 - 2^{10} \cdot 11^4 x$
$x^5 - 5x + 12$	$(x^3 + 100x^2 + 6000x - 40000)^2 - 2^{16} \cdot 10^6 x$
$x^5 - 2$	$x^6 - 2^{10} \cdot 50000x$
$x^5 + 20x + 16$	$(x^3 - 400x^2 + 96000x + 2560000)^2 - 2^{11} \cdot 10^6 x$
$x^5 - 6x + 3$	$(x^3 + 120x^2 + 8640x - 69120)^2 + 2^{10} \cdot 1737531x$
$x^5 - x + 1$	$(x^3 + 20x^2 + 240x - 320)^2 - 2^{10} \cdot 2869x$
$x^5 - 2x^4 - 78x^3 + 159x^2 - 80x + 1$	$(x^3 - 19196x^2 + 115022048x - 212208108672)^2 - 2^{10} \cdot 7^4 \cdot 38177^2 x$
$x^5 + 15x + 12$	$(x^3 - 300x^2 + 54000x + 1080000)^2 - 2^{20} \cdot 3^4 \cdot 5^5 x$
$x^5 - 3125x - 37500$	$(x^3 + 62500x^2 + 2343750000x - 9765625000000)^2 - 2^{22} \cdot 5^{26} x$
$x^5 - 110x^3 - 55x^2 + 2310x + 979$	$(x^3 - 82500x^2 + 1512500000x)^2 - 2^{10} \cdot 5^{20} \cdot 11^4 x$

Fonte: Os autores (2021)

Como já vimos anteriormente, os possíveis grupos de Galois de polinômios irredutíveis de grau 5 serão os subgrupos transitivos de S_5, que estão elencados abaixo:

- O subgrupo cíclico C_5, gerado pela permutação (12345) e isomorfo a $\mathbb{Z}_5$, cuja ordem é 5;
- O subgrupo D_5, grupo de simetrias do pentágono, que é gerado pelas permutações (12345) e (25)(34).
- O grupo de Frobenius $\mathbb{F}_{20}$, apresentado no Exemplo 5.4.6, cuja ordem é 20 e é gerado pelas permutações (12345) e (2354).
- O subgrupo alternado A_5, gerado pelas permutações (12345) e (13452).
- S_5, gerado por (12345) e (12).



Teorema 6.49. *Seja $f(x)$ um polinômio separável e irredutível sobre $K[x]$. Então $G \subseteq S_5$ será o grupo de Galois associado ao polinômio $f(x)$ se possui as seguintes propriedades:*

i) $G \subseteq A_5$ se e somente se $\sqrt{\Delta^2} = \Delta \in K$.

ii) $A_5 \subseteq G$ se e somente se $r_f(x)$ é irredutível sobre K.

iii) *G é conjugado a um subgrupo de $\mathbb{F}_{20}$ se e somente se a sexta resolvente $r_f(x)$ possui uma raiz em K.*

iv) *G é conjugado ao subgrupo C_5 se e somente se $f(x)$ se divide completamente sobre $K[\alpha]$, em que α é uma raiz de $f(x)$.*

Observe que o Item i) vai de acordo com o Corolário 6.27. Além disso, no Item iv), dizer que $f(x)$ se divide completamente sobre $K[\alpha]$ é equivalente a dizer que $f(x)$ possui todas as suas raízes em $K[\alpha]$, ou seja, as demais raízes podem ser obtidas em termos de α.

O Teorema 6.49 contempla todas as opções de subgrupos transitivos de S_5, assim como pode ser observado na Tabela 13. Além disso, faremos um destaque para o enunciado deste teorema. Já vimos que os grupos transitivos possuem apenas uma classe de conjugação, então podemos enxergar G como um subgrupo de $\mathbb{F}_{20}$, podendo ser C_5, D_5 ou $\mathbb{F}_{20}$ no Item iii) (já que são os únicos subgrupos transitivos de $\mathbb{F}_{20}$) e $G = C_5$ no Item iv) (já que há um único subgrupo de C_5 que é transitivo, que é o próprio C_5).

Tabela 13 – Critérios para determinar o grupo de Galois de um polinômio irredutível de grau 5

$\Delta = \sqrt{\Delta^2} \in K$?	$r_f(x)$ tem raiz em K	$f(x)$ se divide complet. em $K[\alpha]$?	Grupo de Galois
Sim	Sim	Sim	C_5
Sim	Sim	Não	D_5
Não	Sim	———	$\mathbb{F}_{20}$
Sim	Não	———	A_5
Não	Não	———	S_5

Fonte: Os autores (2021)

A seguir, apresentamos alguns exemplos de polinômios irredutíveis de grau 5 e seus respectivos grupos de Galois.

