UNIVERSIDADE FEDERAL DO PARANÁ

MARCEL THADEU DE ABREU E SOUZA

TEORIAS DE GALOIS E DE PICARD-VESSIOT: UM PASSEIO COM EXEMPLOS E APLICAÇÕES

CURITIBA
2021

MARCEL THADEU DE ABREU E SOUZA

TEORIAS DE GALOIS E DE PICARD-VESSIOT: UM PASSEIO COM EXEMPLOS E APLICAÇÕES

Monografia apresentada à disciplina "Trabalho de Conclusão de Curso II" como requisito parcial para a obtenção do grau de Licenciado e Bacharel em Matemática pela Universidade Federal do Paraná.
Orientador: Professor Doutor Diego Mano Otero

CURITIBA
2021

MINISTÉRIO DA EDUCAÇÃO E DO DESPORTO
UNIVERSIDADE FEDERAL DO PARANÁ
SETOR DE CIÊNCIAS EXATAS
COORDENAÇÃO DO CURSO DE MATEMÁTICA

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

No dia 15 de Dezembro de 2021, na sala Virtual do Microsoft TEAMS, foi instalada pelo(a) Professor(a) Diego Otero, a Banca Examinadora para o Trabalho de Conclusão de Curso do curso de graduação em Matemática da UFPR. Estiveram presentes ao Ato, professores alunos e visitantes. A banca examinadora foi constituída pelos professores: Alexandre Luis Trovon de Carvalho, e Marcelo Muniz Silva Alves, do Departamento de Matemática da UFPR; e Diego Otero, orientador(a) da monografia a quem coube a presidência dos trabalhos. Às 16 horas, a banca iniciou seus trabalhos, convidando o aluno Marcel Thadeu de Abreu e Souza a fazer a apresentação da monografia intitulada "Teorias de Galois e de Picard-Vessiot: Um passeio com exemplos e aplicações". Encerrada a apresentação, iniciou-se a fase de argüição pelos membros participantes. Após a argüição, a banca com pelo menos 02 (dois) membros reuniu-se para a apreciação do desempenho do estudante. Tendo em vista a monografia e a argüição, os membros presentes da banca decidiram por sua aprovação (aprovação/reprovação), com nota 100.

Curitiba, 15 de Dezembro de 2021.

Prof. Dr. Alexandre Luis Trovon de Carvalho
Titular

Prof. Dr. Marcelo Muniz Silva Alves
Titular

Prof. Dr. Diego Otero
Presidente

AGRADECIMENTOS

A Deus, por zelar pela minha saúde, mesmo nesses momentos difíceis gerados pela pandemia.

À minha mãe Debora, à minha tia Silvana e à minha avó Alice, que sempre me deram suporte, carinho e incentivo. Também pela preocupação que tiveram com os meus estudos e por me proporcionarem uma educação de qualidade.

Ao professor Diego, por ter sido meu orientador nesse trabalho e ter guiado o meu aprendizado, e aos professores Marcelo e Alexandre Trovon, pelo interesse e disponibilidade em fazer parte da minha banca.

Às professoras Mael e Tanise, por também me orientarem em outros trabalhos de iniciação científica ao longo do curso, e ao professor Zeca, por sua tutoria em projetos como o PET, POTI e TOPMAT, os quais contribuíram com a minha formação.

Aos meus amigos de longa data e aos que conheci durante a graduação, pelo companheirismo, pelas conversas, pelas risadas e por todos os momentos de alegria e descontração que tornaram este meu caminho mais tranquilo e divertido.

A todos que participaram, direta ou indiretamente da minha formação.

RESUMO

Este trabalho tem como princípio introduzir ambas as teorias de Galois e de Picard-Vessiot apresentando exemplos e algumas de suas aplicações, bem como um contexto histórico. Entre as aplicações abordadas, apresentaremos resultados que determinam se uma equação polinomial é solúvel por radicais, justificaremos a impossibilidade das construções dadas pelos Problemas Clássicos da Matemática Grega, e mostraremos critérios para determinar se uma função com entrada real possui primitiva elementar.

Palavras-chave: Teoria de Galois; Corpos diferenciais; Teoria de Picard-Vessiot; Teoria de Galois Diferencial; Solubilidade de equações polinomiais; Construções com régua e compasso; Integração em termos de funções elementares.

ABSTRACT

The principle of this work is to introduce both Galois and Picard-Vessiot theories, presenting examples and some of their applications, as well as a historical context. Among the applications discussed, we will present results that determine whether a polynomial equation is solvable by radicals, we will justify the impossibility of the constructions given by the Classical Greek Problems, and we will show criteria to determine whether a real input function has an elementary primitive.

Keywords: Galois Theory; Differential fields; Picard-Vessiot Theory; Differential Galois Theory; Solubility of polynomial equations; Constructions with ruler and compass; Integration in elementary terms.

Sumário

Introdução

A Teoria de Galois é um ramo da matemática, originalmente introduzido por Évariste Galois (1811-1832), que conecta a teoria de corpos com a teoria de grupos. Esta conexão ocorre através do Teorema Fundamental de Galois, que permite trazer alguns problemas da teoria de corpos para a teoria de grupos.

Galois introduziu a matéria ao estudar raízes de equações polinomiais. Este estudo permitiu que ele caracterizasse equações polinomiais que são solúveis por radicais em termos de propriedades do grupo de permutações de suas raízes. Uma equação é dita solúvel por radicais se suas raízes puderem ser expressas por uma fórmula que contenha apenas inteiros, raízes n-ésimas e as quatro operações aritméticas básicas (adição, subtração, multiplicação e divisão). O interessante é que essa descoberta de Galois demonstra o Teorema de Abel-Ruffini, que afirma que um polinômio geral (com coeficientes indeterminados) de grau maior ou igual a 5 não é solúvel por radicais, teorema o qual a prova foi publicada pouco antes de Évariste Galois introduzir sua teoria.

A Teoria de Galois também teve outras aplicações surpreendentes. Através dela, é possível mostrar que os três problemas clássicos da matemática grega não podem ser resolvidos como foram enunciados (a duplicação do cubo, a trisecção do ângulo e a quadratura do círculo), e também é possível caracterizar os polígonos regulares que são construtíveis (esta caracterização foi dada anteriormente por Gauss, mas todas as provas conhecidas de que esta caracterização está completa requer a teoria de Galois).

No final do século XIX foi introduzida a Teoria de Galois Diferencial, também chamada de Teoria de Picard-Vessiot, por Émile Picard e Ernest Vessiot. Esta teoria estuda as soluções de equações diferenciais ordinárias lineares, além de permitir descrever quando uma equação diferencial ordinária linear pode ser resolvida através de quadraturas em termos de propriedades do grupo de Galois diferencial. Uma equação diferencial é dita solúvel por quadraturas se sua solução geral puder ser expressa em termos de uma ou mais integrais. Uma outra aplicação desta teoria é no estudo da integração em termos de funções elementares.

Esse trabalho tem como objetivo introduzir ambas as teorias de Galois e de Picard-Vessiot através de exemplos, e mostrar algumas de suas aplicações.

O trabalho está estruturado da seguinte maneira: o capítulo 1 aborda um pouco a respeito da história das teorias de Galois e Picard-Vessiot, o capítulo 2 apresenta alguns

conceitos preliminares das teorias de grupos, corpos e anéis necessários para os capítulos seguintes, o capítulo 3 apresenta uma introdução à teoria de Galois e algumas de suas aplicações, e o capítulo 4 apresenta uma introdução à teoria de Picard-Vessiot e sua aplicação no estudo da integração em termos de funções elementares.

É fortemente recomendado que o leitor tenha realizado os cursos de Cálculo em uma Variável Real, Álgebra Linear e Teoria de Números antes da leitura deste trabalho. Os conceitos básicos necessários das teorias de grupos, corpos e anéis são introduzidos no trabalho.

Capítulo 1

Um pouco de história

1.1 Teoria de Galois

1.1.1 Surgimento

A Teoria de Galois surgiu com o estudo dos polinômios simétricos. Este estudo foi pela primeira vez formalizado no século XVI pelo matemático francês François Viète. No século XVII, Albert Girard conseguiu entender um padrão geral de formação dos coeficientes das equações polinomiais a partir da soma e do produto de suas raízes.

O problema para equações cúbicas foi parcialmente resolvido no século XVI pelo italiano Scipione del Ferro, que entretanto não publicou seu trabalho. Esta solução depois foi redescoberta de forma independente em 1535 por Niccolò Fontana Tartaglia, que depois compartilhou esses resultados com Girolamo Cardano. Cardano estendeu esse resultado para outros casos. Seu aluno Lodovico Ferrari resolveu o problema para equações quárticas. Em 1545, Cardano publicou resultados incluindo o método de Tartaglia e o problema para equações quárticas em seu livro *Ars Magna*. Entretanto, Cardano não exibiu uma fórmula geral para resolver essas equações em seu livro, pois na época não tinha sido definido os conceitos de números complexos e nem a notação algébrica que pudesse descrever uma equação cúbica geral. Foi apenas em 1572 que Rafael Bombelli conseguiu resolver todas as formas possíveis da equação cúbica.

Um passo adiante nessa área foi dado em 1770 por Joseph-Louis Lagrange, quando analisou em seu artigo *Réflexions sur la résolution algébrique des équations* as soluções das cúbicas e quárticas de Cardano e Ferrari, considerando-as em termos das pemutações de raízes, o que forneceu uma compreensão das soluções em geral e estabeleceu as bases para a teoria de grupos e de Galois.

O problema para equações quínticas foi quase solucionado por Paolo Ruffini em 1799, que trabalhou com grupos de permutações. Mas sua solução tinha uma brecha que só foi resolvida por Niels Henrik Abel, que publicou a prova completa em 1824 da impossibilidade de um polinômio geral (com coeficientes indeterminados) de grau maior ou igual a

5 ser solúvel por radicais, resultado que ficou conhecido como o Teorema de Abel-Ruffini. O critério preciso para determinar se uma equação polinomial de grau 5 ou superior é solúvel ou não só foi dado por Évariste Galois.

1.1.2 Desenvolvimento

Évariste Galois nasceu em 25 de outubro de 1811, na cidade de Bourg-la-Reine, que fica a alguns quilômetros ao sul de Paris. Seu pai, Nicolas-Gabriel era proprietário de uma escola. Sua mãe, Adélaide Demante, era filha e irmã de juristas da Faculdade de Direito de Paris. Ela recebeu de seu pai uma cuidadosa e extensa educação. Até Évariste ter doze anos, ela foi sua única professora. No outono de 1823, ele entrou em Louis-le-Grand, um dos célebres liceus de Paris, a dois passos de Sorbonne e do Collège de France. Aos quinze anos ele começou o seu estudo em matemática, entrando na classe conhecida como *Mathématiques préparatoires*. Um novo mundo se abriu para ele e o estudo da matemática se tornou a paixão de sua vida. Évariste começou a estudar autores originais, especialmente Lagrange.

No outono de 1828, Galois ingressou na classe de *Mathématiques spéciales*, a cargo do matemático e professor Richard. Sob sua direção inteligente e simpática, o progresso de Galois tornou-se ainda mais notável. Suas soluções originais de problemas propostos em classe eram expostas por Richard com muitos elogios.