Tabela 14 – Exemplos de polinômios irredutíveis $f(x)$ de grau 5 com diferentes grupos de Galois sobre $\mathbb{Q}$

$f(x) \in \mathbb{Q}[x]$	Δ^2	$r_f(x)$ tem raiz em $\mathbb{Q}$?	$f(x)$ se fatora em $\mathbb{Q}[\alpha]$?	Grupo de Galois
$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$	11^4	Sim	Sim	C_5
$x^5 - 5x + 12$	$2^6 \cdot 10^6$	Sim	Não	D_5
$x^5 - 2$	50000	Sim	———	$\mathbb{F}_{20}$
$x^5 + 20x + 16$	$2^{10} \cdot 10^6$	Não	———	A_5
$x^5 - 6x + 3$	-1737531	Não	———	S_5
$x^5 - x + 1$	2869	Não	———	S_5
$x^5 - 2x^4 - 78x^3 + 159x^2 - 80x + 1$	$7^4 \cdot 38177^2$	Não	———	A_5
$x^5 + 15x + 12$	259200000	Sim	———	$\mathbb{F}_{20}$
$x^5 - 3125x - 37500$	$2^{12} \cdot 5^{26}$	Sim	Não	D_5
$x^5 - 110x^3 - 55x^2 + 2310x + 979$	$5^{20} \cdot 11^4$	Sim	Sim	C_5

Fonte: Os autores (2021)

Observe que os polinômios acima foram tomados em $\mathbb{Q}[x]$. Se mudarmos o corpo base, o grupo de Galois também pode mudar.

Exemplo 6.50. *Seja $f(x) = x^5 - 2$. Já vimos no Exemplo 5.4.6 que o grupo de Galois sobre $\mathbb{Q}$ é $\mathbb{F}_{20}$. Mas, e se quisermos calcular o grupo de Galois de $f(x)$ sobre $\mathbb{Q}[\sqrt{5}]$?*

Pela Tabela 14, temos $\Delta^2 = 50000$ e $r_f(x) = x^6 - 2^{10} \cdot 50000x = x^6 - 2^{14} \cdot 5^5 x$. Observe que $\sqrt{\Delta^2} \in \mathbb{Q}[\sqrt{5}]$, $r_f(x)$ possui uma raiz em $\mathbb{Q}[\sqrt{5}]$ e $f(x)$ não se divide completamente em $K[\alpha]$, em que $\alpha = \sqrt[5]{2}$. Logo, utilizando o Teorema 6.49 concluímos que o grupo de Galois de $f(x)$ sobre $\mathbb{Q}[\sqrt{5}]$ é D_5.

De fato, observe o diagrama dos corpos intermediários do Exemplo 5.4.6. Temos $[\mathbb{Q}[\sqrt[5]{2}, u] : \mathbb{Q}[\sqrt{5}]] = 5 \cdot 2 = 10 = o(D_5)$.

Como vimos ao longo deste trabalho, os polinômios irredutíveis de grau 5 nem sempre são solúveis por radicais, visto que A_5 e consequentemente S_5 não são grupos solúveis. Assim, terminamos este trabalho apresentando a seguinte proposição:

Proposição 6.51. *Seja $f(x) \in K[x]$ um polinômio irredutível de grau 5, com $charK = 0$. Então $f(x)$ é solúvel por radicais se e somente se o grupo de Galois $Gal(f, K)$ é isomorfo a um subgrupo de $\mathbb{F}_{20}$.*

7 Considerações finais

A busca por soluções de equações polinomiais movimentou a matemática ao longo dos séculos, possibilitando o surgimento de inúmeros avanços nas mais diversas áreas da matemática. A teoria de Galois, apresentada neste trabalho, é um exemplo, e constitui uma das teorias mais lindas que já foi desenvolvida. Envolvendo com maestria tópicos das teorias de grupos e corpos, explica por que nem todos os polinômios com grau maior ou igual a 5 são solúveis por radicais.

Acreditamos que este trabalho tenha sido muito proveitoso para todos os envolvidos, pois permitiu inúmeros momentos de estudos e aprendizados, bem como possibilitou a elaboração de um material recheado de exemplos (que por vezes não são apresentados em livros básicos desta teoria). Esperamos que os leitores interessados possam ter aprofundado seus conhecimentos e se divertido com esta teoria tão bonita.

Referências

ANDRADE, J. F. S. *Tópicos especiais em álgebra*. Rio de Janeiro: Sociedade Brasileira de Matemática, 2013. 172 p. Citado na página 15.