Aos dezessete anos, Galois fez suas primeiras descobertas na teoria das equações que são solúveis por radicais. Ele redigiu um breve texto sobre o assunto e Cauchy o levou para apresentar à Academia de Ciências. Infelizmente, nunca mais se ouviu falar deste texto. Nessa época também foi publicado seu primeiro artigo, intitulado *Démonstration d'un théorème sur les fractions continues périodiques*, aparecendo no *Annales de Gergonne* de março de 1829.

Galois tinha um desejo muito forte de entrar na École Polytechnique, a primeira escola de Matemática da França. Ele se apresentou duas vezes para o exame, mas foi reprovado em ambas as vezes, o que chocou pessoas que conheciam sua genialidade. Galois tinha o hábito de trabalhar quase que exclusivamente em sua cabeça quando fazia matemática. Muitos fatos que requeriam demonstração, para Galois eram triviais e evidentes, o que causou descontentamento dos examinadores. Infelizmente os examinadores eram incapazes de apreciar os extraordinários talentos do jovem que estava em sua frente.

Não sobrava nada para Galois, além de entrar na École Préparatoire, um destino que enchia seu coração com amargura e desespero. Durante esse período, Galois também recebe a péssima notícia do falecimento de seu pai, a quem ele ternamente amava. Mesmo assim, Galois continuou com seus estudos na matemática, expandindo o seu já vasto conhecimento e amadurecendo suas próprias descobertas.

Durante seu primeiro ano na École Préparatoire, ele publicou quatro textos. Em

janeiro de 1830, Galois apresentou à Academia outro texto contendo informações detalhadas sobre sua pesquisa. Este texto foi encaminhado para Fourier, mas infelizmente, Fourier faleceu logo após isso, e o texto se perdeu. No final de 1830, Galois foi expulso da École Préparatoire por se envolver em polêmicas políticas. Logo depois, Poisson convidou Galois a fazer uma nova redação de suas pesquisas e se voluntariou para apresentá-lo pessoalmente à Academia. Inspirado por uma nova esperança, Galois escreve o único texto finalizado que temos registro de sua grande teoria no ramo de solução de equações, cujo título é *Sur les conditions de résolubilité des équations par radicaux*. Neste mesmo período, Galois abriu um curso de Álgebra Avançada que ocorreria em uma livraria perto de Sorbonne. Infelizmente este texto foi declarado ininteligível por Poisson.

Galois estava já associado a facção mais reacionária do partido republicano, e cada vez se afundava ainda mais na confusão política que estava estourando na França. Já havia sido preso duas vezes por ofensas políticas, ele passou a maior parte do último ano de sua vida na prisão de Sainte-Pélagie. Em março de 1832 irrompeu uma epidemia de cólera em Paris e os prisioneiros de Sainte-Pélagie foram libertados. Nas semanas seguintes, Galois se envolveu em um romance com uma mulher chamada Stéphanie-Félice Poterine du Motel. Stéphanie já era comprometida com um cidadão chamado Pescheux d'Herbinville, que descobriu a infidelidade de sua noiva. Pescheux ficou furioso, e sendo um dos melhores atiradores da França, ele não hesitou em desafiar Galois para um duelo ao raiar do dia. Galois tinha o presentimento que morreria e por conta disso, no dia anterior ao duelo, ele registrou todas as suas ideias no papel e escreveu cartas para seus amigos explicando as circunstâncias.

No dia 29 de maio de 1832, na noite anterior ao duelo, Galois que já estava certo que iria morrer escreveu uma carta para seu amigo Auguste Chevalier. Ele pediu para que Chevalier implorasse a Gauss e Jacobi em darem suas opiniões, não na verdade, mas sim na importância de seus teoremas. Em conformidade com os desejos de Galois, a carta foi publicada em setembro de 1832 no Revue Encyclopédique e uma nota editorial afirmava que todos os manuscritos de Galois apareceriam em breve no mesmo jornal sob a direção de Chevalier. Infelizmente, este não foi o caso e a carta não obteve a atenção que merecia. Foi apenas em setembro de 1843 que Liouville, aquele que havia preparado os artigos de Galois para publicação, anunciou para a Academia que Galois havia resolvido o problema da solubilidade de equações por radicais. Mas a publicação do artigo de 1831 em questão foi postergada até 1846. Ao mesmo tempo, entre 1844 e 1846, Cauchy voltou a estudar grupos, estudo no qual ele estava parado desde 1815. Isto o ajudou a esclarecer as ideias de Galois e o significado de seu trabalho começou a ser apreciado. Apenas em 1852, 20 anos após a morte de Galois, que sua teoria foi disponibilizada para o público geral de forma inteligível e estabelecida com total rigor. De acordo com Weber, Kronecker tomou ciência da teoria de Galois durante sua visita a Paris em 1853, onde esteve intimamente associado a Hermite, Bertrand e outros importantes matemáticos franceses. A primeira

menção que Kronecker faz ao nome de Galois está em uma carta a Dirichlet em março de 1856. Dedekind também se familiarizou muito cedo com a teoria de Galois, uma vez que ele lecionou em 1857-1858 sobre álgebra avançada e em especial sobre teoria de Galois. Segundo Weber, este foi provavelmente o primeiro relato a respeito da teoria de Galois feito em uma universidade alemã. O primeiro relato dado em um livro de álgebra está na terceira edição da álgebra de Serret (1866). A partir daí, o conhecimento da teoria de Galois se tornou possível para o mundo todo.

Muitos fragmentos de manuscritos não publicados de Galois foram editados e publicados por Jules Tannery em 1907. Finalmente, em 1961, R. Bourgne e J. P. Azra editaram uma crítica coleção que reúne todos os escritos de Galois (papéis, cartas e rascunhos de seus artigos).

A teoria de corpos foi criada por Steinitz em 1910 e se desenvolveu rapidamente na década seguinte quando Emil Artin demonstrou resultados dentro deste ramo. A Teoria de Galois que conhecemos atualmente se deve em grande parte ao matemático austríaco Emil Artin (1898-1962), também conhecido com um dos fundadores da álgebra abstrata moderna.

1.1.3 Filosofia

A Teoria de Galois observada do ponto de vista filosófico foi e ainda é muito rica, por conta do seu grande significado tanto na evolução da metodologia matemática, quanto na mudança de mentalidade matemática. A Teoria de Galois trouxe justificativa para diversos conteúdos matemáticos algébricos e geométricos, muitos dos quais geralmente são aprendidos durante a Educação Básica. Ela também auxiliou no surgimento e no desenvolvimento da teoria de grupos, estudo que se tornou base do ramo da álgebra abstrata.

1.2 Integração em termos finitos

1.2.1 Estudos de Liouville

O matemático francês Joseph Liouville (1809-1882) é geralmente conhecido como o fundador da teoria de integração em termos finitos. Entre os anos de 1833 e 1835, Liouville investigou se era possível determinar se uma dada integral indefinida poderia ser expressa como uma função explícita finita, isto é, em termos finitos utilizando apenas funções algébricas, logarítmicas, exponenciais, trigonométricas, ou inversas trigonométricas. Em 1834, Liouville determinou uma fórmula para calcular a integral indefinida de uma função algébrica que pode ser expressa em sua forma explícita finita. Esse resultado permitiu que Liouville verificasse que certas integrais elípticas não podiam ser expressas em termos

finitos. Em 1835, Liouville generalizou este resultado, e, com isso, demonstrou que certas integrais, dentre elas a integral $\int \frac{e^x}{x}\,dx$, não podiam ser expressas em termos finitos.

Na verdade, vários matemáticos do século XVIII já tinham mencionado resultados semelhantes e, de fato, inspiraram o estudo de Liouville. Entre estes matemáticos, estão Alexis Fontaine e Marie-Jean Marquis de Condorcet. Liouville disse que faltava prova e exatidão em muitos dos teoremas de Fontaine. A respeito da impossibilidade de expressar certas integrais elípticas em termos finitos, Pierre-Simon Laplace afirmou ter provado, mas nunca publicou provas rigorosas destes seus teoremas.

Após este estudo sobre integrais indefinidas, Liouville começou a estudar as soluções de equações diferenciais ordinárias em termos finitos. A complexidade deste estudo pode ser vista no tempo que se passou desde que ele começou a estudar isto em 1834 até quando ele publicou o seu primeiro artigo sobre este tópico em 1839 (mais que o dobro do tempo que ele necessitou para desenvolver sua teoria da integração em termos finitos). O seu último artigo em 1841 concluiu o seu estudo nessa área.

Para integrais indefinidas, o problema geral de Liouville continuou sem solução: "Dada uma função explícita finita, como podemos determinar, em um número finito de etapas, se a integral desta função também é explícita finita? E caso ela seja, como calcular essa integral?" Esta pergunta ficou sem resposta até 1970 quando Robert H. Risch desenvolveu um algoritmo que resolvia esse problema.

1.2.2 Estudos posteriores

Em 1841, Liouville concluiu seu estudo na teoria de integração em termos finitos e parte da pesquisa feita por Liouville permaneceu oculta por praticamente um século. Em 1948, através do livro *Integration in Finite Terms: Liouville's Theory of Elementary Methods*, o matemático estadunidense Joseph Fels Ritt (1893-1951) trouxe à tona estudos de Liouville nessa área que nunca haviam sido publicados. Por 30 anos, quase até sua morte em 1951, Ritt produziu uma série de artigos e livros que abriram um novo campo da Matemática: a álgebra diferencial.

Em 1946, o matemático ucraniano Alexander Markowich Ostrowski (1893-1986) reformulou o teorema de Liouville em um cenário algébrico, utilizando a noção de extensões de corpos diferenciais.

Em 1968, o matemático estadunidense Maxwell Alexander Rosenlicht (1924-1999) publicou o primeiro trabalho puramente algébrico a respeito da teoria de Liouville nas funções com primitivas elementares, fugindo completamente da abordagem analítica do trabalho de Liouville. Em 1970, Robert Risch (1939), aluno de Rosenlicht, forneceu um algoritmo que resolvia o problema geral.

Os avanços ocorridos no início da década de 1970 vieram juntos com o avanço tecnológico e com a chegada dos computadores, pois refinaram todo esse estudo em ferramentas

práticas, e, com isso, técnicas matemáticas puramente abstratas puderam ser reduzidas em algoritmos funcionais.

1.2.3 Surgimento da Teoria de Picard-Vessiot

O matemático norueguês Sophus Lie (1842-1899) desenvolveu estudos na área da teoria de grupos e equações diferenciais. A teoria dos grupos e álgebras de Lie é hoje uma parte fundamental da matemática que possui muitas aplicações, mas sua inspiração original foi o campo das equações diferenciais. Os matemáticos do século XIX viam a arte de resolver equações diferenciais como simples aplicações de técnicas especiais. Lie percebeu que essas técnicas especiais faziam parte de um procedimento baseado na invariância de soluções das equações diferenciais sob um grupo contínuo de simetrias. Para estudar esses grupos contínuos, Lie associou a cada grupo contínuo um espaço vetorial correspondente munido de uma multiplicação que era "antiassociativa". Disto, surgiu o que chamamos hoje de grupos de Lie e álgebras de Lie. Lie tentou associar grupos contínuos com equações diferenciais no mesmo espírito do trabalho de Galois com equações polinomiais. Ele provou que as equações que correspondiam à grupos contínuos solúveis eram solúveis por quadraturas. A teoria de equações diferenciais proposta por Lie ficou tão famosa na época que encontrou lugar até no currículo de algumas universidades. Entretanto, este tópico sumiu depois da formulação abstrata dos grupos de Lie e álgebras de Lie dada por Élie Cartan (1869-1951) ter ganhado dominância.