AWTREY, C.; BEUERLE, J.; KEENAN, M. Algorithms for computing quartic galois groups over fields of characteristic 0. *International Journal of Pure and Applied Mathematics*, Academic Publications, Ltd., v. 112, n. 4, p. 709–740, 2017. Citado na página 15.

AWTREY, C.; CESARSKI, T.; JAKES, P. Determining galois groups of reducible polynomials via discriminants and linear resolvents. *JP Journal of Algebra Number Theory and Applications*, v. 39, n. 5, p. 685–702, 2017. Disponível em: <https://facstaff.elon.edu/cawtrey/acj-reducible.pdf>. Citado na página 15.

BARAI, R. On determination of galois group of quartic polynomials. *Indian Mathematical Society*, Maharashtra, v. 87, p. 73–85, 2019. Disponível em: <https://www.researchgate.net/publication/334389725_ON_DETERMINATION_OF_GALOIS_GROUP_OF_QUARTIC_POLYNOMIALS>. Citado na página 15.

BERGLUND, J. Analyzing the galois groups of fifth-degree and fourth-degree polynomials. *Undergraduate Review*, v. 7, n. 1, p. 22–28, 2011. Disponível em: <https://vc.bridgew.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1182&context=undergrad_rev>. Citado na página 15.

CASTRO, D. E. *Cálculo do grupo de Galois*. São Paulo: [s.n.], 2007. Orientador: Paulo Agozzini Martin. 2007. 77 p. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação). Disponível em: <https://bcc.ime.usp.br/tccs/2007/danilo/monografia.pdf>. Citado na página 15.

COELHO, F. U.; LOURENCO, M. L. *Um curso de álgebra linear*. 2. ed. São Paulo: Editora da Universidade de São Paulo, 2018. Citado 3 vezes nas páginas 15, 21 e 48.

CONRAD, K. Galois groups as permutation groups. *Expository papers*, 2010. Disponível em: <https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisaspermgp.pdf>. Citado na página 15.

CONRAD, K. Galois groups of cubics and quartics (not in characteristic 2). *Expository papers*, v. 10, 2010. Disponível em: <https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquartic.pdf>. Citado na página 15.

COX, D. A. *Galois theory*. New Jersey: John Wiley & Sons, 2004. Citado na página 15.

CRUZ, K. B. *Introdução à teoria de Galois*. São Carlos: [s.n.], 2014. 117 p. Orientador: Waldeck Schützer. 2014. 117 p. Trabalho de Conclusão de Curso (Licenciatura e Bacharelado em Matemática) - Universidade Federal de São Carlos. Disponível em: <https://www.dm.ufscar.br/dm/index.php/component/attachments/download/46>. Citado na página 15.

DOMINGUES, H. H.; IEZZI, G. *Álgebra moderna*. 4. ed. São Paulo: Atual, 2003. Citado 6 vezes nas páginas 15, 21, 22, 23, 27 e 30.

DUMMIT, D. S. Solving solvable quintics. *Mathematics of computation*, v. 57, n. 195, p. 387–401, 1991. Disponível em: <https://www.ams.org/journals/mcom/1991-57-195/S0025-5718-1991-1079014-X/S0025-5718-1991-1079014-X.pdf>. Citado na página 15.

FERNANDES, L. S. *Polinômios, corpos de decomposição e uma introdução à teoria de Galois*. Belo Horizonte: [s.n.], 2016. 65 p. Orientador: John MacQuarrie. Monografia (Especialização em Matemática) - Universidade Federal de Minas Gerais. Disponível em: <http://hdl.handle.net/1843/EABA-ACAHA3>. Citado na página 15.

FREIRE, R. A. Os fundamentos do pensamento matemático no século xx e a relevância fundacional da teoria de modelos. Campinas, p. 127, 2009. Disponível em: <http://www.repositorio.unicamp.br/handle/REPOSIP/281061>. Citado na página 14.

GARBI, G. G. *O romance das equações algébricas*. 4. ed. São Paulo: Editora Livraria da Física, 2010. Citado 2 vezes nas páginas 14 e 17.

GARCIA A.; IEQUAIN, Y. *Elementos de álgebra*. 6. ed. Rio de Janeiro: IMPA, 2013. Citado 2 vezes nas páginas 15 e 27.

GONÇALVES, A. *Introdução à álgebra*. 5. ed. Rio de Janeiro: IMPA, 2012. Citado 6 vezes nas páginas 15, 21, 31, 32, 33 e 48.

GUDKOV, K. Y.; LUR'E, B. B. Cyclic galois extensions for quintic equation. *Journal of Mathematical Sciences*, Springer, v. 222, n. 4, p. 417–425, 2017. Citado na página 15.