Uma teoria mais refinada, a "Teoria de Galois para equações diferenciais" foi proposta por Charles Émile Picard e Ernest Vessiot para equações diferenciais ordinárias lineares homogêneas. Em 1948, o matemático estadunidense Ellis Robert Kolchin (1916-1991) escreveu o artigo *Algebraic matric groups and the Picard-Vessiot Theory of homogeneous linear ordinary differential equations*, formalizando a Teoria de Picard-Vessiot que conhecemos atualmente. O estudo de Kolchin abriu portas para o desenvolvimento da teoria de grupos algébricos lineares e impulsionou a pesquisa na área de álgebra diferencial iniciada por Ritt.

Capítulo 2

Conceitos preliminares

Neste capítulo, iremos introduzir conceitos preliminares necessários para o desenvolvimento do trabalho. Estes conceitos abrangem definições e resultados básicos do estudo de grupos, corpos e anéis, bem como critérios de irredutibilidade de polinômios.

2.1 Grupos

Definição 2.1. Um **grupo** é um conjunto G munido de uma operação $(*)$ que satisfaz as seguintes propriedades:

(a) Existe um elemento $e \in G$ tal que $e * g = g * e = g$, $\forall\, g \in G$ (elemento neutro);

(b) Para qualquer $g \in G$, existe um elemento $h \in G$ tal que $g * h = h * g = e$ (todo elemento possui inversa);

(c) $g * (h * k) = (g * h) * k$, $\forall\, g, h, k \in G$ (associatividade).

Se G é um grupo, então G é dito um **grupo abeliano** se

(d) $g * h = h * g$, $\forall\, g, h \in G$ (comutatividade).

Normalmente chamamos a operação $(*)$ de multiplicação e omitimos o seu símbolo, isto é, podemos escrever gh ao invés de $g * h$.

O elemento neutro de um grupo é único. Da mesma forma, a inversa de todo elemento de um grupo é única.

Definição 2.2. Sejam G um grupo e H um subconjunto não vazio de G. Se H é um grupo com a mesma operação de G, então dizemos que H é um **subgrupo** de G, e denotamos $H \leq G$.

Proposição 2.3. *Sejam G um grupo e H um subconjunto não vazio de G. Dizemos que H é um subgrupo de G se, e somente se, H satisfaz as seguintes propriedades:*

(a) $e_G \in H$;

(b) $g, h \in H \Rightarrow gh \in H$;

(c) $h \in H \Rightarrow h^{-1} \in H$.

Demonstração.

($\Rightarrow$) Seja H um subgrupo de G. Então as propriedades (a), (b) e (c) seguem de imediato pelo fato do elemento neutro ser único e da inversa de todo elemento de G ser única.

($\Leftarrow$) A condição (a) mostra a existência do elemento neutro em H. A condição (b) nos mostra que a operação de G induz uma operação em H e essa operação é também associativa em H, pois ela é associativa em G. A condição (c) mostra que todo elemento de H possui inversa em H. Logo, H é um subgrupo de G. □

Definição 2.4. Seja S um subconjunto do grupo G. O **subgrupo gerado** por S é o menor subgrupo de G que contém S e é denotado por $\langle S \rangle$.

Você pode se perguntar o motivo de tal menor subgrupo sempre existir. Uma maneira de entender isto é perceber que dada uma família arbitrária $\{H_j\}_{j \in J}$ de subgrupos de G, a interseção $\bigcap_{j \in J} H_j$ também define um subgrupo de G. Então, para determinar $\langle S \rangle$, basta intersectar os elementos da família $\{H : S \subseteq H \leq G\}$.

Definição 2.5. A **ordem de um grupo** G é a quantidade de elementos de G, e é denotada por $|G|$. Se G não é finito, dizemos que G possui ordem infinita. A **ordem de um elemento** $g \in G$, denotada por $\mathcal{O}(g)$, é definida como o menor número natural tal que $g^n = e$, se tal n existir. Caso contrário, dizemos que g possui ordem infinita.

Definição 2.6. Um grupo G é dito **grupo cíclico** se ele é gerado por um único elemento, ou seja, $G = \langle g \rangle$ para algum $g \in G$. Em geral, se $S \subseteq G$ e $\langle S \rangle = G$, dizemos que G é gerado por S.

Vamos ver alguns exemplos de grupos.

Exemplos 2.7.

1. O conjunto $\mathbb{Z}$ munido da operação de adição usual $(+)$ é um grupo abeliano.

2. O conjunto $\mathbb{Z}$ munido da operação de multiplicação usual $(\cdot)$ não é um grupo, pois os únicos elementos de $\mathbb{Z}$ que têm inverso são -1 e 1.

3. O conjunto $\mathrm{M}_n(\mathbb{R}), n \geq 2$ munido da operação de multiplicação usual $(\cdot)$ não é um grupo, pois nem toda matriz é invertível, mas perceba que o conjunto

$$\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathrm{M}_n(\mathbb{R}) : \det(A) \neq 0\}$$

munido da operação de multiplicação usual $(\cdot)$ define um grupo. O subconjunto

$$\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) : \det(A) = 1\}$$

de $\mathrm{GL}_n(\mathbb{R})$ é um subgrupo de $\mathrm{GL}_n(\mathbb{R})$.

Definição 2.8. Sejam G um grupo munido de uma operação $(*)$ e H um grupo munido de uma operação $(\cdot)$, e considere a função $f : G \to H$. Dizemos que f é um **homomorfismo de grupos** se $f(g * h) = f(g) \cdot f(h)$, $\forall\, g, h \in G$. Se f é um homomorfismo de grupos bijetivo, então dizemos que f é um **isomorfismo de grupos**. Neste caso, dizemos que G e H são isomorfos e denotamos $G \cong H$.

Definição 2.9. Seja $f : G \to H$ um homomorfismo de grupos. O conjunto

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

é chamado de **núcleo** de f, e o conjunto

$$\mathrm{Im}(f) = \{f(g) \in H : g \in G\}$$

é chamado de **imagem** de f.

Alguns fatos interessantes a respeito desses conjuntos é que o núcleo e a imagem de um homomorfismo de grupos $f : G \to H$ são subgrupos de G e H, respectivamente, e que $\ker(f) = \{e_G\}$ se, e somente se, f é injetora.

Definição 2.10. Sejam G um grupo, H um subgrupo de G e $g \in G$. A **classe lateral à esquerda** de g módulo H é $gH = \{gh : h \in H\}$. Analogamente, a **classe lateral à direita** de g módulo H é $Hg = \{hg : h \in H\}$. O conjunto de todas as classes laterais à esquerda (ou à direita) de H em G é denotado por G/H.

Proposição 2.11. *Sejam G um grupo, H um subgrupo de G e $g \in G$. Dizemos que $a \in gH$ se, e somente se, $g^{-1}a \in H$, o que acontece se, e só se, $gH = aH$. Logo, classes laterais distintas são disjuntas.*

Demonstração.

Note que:

$$a \in gH \Leftrightarrow a = gh \text{ para algum } h \in H \Leftrightarrow g^{-1}a \in H \Leftrightarrow a^{-1}g \in H \Leftrightarrow g \in aH.$$

Se $a = gh$ para algum $h \in H$, então $aH = (gh)H = g(hH) = gH$. □

Como classes laterais distintas são disjuntas, então as classes laterais de qualquer subgrupo formam uma partição do grupo todo.

Suponha que G/H possui exatamente n classes laterais, isto é,

$$G/H = \{g_1H, g_2H, \ldots, g_nH\},$$

onde $g_1, \ldots, g_n \in G$. Como $\{g_1H, \ldots, g_nH\}$ é uma partição de G, então $g_iH \cap g_jH = \emptyset$ se $i \neq j$ e, portanto, $G = \bigsqcup_{i=1}^{n} g_iH$ (união disjunta).

Definição 2.12. Sejam G um grupo e H um subgrupo de G. O número de classes laterais distintas de H em G é dito **índice** de H em G, e é denotado $|G : H|$.

Vamos provar agora o Teorema de Lagrange.

Teorema 2.13 (Teorema de Lagrange)**.** *Se G é um grupo finito e $H \leq G$, então $|H|$ divide $|G|$.*

Demonstração.

Seja $H \leq G$. Suponha que $g_1H, \ldots, g_nH$ são as classes laterais distintas de H em G. Note que as funções $\psi_i : H \to g_iH$, $h \mapsto g_ih$ são claramente sobrejetivas, e mais se $\psi_i(h_1) = \psi_i(h_2)$ tem-se $g_ih_1 = g_ih_2 \Rightarrow h_1 = h_2$, o que implica que ψ_i são bijetivas e portanto $|g_iH| = |H|$. Como o conjunto de classes distintas é uma partição de G, então

$$|G| = \left|\bigcup_{i=1}^{n} g_iH\right| = \sum_{i=1}^{n} |g_iH| = \sum_{i=1}^{n} |H| = n \cdot |H|,$$

e portanto $|H|$ divide $|G|$. □

Da demonstração do Teorema de Lagrange, segue de graça o seguinte corolário:

Corolário 2.14. *Se G é um grupo finito e $H \leq G$, então $|G| = |G : H| \cdot |H|$.*

Vamos definir agora os subgrupos mais importantes da teoria de grupos: os subgrupos normais.

Definição 2.15. Seja G um grupo. Um subgrupo N de G é dito **subgrupo normal** de G se $ghg^{-1} \in N$, $\forall\, h \in N$, $\forall\, g \in G$ ou, equivalentemente, se $gN = Ng$, $\forall\, g \in G$.

Proposição 2.16. *Seja $f : G \to H$ um homomorfismo de grupos. O subgrupo* $\ker(f)$ *de G é subgrupo normal.*

Demonstração.

Sejam $g \in G$ e $h \in \ker(f)$. Note que $f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)e_Hf(g^{-1}) = f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H$. Logo $ghg^{-1} \in \ker(f)$ e segue que $\ker(f)$ é um subgrupo normal de G. □

Com o conceito de subgrupo normal, agora podemos definir grupo quociente e demonstrar um resultado muito importante: o teorema do isomorfismo para grupos.

Definição 2.17. Seja N um subgrupo normal do grupo G. O **grupo quociente** G/N é o conjunto das classes laterais gN de N em G munido com a operação

$$(gN)(hN) = (gh)N.$$

Se $N \leq G$ não é normal, então G/N ainda denota o conjunto das classes laterais de N em G, mas sem estar munido com a operação acima.

Teorema 2.18 (Teorema do isomorfismo de grupos)**.** *Seja $f : G \to H$ um homomorfismo de grupos. Então $G/\ker(f) \cong \mathrm{Im}(f)$.*

Demonstração.

Seja $K = \ker(f)$ e defina a aplicação $\varphi : G/K \to \mathrm{Im}(f)$ dada por $\varphi(gK) = f(g)$.

Suponha que $gK = hK$. Então $g = hk$ para algum $k \in K$ e, portanto,

$$f(g) = f(hk) = f(h)f(k) = f(h)e = f(h),$$

o que mostra que φ está bem definida.

Perceba também que, dados $g, h \in G$ quaisquer, temos

$$\varphi((gh)K) = f(gh) = f(g)f(h) = \varphi(gK)\varphi(hK),$$

o que mostra que φ é um homomorfismo.

A aplicação φ é sobrejetiva por definição, e é injetiva pois, dados $g, h \in G$ tais que $\varphi(gK) = \varphi(hK)$, temos

$$\varphi(gK) = \varphi(hK) \Rightarrow f(g) = f(h) \Rightarrow f(gh^{-1}) = e_H \Rightarrow gh^{-1} \in K \Rightarrow gK = hK.$$

Logo, φ é um isomorfismo de grupos e concluímos que $G/\ker(f) \cong \mathrm{Im}(f)$. □

Enunciaremos a seguir mais um resultado que será utilizado no decorrer do trabalho. A demonstração podem ser encontrada em [7], Capítulo VI, Teorema 6.

Teorema 2.19 (Teorema de Cauchy)**.** *Seja G um grupo finito cuja ordem é divisível por um número primo p. Então o grupo G contém um elemento de ordem p.*

Vamos agora estudar mais dois exemplos de grupos importantíssimos: os grupos cíclicos e os grupos de permutações.

Exemplos 2.20.

1. O conjunto $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, $n \geq 2$ inteiro, munido da operação de adição usual $(+)$ é um grupo cíclico de ordem n.

2. Seja $S = \{1, 2, \ldots, n\}$. O conjunto $S_n = \{f : S \to S : f \text{ é bijetiva}\}$ munido da operação de composição de funções $(\circ)$ é um grupo, chamado de **grupo de permutações**, e possui ordem $n!$. Utilizamos a notação $(a_1 a_2 \cdots a_k)$ com k inteiro, $1 \leq k \leq n$, e $a_1, \ldots, a_k \in S$, para indicar a função que leva a_1 em a_2, a_2 em a_3, sucessivamente até a_k em a_1, e fixa outros elementos de S. Para o caso $n = 3$, temos $S = \{1, 2, 3\}$ e

$$S_3 = \{(1), (12), (13), (23), (123), (132)\}.$$

   Note que:

   - (1) é a função que fixa todos os elementos.
   - (12) leva 1 em 2, 2 em 1, e fixa 3.
   - (13) leva 1 em 3, 3 em 1, e fixa 2.
   - (23) leva 2 em 3, 3 em 2, e fixa 1.
   - (123) leva 1 em 2, 2 em 3, e 3 em 1.
   - (132) leva 1 em 3, 3 em 2, e 2 em 1.

   Um fato interessante é que o grupo S_n é gerado pelo ciclo $\sigma = (12 \cdots n)$ e pela transposição $\tau = (12)$. No caso $n = 3$, $S_3 = \langle (12), (123) \rangle$.

2.2 Corpos e anéis

Definição 2.21. Um **corpo** é um conjunto K munido das operações de adição $(+)$ e multiplicação $(\cdot)$ e dois elementos distintos 0 e 1, que satisfaz as seguintes propriedades:

(a) $(K, +, 0)$ é um grupo abeliano;

(b) $(K \setminus \{0\}, \cdot, 1)$ é um grupo abeliano;

(c) $a \cdot (b + c) = a \cdot b + a \cdot c$, $\forall\, a, b, c \in K$.

Definição 2.22. Um corpo K é dito **algebricamente fechado** se qualquer polinômio não constante $p \in K[x]$ tiver uma raiz em K.

Definição 2.23. A **característica** de um corpo é o menor inteiro positivo n tal que

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ parcelas}} = 0.$$

Se tal n não existe, dizemos que o corpo possui característica zero.

Observação 1. Ao longo deste trabalho, se um corpo tomado arbitrariamente estiver com a característica omitida, considere que ele possui característica zero.

Uma estrutura um pouco mais fraca que um corpo, mas também muito importante, é chamada de anel.

Definição 2.24. Um **anel comutativo** é um conjunto A munido das operações de soma $(+)$ e multiplicação $(\cdot)$ e dois elementos distintos 0 e 1, que satisfaz as seguintes propriedades:

(a) $(A, +, 0)$ é um grupo abeliano;

(b) A operação de multiplicação $(\cdot)$ é comutativa e associativa;

(c) $a \cdot 1 = 1 \cdot a = a$, $\forall\, a \in A$;

(d) $a \cdot (b + c) = a \cdot b + a \cdot c$, $\forall\, a, b, c \in A$.

Observação 2. Ao longo deste trabalho, utilizaremos o termo *anel* para indicar um anel comutativo com unidade conforme a definição dada acima.

Definição 2.25. Seja A um anel e B um subconjunto de A. Se B munido da adição e da multiplicação de A é um anel tal que $0_A, 1_A \in B$, então B é um **subanel** de A. Se B munido da adição e da multiplicação de A é um corpo tal que $0_A, 1_A \in B$, então B é um **subcorpo** de A.

Proposição 2.26. *Sejam A um anel e B um subconjunto não vazio de A. Dizemos que B é um subanel de A se, e somente se, B satisfaz as seguintes propriedades:*

(a) $0_A \in B$;

(b) $x, y \in B \Rightarrow x - y \in B$;

(c) $x, y \in B \Rightarrow xy \in B$.

Proposição 2.27. *Sejam A um anel e B um subconjunto não vazio de A. Dizemos que B é um subcorpo de A se, e somente se, B é um subanel de A e $x \in B \Rightarrow x^{-1} \in B$.*

Definição 2.28. Seja S um subconjunto do anel A. O **subanel gerado** por S é o menor subanel de A que contém S. Se A é corpo, então o **subcorpo gerado** por S é o menor subcorpo de A que contém S.

O motivo de tal menor subanel/subcorpo sempre existir é que dada uma família arbitrária $\{N_j\}_{j \in J}$ de subanéis/subcorpos de K, a interseção $\bigcap_{j \in J} N_j$ também define um subanel/subcorpo de K.

Definiremos agora mais duas estruturas que nos serão úteis.

Definição 2.29. Seja A um anel. Se $A \neq \{0\}$ e $ab \neq 0$, $\forall\, a, b \in A \setminus \{0\}$, então A é dito **domínio de integridade**.

Definição 2.30. O **corpo de frações** de um anel A é o corpo

$$\mathrm{Frac}(A) = \left\{ \frac{a}{b} : a, b \in A,\ b \neq 0 \right\},$$

munido das operações usuais de modo que

$$\frac{a}{b} = \frac{c}{d} \Longleftrightarrow ad = bc.$$

Um fato interessante é que um anel A é um subanel de $\mathrm{Frac}(A)$.

Agora vamos ver alguns exemplos das estruturas que definimos acima.

Exemplos 2.31.

1. Corpos são domínios de integridade, que por sua vez são anéis comutativos.
2. Os conjuntos $\mathbb{C}$, $\mathbb{R}$ e $\mathbb{Q}$ são corpos. Como $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, então $\mathbb{R}$ é subcorpo de $\mathbb{C}$ e $\mathbb{Q}$ é subcorpo de $\mathbb{C}$ e $\mathbb{R}$.
3. O conjunto $\mathbb{Z}$ é anel. Como $\mathbb{Z} \subseteq \mathbb{Q}$, então $\mathbb{Z}$ é subanel de $\mathbb{Q}$.
4. Dado $n \geq 2$ inteiro, o conjunto $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ é um anel. O conjunto $\mathbb{Z}_p$ é corpo se, e somente se, p é primo.
5. Se $\Omega \subseteq \mathbb{C}$ é aberto e conexo, então o conjunto das funções meromorfas[1] em Ω é um corpo.
6. O conjunto dos números algébricos sobre $\mathbb{Q}$

   $$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \exists\, f \in \mathbb{Q}[x],\ f \neq 0,\ f(\alpha) = 0\}$$

   é um corpo.
7. Seja A um anel. O conjunto

   $$A[x] = \{f(x) : f \text{ é um polinômio com coeficientes em } A\}$$

   é um anel comutativo.
8. Seja K um corpo. O conjunto das funções racionais

   $$K(x) = \left\{ \frac{f(x)}{g(x)} : f, g \in K[x] \text{ e } g(x) \neq 0 \right\}$$

[1] Uma função f é dita meromorfa em uma região Ω se for analítica em Ω, à exceção de polos isolados.

é um corpo.

Dado um corpo K, é possível realizar as operações de soma, subtração e multiplicação no anel de polinômios $K[x]$, mas não conseguimos dividir na maioria das vezes. Por exemplo, o elemento x^{-1} não pertence ao anel $K[x]$.

Entretanto, conseguimos ampliar $K[x]$ de forma que ele nos forneça inversas de uma forma natural. Basta tomarmos as funções racionais $\frac{p(x)}{q(x)} \in K(x)$. Note que agora o domínio de $\frac{p(x)}{q(x)}$ não é todo o corpo K, mas sim o conjunto $\{z \in K : q(z) \neq 0\}$.

Da mesma forma, é possível construir o anel $K[x_1, x_2, \ldots, x_n]$ de todos os polinômios em n variáveis e o corpo $K(x_1, x_2, \ldots, x_n)$ de todas as funções racionais em n variáveis:

$$K[x_1, \ldots, x_n] = \{f(x_1, \ldots, x_n) : f \text{ é um polinômio com coeficientes em } K\};$$

$$K(x_1, \ldots, x_n) = \left\{ \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} : f, g \in K[x_1, \ldots, x_n] \text{ e } g(x_1, \ldots, x_n) \neq 0 \right\}.$$

Definição 2.32. Sejam A e B anéis e considere a função $f : A \to B$. Dizemos que f é um **homomorfismo de anéis** se satisfaz as seguintes condições:

(a) $f(a + b) = f(a) + f(b)$, $\forall\, a, b \in A$;

(b) $f(ab) = f(a)f(b)$, $\forall\, a, b \in A$;

(c) $f(1) = 1$.

Se A e B são corpos e $f : A \to B$ é um homomorfismo de anéis, então f é um **homomorfismo de corpos**. Se f é um homomorfismo bijetivo, então dizemos que f é um **isomorfismo**. Neste caso, dizemos que A e B são isomorfos e denotamos $A \cong B$.

Definição 2.33. Seja $f : A \to B$ um homomorfismo de anéis. O conjunto

$$\ker(f) = \{a \in A : f(a) = 0\}$$

é chamado de **núcleo** de f, e o conjunto

$$\mathrm{Im}(f) = \{f(a) \in B : a \in A\}$$

é chamado de **imagem** de f.

Um fato que pode ser verificado é que se f é um homomorfismo de anéis, então $\ker(f) = \{0\}$ se, e somente se, f é injetora.