HOWIE, J. M. *Fields and Galois theory*. London: Springer-Verlag, 2006. Citado 2 vezes nas páginas 15 e 87.

KAPPE, L. C.; WARREN, B. An elementary test for the galois group of a quartic polynomial. *The American Mathematical Monthly*, Taylor & Francis, v. 96, n. 2, p. 133–137, 1989. Disponível em: <https://www.jstor.org/stable/2323198?seq=1#metadata_info_tab_contents>. Citado na página 15.

KAVANAGH, R. On irreducible rational quintics. *Mathematics Subject Classification*, 2010. Disponível em: <https://rak.ac/publication/2014-on-irreducible-rational-quintics/galois.pdf>. Citado na página 15.

LAVALLEE, M. J. *Dihedral quintic fields with a power basis*. Okanagan: [s.n.], 2008. 101 p. Thesis (Master of Science) - The University of British Columbia. Disponível em: <https://open.library.ubc.ca/cIRcle/collections/ubctheses/24/items/1.0066793>. Citado na página 15.

LIMA, E. L. *Curso de análise*. 12. ed. Rio de Janeiro: Coleção Projeto Euclides, 2008. v. 1. Citado na página 49.

MILNE, J. S. *Fields and Galois theory*. [s.n.], 2020. 138 p. Disponível em: <https://www.math.mcgill.ca/darmon/courses/16-17/algebra/milne.pdf>. Citado na página 15.

MORANDI, P. *Field and Galois theory*. New York: Springer-Verlag, 1996. Citado na página 15.

REZENDE, J. C. *Um estudo sobre as raízes da unidade e suas aplicações em matemática*. Rio Claro: [s.n.], 2017. 70 p. Orientador: Carina Alves. Dissertação (Mestrado em Matemática) - Universidade Estadual Paulista. Disponível em: <https://igce.rc.unesp.br/Home/Pos-Graduacao44/programasdepos/rezende_jc_me_rcla.pdf>. Citado 2 vezes nas páginas 15 e 86.

ROMERO, A. T. S. *Computação em grupos de permutação finitos com GAP*. Goiânia: [s.n.], 2018. 102 p. Dissertação (Mestrado em Matemática) - Universidade Federal de Goiás. Citado na página 15.

ROTH, R. L. On extensions of $\mathbb{Q}$ by square roots. *The American Mathematical Monthly*, v. 96, p. 392–393, 1971. Disponível em: <https://www.tandfonline.com/doi/abs/10.1080/00029890.1971.11992772>. Citado na página 15.

SOUZA, M. A. *Introdução a teoria de Galois*. Rio Grande: [s.n.], 2017. 69 p. Orientadora: Daiane Silva de Freitas. Trabalho de Conclusão de Curso (Licenciatura em Matemática) - Universidade Federal do Rio Grande. Disponível em: <https://imef.furg.br/images/stories/Monografias/Matematica_licenciatura/MarciodeSouza.pdf>. Citado na página 15.

STEWART I, N. *Galois theory*. [S.l.]: CRC press, 2015. Citado 6 vezes nas páginas 15, 63, 100, 101, 104 e 105.

Índice

Anel, 27
    com identidade, 28
    comutativo, 28
    de polinômios, 31
    sem divisores de zero, 28
Automorfismo, 29
Ação
    de grupos, 107
    transitiva, 107

Corpo, 28
    ciclotômico, 86
    fixo, 62
    intermediário, 38

Discriminante, 105
Domínio de integridade, 28
    característica de um, 28

Elemento
    algébrico, 39
    transcendente, 39
Endomorfismo, 29
Extensão, 35
    algébrica, 39
    finita, 49
    galoisiana, 57
    infinita, 49
    normal, 57
    separável, 60
    simples, 37

Fecho normal, 65

Grau de um polinômio, 31
Grupo, 21
    de permutações, 22
    abeliano, 21
    de Frobenius, 95
    de Galois, 61
    finito, 21
    ordem de um, 21
    quociente, 27
    simples, 100
    solúvel, 99

Homomorfismo
    de anéis, 29
    de grupos, 26
    núcleo de um, 29

Ideal, 29
    maximal, 29
    primo, 29
Isomorfismo, 26
Isomorfismo de extensões, 38

K-automorfismo de L, 61
K-monomorfismo de M em L, 64

Polinômio
    solúvel por radicais, 102
    ciclotômico, 86
    corpo de decomposição de um, 46
    derivada de um, 45
    irredutível, 32
    minimal, 40
    mônico, 31

Raiz da unidade, 85
    primitiva, 86

Subanel, 28
Subcorpo, 29
Subgrupo, 23
    normal, 26