Vamos definir agora o que é um ideal, objeto muito importante no estudo de anéis. Depois disso, poderemos definir anel quociente e demonstrar o teorema do isomorfismo para anéis.

Definição 2.34. Um **ideal** de um anel A é um subconjunto $I \subseteq A$ que satisfaz as seguintes propriedades:

(a) I é um subgrupo de A em relação à adição;

(b) Para todo $a \in A$ e todo $b \in I$, $a \cdot b \in I$.

Definição 2.35. Seja S um subconjunto do anel A. O **ideal gerado** por S é o menor ideal de A que contém S e é denotado $\langle S \rangle$.

Definição 2.36. Seja I um ideal próprio de um anel A. Dizemos que I é um **ideal maximal** de A se para todo ideal J de A tal que $I \subseteq J \subseteq A$, temos $J = I$ ou $J = A$.

A seguir, listamos alguns exemplos de ideais.

Exemplos 2.37.

1. Se $f : A \to B$ é um homomorfismo de anéis, então $\ker(f)$ é um ideal de A.
2. O conjunto $n\mathbb{Z} = \{\ldots, -2n, -1n, 0n, 1n, 2n, \ldots\}$ para qualquer $n \in \mathbb{N}$ é um ideal do anel $\mathbb{Z}$.
3. Seja $p(x) = x^2 + 1$. O ideal $\langle p \rangle$ é ideal maximal de $\mathbb{R}[x]$.

Com o conceito de ideal, agora podemos definir anel quociente.

Definição 2.38. Sejam A um anel, I um ideal de A e $a \in A$. A **classe de equivalência** do elemento $a \in A$ é o subconjunto $\overline{a} = a + I = \{a + m : m \in I\}$. O conjunto de todas as classes de equivalência de I em A é denotado por A/I.

Proposição 2.39. *Sejam A um anel, I um ideal de A e $b \in A$. Dizemos que $a \in \overline{b}$ se, e somente se, $a - b \in I$, o que acontece se, e só se, $\overline{a} = \overline{b}$. Logo, classes de equivalência distintas são disjuntas.*

Demonstração.

Note que:

$$a \in \overline{b} \Leftrightarrow a = b + m \text{ para algum } m \in I \Leftrightarrow a - b \in I \Leftrightarrow -(a - b) \in I \Leftrightarrow b \in \overline{a}.$$

Se $a = b + m$ para algum $m \in I$, então $\overline{a} = \overline{b + m} = \overline{b} + \overline{m} = \overline{b} + \overline{0} = \overline{b}$. □

Definição 2.40. Seja I um ideal do anel A. O **anel quociente** A/I é o conjunto das classes de equivalência $\overline{a}$ de I em A munido com as operações

$$\overline{a} + \overline{b} = \overline{a + b},$$

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Definição 2.41. Seja I um ideal próprio de um anel A. Dizemos que I é um **ideal primo** de A se A/I é domínio de integridade.

A demonstração do teorema seguinte pode ser encontrada em [7], Capítulo III, Teorema 3.

Teorema 2.42. *Sejam A um anel e I um ideal de A. Então I é ideal maximal de A se, e somente se, A/I é corpo.*

Com esse teorema, pode-se concluir que todo ideal maximal é um ideal primo. Outro fato que decorre do teorema anterior é que se K é um corpo e $p(x) \in K[x]$, então $p(x)$ é irredutível em K se, e somente se, $K[x]/\langle p(x)\rangle$ é um corpo.

Teorema 2.43 (Teorema do isomorfismo de anéis)**.** *Seja $f : A \to B$ um homomorfismo de anéis. Então $A/\ker(f) \cong \mathrm{Im}(f)$.*

Demonstração.

Seja $K = \ker(f)$ e defina a aplicação $\varphi : A/K \to \mathrm{Im}(f)$ dada por $\varphi(\overline{a}) = f(a)$.
Suponha que $\overline{a} = \overline{b}$. Então $a - b \in K$ e, portanto,

$$f(a-b) = 0 \Leftrightarrow f(a) - f(b) = 0 \Leftrightarrow f(a) = f(b),$$

o que mostra que φ está bem definida.

Perceba também que, dados $a, b \in A$ quaisquer, temos

$$\varphi(\overline{a+b}) = f(a+b) = f(a) + f(b) = \varphi(\overline{a}) + \varphi(\overline{b}),$$

$$\varphi(\overline{ab}) = f(ab) = f(a)f(b) = \varphi(\overline{a})\varphi(\overline{b}),$$

o que mostra que φ é um homomorfismo.

A aplicação φ é sobrejetiva por definição, e é injetiva pois, dados $a, b \in A$ tais que $\varphi(\overline{a}) = \varphi(\overline{b})$, temos

$$\varphi(\overline{a}) = \varphi(\overline{b}) \Rightarrow f(a) = f(b) \Rightarrow f(a-b) = 0 \Rightarrow a - b \in K \Rightarrow \overline{a} = \overline{b}.$$

Logo, φ é um isomorfismo de anéis e concluímos que $A/\ker(f) \cong \mathrm{Im}(f)$. □

2.3 Critérios de irredutibilidade de polinômios

Verificar se um polinômio é irredutível sobre um corpo é, em geral, uma tarefa difícil. Nesta seção iremos enunciar, sem demonstração, alguns critérios que verificam se um polinômio é irredutível sobre o corpo dos racionais $\mathbb{Q}$ e que serão úteis no desenvolvimento do trabalho. As demonstrações podem ser encontradas em [7], Capítulo IV, Seção 6.

Lema 2.44 (Lema de Gauss)**.** *Seja $f \in \mathbb{Z}[x]$ tal que f é irredutível sobre $\mathbb{Z}$. Então f é irredutível sobre $\mathbb{Q}$.*

Teorema 2.45 (Critério de Eisenstein)**.** *Seja $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$. O critério de Eisenstein diz que se existe um primo $p \in \mathbb{Z}$ tal que $p \mid a_0, \ldots, p \mid a_{n-1}, p \nmid a_n$ e $p^2 \nmid a_0$, então, $f(x)$ é irredutível sobre $\mathbb{Q}$.*

Proposição 2.46. *Sejam K um corpo, $a \in K$ e $f(x) \in K[x]$. Então $f(x)$ é irredutível sobre K se, e somente se, $f(x+a)$ é irredutível sobre K.*

Teorema 2.47. *Seja $f \in \mathbb{Z}[x]$ um polinômio não constante. Seja p um número primo tal que $\overline{f}$ também tenha grau n em $\mathbb{Z}_p[x]$. Se $\overline{f}$ é irredutível em $\mathbb{Z}_p[x]$, então f não se escreve como produto de polinômios não constantes em $\mathbb{Z}[x]$. Em particular, f é irredutível sobre $\mathbb{Q}$.*

Vamos ver alguns exemplos.

Exemplos 2.48.

1. O polinômio $f(x) = x^7 + 7x^3 - 14x + 14$ é irredutível sobre $\mathbb{Q}$.

   Solução.

   Pelo Teorema 2.45 (Critério de Eisenstein), tomando $p = 7$, temos $7 \nmid 1$, $7 \mid 7$, $7 \mid -14$, $7 \mid 14$ e $7^2 = 49 \nmid 14$. Logo, $f(x)$ é irredutível sobre $\mathbb{Q}$. □

2. O polinômio $g(x) = x^3 + 3x + 9$ é irredutível sobre $\mathbb{Q}$.

   Solução.

   Pelo Teorema 2.47 (critério redução módulo 2), temos $\overline{g}(x) = x^3 + x + \overline{1} \in \mathbb{Z}_2[x]$. Perceba que $\overline{g}(\overline{0}) = \overline{1}$ e $\overline{g}(\overline{1}) = \overline{1}$. Logo, $f(x)$ é irredutível sobre $\mathbb{Q}$. □

3. O polinômio $h(x) = x^4 + x^3 + x^2 + x + 1$ é irredutível sobre $\mathbb{Q}$.

   Solução.

   Temos $h(x+1) = x^4 + 5x^3 + 10x^2 + 10x + 5$. Pelo Teorema 2.45 (Critério de Eisenstein), tomando $p = 5$, temos $5 \nmid 1$, $5 \mid 5$, $5 \mid 10$ e $5^2 = 25 \nmid 5$. Logo, $h(x+1)$ é irredutível sobre $\mathbb{Q}$. Pela Proposição 2.46 segue que $h(x)$ é irredutível sobre $\mathbb{Q}$. □

Capítulo 3

Teoria de Galois

Neste capítulo, estudaremos os conceitos básicos da Teoria de Galois. A Teoria de Galois tem como propósito conectar a teoria de corpos e a teoria de grupos para facilitar o entendimento de uma dada extensão de corpos. Esta conexão ocorre através do Teorema Fundamental de Galois. Introduziremos todos os conceitos necessários para demonstração deste teorema e mostraremos algumas aplicações através de exemplos.

É interessante notar que os elementos de extensões foram definidos por Galois e Abel na primeira metade do século XIX, mas nessa época ainda não havia sido definido corpo. O conceito de corpo só apareceu com o trabalho de Dedekind entre 1857 e 1871, e a definição formal de corpo só foi dada 20 anos depois por Weber e Moore. Nesta época, a linguagem da álgebra linear não existia como conhecemos hoje e por isso os resultados eram formulados de forma completamente diferente.

3.1 Extensões de corpos

Definição 3.1. Seja L um corpo e $K \subseteq L$ um subcorpo de L. Dizemos que L é uma **extensão de corpo** de K e denotamos essa extensão de corpo como $L : K$.

Definição 3.2. Seja $L : K$ uma extensão de corpos. Um elemento $\alpha \in L$ é dito **algébrico** sobre K se existe um polinômio não nulo $f \in K[x]$ tal que $f(\alpha) = 0$. Se tal polinômio não existe, então α é dito **transcendente** sobre K.

Exemplos 3.3.

1. O número $\sqrt{2}$ é algébrico sobre $\mathbb{Q}$.

   Solução.

   Seja $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Note que $\sqrt{2}$ é raiz de $f(x) = 0$. Logo, $\sqrt{2}$ é algébrico sobre $\mathbb{Q}$. □

2. O número $\sqrt[5]{\pi}$ é algébrico sobre $\mathbb{Q}(\pi)$.

   Solução.

   Seja $g(x) = x^5 - \pi \in \mathbb{Q}(\pi)[x]$. Note que $\sqrt[5]{\pi}$ é raiz de $g(x) = 0$. Logo, $\sqrt[5]{\pi}$ é algébrico sobre $\mathbb{Q}(\pi)$. □

3. O número i é algébrico sobre $\mathbb{Q}$.

   Solução.

   Seja $h(x) = x^2 + 1 \in \mathbb{Q}[x]$. Note que i é raiz de $g(x) = 0$. Logo, i é algébrico sobre $\mathbb{Q}$. □

4. O número π é transcendente sobre $\mathbb{Q}$.

   Solução.

   Suponha que π é algébrico sobre $\mathbb{Q}$. Como i é algébrico sobre $\mathbb{Q}$ e o conjunto dos números algébricos é um corpo, então o produto $i\pi$ é também algébrico sobre $\mathbb{Q}$. Pelo Teorema de Hermite-Lindemann-Weierstrass[1], $e^{i\pi}$ é transcendente sobre $\mathbb{Q}$. Mas $e^{i\pi} = -1$ é zero do polinômio $h(z) = z + 1$. Portanto, $e^{i\pi}$ é algébrico sobre $\mathbb{Q}$, o que é uma contradição. Logo, π é transcendente sobre $\mathbb{Q}$. □

Definição 3.4. Seja $L : K$ uma extensão de corpos. Se $\alpha \in L$ é algébrico sobre K, então o único polinômio mônico $f \in K[x]$ de menor grau para o qual $f(\alpha) = 0$ é dito **polinômio minimal** de α sobre K.

Observação 3. Ao longo deste trabalho, se f é um polinômio, denotaremos o grau de f como $\partial(f)$.

Proposição 3.5. *Seja $L : K$ uma extensão de corpos. Seja $\alpha \in L$ algébrico sobre K.*

(a) O polinômio minimal de α sobre K é irredutível e divide todo polinômio $q \in K[x]$ tal que $q(\alpha) = 0$.

(b) Se $f \in K[x]$ é um polinômio mônico irredutível tal que $f(\alpha) = 0$, então f é o polinômio minimal de α sobre K.

Demonstração.

(a) Seja p o polinômio minimal de α sobre K. Se $p = fg$, onde $\partial f < \partial g$ e $\partial g < \partial p$, então $p(\alpha) = 0$ implica que $f(\alpha) = 0$ ou $g(\alpha) = 0$, o que contradiz o fato de p ser o polinômio de menor grau que possui α como zero.

[1] O Teorema de Hermite-Lindemann-Weierstrass afirma que se $z \in \mathbb{C}$ é um número algébrico não nulo, então e^z é transcendente sobre $\mathbb{Q}$.

(b) Seja $q \in K[x]$ tal que $q(\alpha) = 0$. Se dividirmos q por p, temos $q(x) = d(x)p(x)+r(x)$, onde $r(x) = 0$ ou $\partial\, r < \partial\, p$.

Para $x = \alpha$: $q(\alpha) = d(\alpha)p(\alpha) + r(\alpha) \Rightarrow r(\alpha) = 0$.

Como p é minimal, então não podemos ter $\partial\, r < \partial\, p$. Logo $r(x) = 0$ e portanto p divide q.

□

Exemplos 3.6. Dado $\alpha \in L \supseteq K$, sabemos que $K[\alpha] = \{f(\alpha) : f(x) \in K[x]\}$. Utilizando este fato, vamos provar as igualdades abaixo.

1. $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

   Solução.

   Por definição, $\mathbb{Q}[\sqrt{2}] = \{f(\sqrt{2}) : f(x) \in \mathbb{Q}[x]\}$. Se $f(x) \in \mathbb{Q}[x]$, segue pelo algoritmo da divisão que existem $q(x), r(x) \in \mathbb{Q}[x]$ tais que $f(x) = q(x)(x^2 - 2) + r(x)$, onde $r(x) = a + bx$. Portanto,

   $$f(\sqrt{2}) = q(\sqrt{2})[(\sqrt{2})^2 - 2] + r(\sqrt{2}) = r(\sqrt{2}) = a + b\sqrt{2},\ a, b \in \mathbb{Q}.$$

   □

2. $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 : a, b, c \in \mathbb{Q}\}$.

   Solução.

   Por definição, $\mathbb{Q}[\sqrt[3]{2}] = \{f(\sqrt[3]{2}) : f(x) \in \mathbb{Q}[x]\}$. Se $f(x) \in \mathbb{Q}[x]$, segue pelo algoritmo da divisão que existem $q(x), r(x) \in \mathbb{Q}[x]$ tais que $f(x) = q(x)(x^3 - 2) + r(x)$, onde $r(x) = a + bx + cx^2$. Portanto,

   $$f(\sqrt[3]{2}) = q(\sqrt[3]{2})[(\sqrt[3]{2})^3 - 2] + r(\sqrt[3]{2}) = r(\sqrt[3]{2}) = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2,\ a, b, c \in \mathbb{Q}.$$

   □

Definição 3.7. Sejam $L : K$ uma extensão de corpos e $a_1, \ldots, a_n \in L$. Então $K(a_1, \ldots, a_n)$ é o menor subcorpo de L que contém K e os elementos $a_1, \ldots, a_n$.

Proposição 3.8. *Seja $L : K$ uma extensão de corpos. Se $\alpha \in L$ é algébrico sobre K, então $K(\alpha) = K[\alpha]$.*

Demonstração.

Claramente $K[\alpha] \subseteq K(\alpha)$. Basta então provar que $K(\alpha) \subseteq K[\alpha]$. Como $\alpha \in L$ é

algébrico sobre K, então existe um polinômio irredutível não nulo $f(x) = \sum_{k=0}^{n} a_k x^k \in K[x]$ tal que $f(\alpha) = a_0 + \sum_{k=1}^{n} a_k \alpha^k = 0$. Como f é irredutível, então $a_0 \neq 0$. Temos:

$$a_0 = -\alpha \sum_{k=1}^{n} a_k \alpha^{k-1}.$$

Multiplicando ambos os lados por $\frac{1}{a_0} \in K$, temos:

$$-\frac{\alpha}{a_0} \sum_{k=1}^{n} a_k \alpha^{k-1} = 1$$

$$\Rightarrow -\frac{1}{a_0} \sum_{k=1}^{n} a_k \alpha^{k-1} = \alpha^{-1} \in K[\alpha].$$

Então, $K(\alpha) \subseteq K[\alpha]$ e portanto, $K(\alpha) = K[\alpha]$. □

Proposição 3.9. *Se $L : K$ é uma extensão de corpos e $\alpha, \beta \in L$, então $K(\alpha, \beta) = K(\alpha)(\beta)$.*

Demonstração.

Note que $K(\alpha) \subseteq K(\alpha)(\beta)$. Então, $K \subseteq K(\alpha)(\beta)$ e $\alpha \in K(\alpha)(\beta)$. Claramente também temos $\beta \in K(\alpha)(\beta)$. Logo, $K(\alpha, \beta) \subseteq K(\alpha)(\beta)$.

Por outro lado, $K \subseteq K(\alpha, \beta)$ e $\alpha \in K(\alpha, \beta)$, o que implica que $K(\alpha) \subseteq K(\alpha, \beta)$. Mas $\beta \in K(\alpha, \beta)$. Logo, $K(\alpha)(\beta) \subseteq K(\alpha, \beta)$.

Portanto, $K(\alpha, \beta) = K(\alpha)(\beta)$. □

É possível generalizar a proposição acima para mais variáveis. Por exemplo, $K(\alpha, \beta, \gamma) = K(\gamma)(\alpha, \beta)$, $K(\alpha, \beta, \gamma, \delta) = K(\delta)(\alpha, \beta, \gamma)$, $K(\alpha, \beta, \gamma, \delta) = K(\delta, \gamma)(\alpha, \beta)$, e assim por diante.

Exemplo 3.10. Seja $L : K$ é uma extensão de corpos. Dado $\alpha \in L$ algébrico sobre K, sabemos, pela Proposição 3.8 que $K(\alpha) = K[\alpha] = \{f(\alpha) : f(x) \in K[x]\}$. Utilizando este fato, vamos provar que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$.

Solução.

Sabemos, pela Proposição 3.9, que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \{f(\sqrt{3}) : f(x) \in \mathbb{Q}(\sqrt{2})[x]\}$.

Se $f(x) \in \mathbb{Q}(\sqrt{2})[x]$, então existem $q(x), r(x) \in \mathbb{Q}(\sqrt{2})[x]$ tais que $f(x) = q(x)(x^2 - 3) + r(x)$, onde $r(x) = m + nx$. Então,

$$f(\sqrt{3}) = r(\sqrt{3}) = m + n\sqrt{3},\ m, n \in \mathbb{Q}(\sqrt{2})[x].$$

Como $m, n \in \mathbb{Q}(\sqrt{2})$, temos: $m = a + b\sqrt{2}$ e $n = c + d\sqrt{2}$.

Portanto, $f(\sqrt{3}) = r(\sqrt{3}) = m + n\sqrt{3} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6},\ a, b, c, d \in \mathbb{Q}$. □

Definição 3.11. Uma extensão de corpos $L : K$ é dita **extensão simples** se $L = K(\alpha)$ para algum $\alpha \in L$.

Exemplos 3.12.

1. A extensão $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ é simples.

   Solução.

   É evidente. Basta notar que $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. □

2. A extensão $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$ é simples.

   Solução.

   Basta verificar que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

   Como $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, então $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, visto que $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ é corpo. Logo, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

   Por outro lado, note que

   $$(\sqrt{2} + \sqrt{3})^{-1} = \frac{1}{\sqrt{2} + \sqrt{3}} \cdot \frac{\sqrt{2} - \sqrt{3}}{\sqrt{2} - \sqrt{3}} = \frac{\sqrt{2} - \sqrt{3}}{2 - 3} = \sqrt{3} - \sqrt{2}.$$

   Como $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ é corpo, então $\sqrt{3} - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Logo

   $$\sqrt{2} + \sqrt{3} + \sqrt{3} - \sqrt{2} = 2\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

   e, portanto, $\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Da mesma forma

   $$\sqrt{2} + \sqrt{3} - (\sqrt{3} - \sqrt{2}) = 2\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

   e, portanto, $\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Disto temos $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

   Logo, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. □

Proposição 3.13. *Seja $L : K$ uma extensão de corpos. Então as operações*

$$(u, v) \mapsto u + v; \quad u, v \in L$$

$$(\lambda, u) \mapsto \lambda \cdot u; \quad u \in L, \ \lambda \in K$$

definem em L uma estrutura de espaço vetorial sobre K.

Demonstração.

Como L é corpo, então $(L, +)$ é um grupo abeliano, e portanto satisfaz os axiomas da adição para ser um espaço vetorial sobre K. A associatividade e a distributividade claramente valem para a multiplicação por escalar em L. Como $K \subseteq L$, a associatividade e a distributividade também valem para a multiplicação por escalar de elementos de K, o que conclui a prova que L é um espaço vetorial sobre K. □

Definição 3.14. Seja $L : K$ uma extensão de corpos. Denotamos $[L : K]$ o **grau da extensão**, que é a dimensão de L visto como espaço vetorial sobre K. Se $[L : K]$ é finito, dizemos que $L : K$ é uma **extensão finita**. Se $[L : K]$ não é finito, denotamos $[L : K] = \infty$ e dizemos que $L : K$ é uma **extensão infinita**.

Teorema 3.15 (Teorema da extensão simples)**.** *Seja $L : K$ uma extensão de corpos.*

(a) Se $\alpha \in L$ é algébrico sobre K, então cada elemento em $K(\alpha)$ pode ser representado de forma única como $\sum_{j=0}^{n-1} a_j \alpha^j$, onde $a_j \in K$ e n é o grau do polinômio minimal de α sobre K. Então $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é base de $K(\alpha)$ sobre K e $[K(\alpha) : K] = n$.

(b) Se $\alpha \in L$ é transcendente sobre K, então $K[\alpha] \cong K[x]$.

Demonstração.

(a) Seja $p(x) = \sum_{j=0}^{n} b_j x^j \in K[x]$ o polinômio minimal de α sobre K. Sabemos que $K(\alpha) = K[\alpha] = \{f(\alpha) : f(x) \in K[x]\}$. Se $f(x) \in K[x]$, segue pelo algoritmo da divisão que existem $q(x), r(x) \in K[x]$ tais que $f(x) = q(x)p(x) + r(x)$, onde $r(x) = \sum_{j=0}^{n-1} a_j x^j$. Portanto,

$$f(\alpha) = q(\alpha)p(\alpha) + r(\alpha) = r(\alpha) = \sum_{j=0}^{n-1} a_j \alpha^j.$$

Logo, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ gera $K(\alpha)$.

Vamos agora mostrar que $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é linearmente independente. Suponha, por absurdo, que é linearmente dependente. Então existe $a_j \neq 0$ tal que $r(\alpha) = \sum_{j=0}^{n-1} a_j \alpha^j = 0$. Logo r anula α e $\partial(r) < \partial(p)$. Mas p é o polinômio minimal de α sobre K. Contradição! Portanto $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é linearmente independente.

Então $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é base de $K(\alpha)$ sobre K e $[K(\alpha) : K] = n$.

(b) Defina o homomorfismo de anéis sobrejetor $\varphi : K[x] \to K[\alpha]$, $\varphi(f(x)) = f(\alpha)$. Se $\alpha \in L$ é transcendente sobre K, então $\ker(\varphi) = \{0\}$ e portanto φ é injetor. Logo, φ é um isomorfismo de anéis e segue que $K[x] \cong K[\alpha]$.

□

Teorema 3.16 (Lei da torre)**.** *Sejam $M : L$ e $L : K$ extensões de corpos finitas. Então a extensão de corpos $M : K$ é finita e*

$$[M : K] = [M : L] \cdot [L : K].$$

Demonstração.

Seja $\{e_i\}_{i=1,\ldots,l}$ base de L sobre K e $\{f_j\}_{j=1,\ldots,m}$ base de M sobre L. Se $x \in M$, então $x = \sum_{j=1}^{m} b_j f_j$, onde $b_j \in L$. Para cada j, temos $b_j = \sum_{i=1}^{l} a_{ij} e_i$, onde $a_{ij} \in K$. Então $x = \sum_{j=1}^{m} b_j f_j = \sum_{j=1}^{m} \sum_{i=1}^{l} a_{ij}(e_i f_j)$. Logo, $\{e_i f_j\}$ é conjunto gerador de M sobre K. Vamos agora mostrar que $\{e_i f_j\}$ é linearmente independente. Se $\sum_{j=1}^{m} \sum_{i=1}^{l} a_{ij}(e_i f_j) = 0$, onde $a_{ij} \in K$, então:

$$\left(\sum_{i=1}^{l} a_{i1} e_i\right) f_1 + \cdots + \left(\sum_{i=1}^{l} a_{im} e_i\right) f_m = 0.$$

Como os e_i's estão em L segue, pela independência linear dos f_j's em M sobre L, que $\sum_{i=1}^{l} a_{ij} e_i, 1 \leq j \leq m$.

Como os a_{ij}'s estão em K, segue pela independência linear dos e_i's em L sobre K que $a_{ij} = 0, 1 \leq i \leq l, 1 \leq j \leq m$. Logo, $\{e_i f_j\}$ é linearmente independente.

Portanto, $\{e_i f_j\}$ é base de M sobre K com lm elementos e temos

$$\underbrace{[M : K]}_{l \cdot m} = \underbrace{[M : L]}_{m} \cdot \underbrace{[L : K]}_{l}.$$

□

Definição 3.17. Seja $L : K$ uma extensão de corpos. Dizemos que $L : K$ é **finitamente gerada** se existem elementos $\alpha_1, \alpha_2, \ldots, \alpha_k \in L$ tais que $L = K(\alpha_1, \alpha_2, \ldots, \alpha_k)$.

Definição 3.18. Seja $L : K$ uma extensão de corpos. Dizemos que $L : K$ é uma **extensão algébrica** se todo elemento de L é algébrico sobre K.

Definição 3.19. Seja $L : K$ uma extensão de corpos. O corpo de todos os elementos algébricos de L sobre K é chamado de **fecho algébrico** de K em L.

Extensões algébricas não precisam ser finitas, mas toda extensão finita é algébrica. De maneira mais geral, vale a seguinte proposição:

Proposição 3.20. *Uma extensão de corpos $L : K$ é finita se, e somente se, é algébrica e finitamente gerada.*

Demonstração.

($\Rightarrow$) Seja $L : K$ uma extensão de corpos finita de grau n. Então existe uma base

$\{e_1, \ldots, e_n\}$ de L sobre K, e temos $L = K(e_1, \ldots, e_n)$, ou seja, L é finitamente gerada sobre K. Se $x \in L$, então $1, x, x^2, \ldots, x^n \in L$. O conjunto $\{1, x, x^2, \ldots, x^n\}$ é linearmente dependente sobre K, pois o conjunto possui $n+1$ elementos. Portanto, $\sum_{j=0}^{n} a_j x^j = 0$ implica que nem todo a_j é nulo. Isto garante a existência de um polinômio não nulo com coeficientes em K que anulam x. Logo x é algébrico sobre K, o que implica que $L : K$ é uma extensão algébrica.

($\Leftarrow$) Assuma que $L : K$ é algébrica e finitamente gerada, ou seja, $L = K(\alpha_1, \alpha_2, \ldots, \alpha_r)$, onde $K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq K(\alpha_1, \ldots, \alpha_r)$, com $\alpha_1, \alpha_2, \ldots, \alpha_r \in L$ algébricos sobre K. Então para $2 \leq j \leq r$, α_j é algébrico sobre $K(\alpha_1, \ldots, \alpha_{j-1})$. Logo, pelo Teorema 3.15, a extensão $K(\alpha_1, \ldots, \alpha_j) : K(\alpha_1, \ldots, \alpha_{j-1})$ é finita. Pelo Teorema 3.16, segue que $L : K$ é finita, pois

$$[L : K] = [K(\alpha_1) : K] \cdot \prod_{j=2}^{r} [K(\alpha_1, \ldots, \alpha_j) : K(\alpha_1, \ldots, \alpha_{j-1})].$$

□

Exemplos 3.21. Vamos determinar o grau e uma base para as extensões de corpos a seguir.

1. $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$

   Solução.

   Considere o polinômio $f(x) = x^2 - 2$. Note que $f(\sqrt{2}) = 0$ e f é irredutível sobre $\mathbb{Q}$ pelo Teorema 2.45 (Critério de Eisenstein) tomando $p = 2$. Portanto, $\sqrt{2}$ é algébrico sobre $\mathbb{Q}$.

   Então, pelo Teorema 3.15, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \partial(f) = 2$, e $y = a + b\sqrt{2}$, $\forall\, y \in \mathbb{Q}(\sqrt{2})$, onde $a, b \in \mathbb{Q}$. Logo, $\{1, \sqrt{2}\}$ é uma base para a extensão $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$. □

2. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$

   Solução.

   Note que $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Vimos anteriormente que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Seja $f \in \mathbb{Q}(\sqrt{2})[x]$ tal que $f(x) = x^2 - 3$. Note que $f(\sqrt{3}) = 0$. Se $x \in \mathbb{Q}(\sqrt{2})$, temos:

   $$\begin{aligned} & x^2 - 3 = 0 \\ \Rightarrow \quad & x^2 = 3 \\ \Rightarrow \quad & (a + b\sqrt{2})^2 = 3 \\ \Rightarrow \quad & a^2 + 2ab\sqrt{2} + 2b^2 = 3. \end{aligned}$$

Portanto, $a^2 + 2b^2 = 3$ e $2ab = 0$. Se $a = 0$, então $2b^2 = 3$, o que implica que $b \notin \mathbb{Q}$. Se $b = 0$, então $a^2 = 3$, o que implica que $a \notin \mathbb{Q}$. Logo f é irredutível sobre $\mathbb{Q}(\sqrt{2})$. Segue que $\{1, \sqrt{3}\}$ é base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$ e, portanto, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$.

Pelo Teorema 3.16, temos:

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Perceba que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$. Logo, dado $y \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, temos $y = a+b\sqrt{3}$, onde $a, b \in \mathbb{Q}(\sqrt{2})$, visto que $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. Como $a, b \in \mathbb{Q}(\sqrt{2})$, então $a = a_1 + a_2\sqrt{2}$ e $b = b_1 + b_2\sqrt{2}$, onde $a_1, a_2, b_1, b_2 \in \mathbb{Q}$. Portanto, dado $x \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, temos

$$y = a + b\sqrt{3} = a_1 + a_2\sqrt{2} + (b_1 + b_2\sqrt{2})\sqrt{3} = a_1 + a_2\sqrt{2} + b_1\sqrt{3} + b_2\sqrt{6}.$$

Como a dimensão de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ como um espaço vetorial sobre $\mathbb{Q}$ é 4, então $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ é base de $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$. □

3. $\mathbb{Q}(\sqrt{3 + \sqrt{2}}) : \mathbb{Q}$

   Solução.

   Considere o polinômio $f(x) = x^4 - 6x^2 + 7$. Note que $f(\sqrt{3 + \sqrt{2}}) = 0$ e f é irredutível sobre $\mathbb{Q}$ ao aplicar o Teorema 2.45 (Critério de Eisenstein) em $f(x + 1)$ tomando $p = 2$. Portanto, $\sqrt{3 + \sqrt{2}}$ é algébrico sobre $\mathbb{Q}$ e $f(x)$ é o seu polinômio minimal sobre $\mathbb{Q}$.

   Então, pelo Teorema 3.15, $[\mathbb{Q}(\sqrt{3 + \sqrt{2}}) : \mathbb{Q}] = \partial(f) = 4$, e $y = a + b(3 + \sqrt{2})^{\frac{1}{2}} + c(3 + \sqrt{2}) + d(3 + \sqrt{2})^{\frac{3}{2}}$, $\forall\, y \in \mathbb{Q}(\sqrt{3 + \sqrt{2}})$, onde $a, b \in \mathbb{Q}$. Logo, $\{1, (3 + \sqrt{2})^{\frac{1}{2}}, 3 + \sqrt{2}, (3 + \sqrt{2})^{\frac{3}{2}}\}$ é uma base para a extensão $\mathbb{Q}(\sqrt{3 + \sqrt{2}}) : \mathbb{Q}$. □

4. $\mathbb{Q}(\sqrt{8 + 2\sqrt{7}}) : \mathbb{Q}$

   Solução.

   Perceba que $(1 + \sqrt{7})^2 = 1 + 2\sqrt{7} + 7 = 8 + 2\sqrt{7}$, o que implica que $\sqrt{8 + 2\sqrt{7}} = 1 + \sqrt{7}$. Então $\mathbb{Q}(\sqrt{8 + 2\sqrt{7}}) = \mathbb{Q}(1 + \sqrt{7}) = \mathbb{Q}(\sqrt{7})$.

   Considere o polinômio $f(x) = x^2 - 7$. Note que $f(\sqrt{7}) = 0$ e f é irredutível sobre $\mathbb{Q}$ pelo Teorema 2.45 (Critério de Eisenstein) tomando $p = 7$. Portanto, $\sqrt{7}$ é algébrico sobre $\mathbb{Q}$.

   Então, pelo Teorema 3.15, $[\mathbb{Q}(\sqrt{8 + 2\sqrt{7}}) : \mathbb{Q}] = \partial(f) = 2$, e $y = a + b\sqrt{7}$, $\forall\, y \in \mathbb{Q}(\sqrt{8 + 2\sqrt{7}})$, onde $a, b \in \mathbb{Q}$.

   Logo, $\{1, \sqrt{7}\}$ é uma base para a extensão $\mathbb{Q}(\sqrt{8 + 2\sqrt{7}}) : \mathbb{Q}$. □

3.2 Corpos de decomposição

Definição 3.22. Sejam K um corpo e $f \in K[x]$. Então f **cinde** sobre K se f for produto de fatores lineares em K, isto é, $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$, onde $a, \alpha_1, \ldots, \alpha_n \in K$.

Exemplos 3.23.

1. O polinômio $f(x) = x^2 + 1 \in \mathbb{Q}[x]$ cinde sobre $\mathbb{C}$.

   Solução.

   Perceba que f pode ser reescrito como $f(x) = (x-i)(x+i)$. Como $i, -i \in \mathbb{C}$, então f cinde sobre $\mathbb{C}$. □

2. O polinômio $f(x) = x^4 - x^2 - 2 \in \mathbb{Q}[x]$ não cinde sobre $\mathbb{Q}(\sqrt{2})$.

   Solução.

   Perceba que a melhor fatoração de f sobre $\mathbb{Q}(\sqrt{2})$ que podemos escrever é $f(x) = (x-\sqrt{2})(x+\sqrt{2})(x^2+1)$, pois o fator x^2+1 é irredutível sobre $\mathbb{Q}(\sqrt{2})$. Como esta fatoração não é um produto de fatores lineares em $\mathbb{Q}(\sqrt{2})$, então f não cinde sobre $\mathbb{Q}(\sqrt{2})$. □

Definição 3.24. Sejam K um corpo e $f \in K[x]$. Então dizemos que L é **corpo de decomposição** de f sobre K se f cinde sobre L e $L = K(\alpha_1, \ldots, \alpha_n)$, onde $\alpha_1, \ldots, \alpha_n$ são as raízes de f em L.

Proposição 3.25. *Sejam K um corpo e $f \in K[x]$. Então existe uma extensão de corpos $L : K$ tal que L é corpo de decomposição de f sobre K. Quaisquer dois corpos de decomposição de f sobre K são isomorfos.*

A demonstração da proposição acima pode ser encontrada em [1], Capítulo 5, T.5.2.

Exemplos 3.26. Vamos determinar o corpo de decomposição L de $f(x) \in K[x]$ sobre K nos casos a seguir.

1. $f(x) = x^3 - 2$ e $K = \mathbb{Q}$

   Solução.

   Os zeros de f são $\sqrt[3]{2}, \sqrt[3]{2}\,\omega, \sqrt[3]{2}\,\omega^2$, onde $\omega = \cos\left(\frac{2\pi}{3}\right) + i\,\mathrm{sin}\left(\frac{2\pi}{3}\right)$ é uma raiz cúbica da unidade. Perceba que nenhum zero de f pertence ao conjunto $\mathbb{Q}$. Então $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\,\omega, \sqrt[3]{2}\,\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$. □

2. $f(x) = x^2 + 1$ e $K = \mathbb{Q}(i)$

Solução.

Os zeros de f são $i, -i$. Perceba que ambos os zeros de f pertencem ao conjunto $\mathbb{Q}(i)$. Então $L = \mathbb{Q}(i)$. □

3. $f(x) = (x^2 - 2)(x^2 - 7)$ e $K = \mathbb{Q}(i)$

Solução.

Os zeros de f são $\sqrt{2}, -\sqrt{2}, \sqrt{7}, -\sqrt{7}$. Perceba que nenhum zero de f pertence ao conjunto $\mathbb{Q}(i)$. Então $L = \mathbb{Q}(i)(\sqrt{2}, -\sqrt{2}, \sqrt{7}, -\sqrt{7}) = \mathbb{Q}(i, \sqrt{2}, \sqrt{7})$. □

3.3 Extensões normais

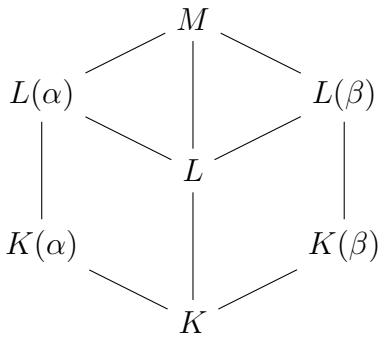
Definição 3.27. Sejam $L : K$ uma extensão de corpos. Dizemos que $L : K$ é uma **extensão normal** se todo polinômio irredutível $f \in K[x]$ que possui uma raiz em L tem todas as raízes em L.

Teorema 3.28. *Uma extensão finita $L : K$ é normal se, e somente se, L é corpo de decomposição de um polinômio $f \in K[x]$.*

Demonstração.

($\Rightarrow$) Seja $L = K(\alpha_1, \ldots, \alpha_n)$ e seja f_i o polinômio minimal de α_i sobre K para $\forall\, i \in \{1, 2, \ldots, n\}$. Pela definição de extensão normal, todo polinômio f_i tem todas as raízes em L. O mesmo vale para o produto $f = f_1 \cdots f_n$, o que implica que L é corpo de decomposição de f sobre K, visto que contém todas as raízes de f e $L = K(\alpha_1, \ldots, \alpha_n)$.

($\Leftarrow$) Suponha que L é corpo de decomposição de um polinômio $f \in K[x]$. Seja $g \in K[x]$ um polinômio irredutível que possui uma raiz em L. Queremos mostrar que g tem todas as raízes em L. Seja M o corpo de decomposição de g sobre L e seja $\beta \in M$ tal que $g(\beta) = 0$. Vamos mostrar que $\beta \in L$. Considere a seguinte cadeia de extensões de corpos:



Como L é corpo de decomposição de f sobre K, então ambos $L(\alpha)$ e $L(\beta)$ são corpos de decomposição de f sobre $K(\alpha)$ e $K(\beta)$, respectivamente. Pela Proposição 3.25, como $K(\alpha) \cong K(\beta)$, existe um isomorfismo dos corpos de decomposição $L(\alpha)$ e $L(\beta)$ de f estendendo um isomorfismo de $K(\alpha)$ e $K(\beta)$. Então $[L(\alpha) : K(\alpha)] = [L(\beta) : K(\beta)]$ e $[K(\alpha) : K] = [K(\beta) : K]$. Então:

$$\begin{aligned}[L(\alpha) : L] &= \frac{[L(\alpha) : K]}{[L : K]} = \frac{[L(\alpha) : K(\alpha)][K(\alpha) : K]}{[L : K]} \\ &= \frac{[L(\beta) : K(\beta)][K(\beta) : K]}{[L : K]} = \frac{[L(\beta) : K]}{[L : K]} = [L(\beta) : L].\end{aligned}$$

Mas $[L(\alpha) : L] = 1$, pois $\alpha \in L$ e, portanto, $[L(\beta) : L] = 1$, o que implica que $L(\beta) = L$, ou seja, $\beta \in L$. Isto prova que $L : K$ é normal. □

Exemplos 3.29. Vamos verificar se as extensões de corpos a seguir são normais.

1. $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$

   Solução.

   Considere o polinômio $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Note que $\mathbb{Q}(\sqrt{2})$ é corpo de decomposição de f. Pelo Teorema 3.28, segue que $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ é uma extensão normal. □

2. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$

   Solução.

   Considere o polinômio $f(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$. Note que $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ é corpo de decomposição de f. Pelo Teorema 3.28, segue que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$ é uma extensão normal. □

3. $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$

   Solução.

   Considere o polinômio $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. Note que f é irredutível sobre $\mathbb{Q}$ pelo Teorema 2.45 (Critério de Eisenstein) tomando $p = 2$. As raízes de $f(x) = 0$ são $\sqrt[4]{2}, \sqrt[4]{2}\, i, -\sqrt[4]{2}, -\sqrt[4]{2}\, i$. Suponha que $\sqrt[4]{2}\, i \in \mathbb{Q}(\sqrt[4]{2})$. Como $\mathbb{Q}(\sqrt[4]{2})$ é corpo, então sabemos que $(\sqrt[4]{2})^{-1} = \frac{1}{\sqrt[4]{2}} \in \mathbb{Q}(\sqrt[4]{2})$, implicando que $(\sqrt[4]{2})^{-1} \cdot \sqrt[4]{2} \cdot i = i \in \mathbb{Q}(\sqrt[4]{2})$. Contradição, pois $i \notin \mathbb{R} \supseteq \mathbb{Q}(\sqrt[4]{2})$. Disto segue que $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ não é uma extensão normal. □

3.4 Separabilidade

Definição 3.30. Sejam $L : K$ uma extensão de corpos e $f \in K[x]$ um polinômio irredutível sobre K. Dizemos que f é **separável** sobre K se todas suas raízes forem distintas. Dizemos que $\alpha \in L$ é um **elemento separável** sobre K se α é algébrico e o polinômio minimal de α sobre K é separável sobre K. Dizemos que $L : K$ é uma **extensão separável** se todo elemento de L é separável sobre K.

Exemplos 3.31. Vamos verificar se os polinômios irredutíveis $f \in K[x]$ a seguir são separáveis sobre K.

1. $f(x) = x^2 + x + 1$, $K = \mathbb{Q}$

   Solução.

   As raízes de $f(x) = 0$ são ω, ω^2, onde $\omega = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right)$.

   Logo, as raízes são distintas o que implica que f é separável sobre K. □

2. $f(x) = x^3 - t$, $K = \mathbb{Z}_3(t)$

   Solução.

   Perceba que nesse exemplo, K possui característica 3. Note que:

   $$f(x) = x^3 - t = x^3 - 3x^2\sqrt[3]{t} + 3x(\sqrt[3]{t})^2 - t = (x - \sqrt[3]{t})^3.$$

   Portanto, $\sqrt[3]{t}$ é raiz de multiplicidade 3 de $f(x) = 0$, o que mostra que f é inseparável sobre K. □

A próxima proposição é um critério simples para verificar se um polinômio possui raízes múltiplas.

Definição 3.32. A **derivada** do polinômio

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$$

é definida como

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

Proposição 3.33. *Sejam K um corpo e $f, g \in K[x]$. Então $(f+g)' = f' + g'$ e $(fg)' = f'g + fg'$.*

Proposição 3.34. *Seja $L : K$ uma extensão de corpos. Um polinômio $f \in K[x]$ não possui raízes múltiplas em L se, e somente se,* $\text{mdc}(f, f') = 1$.

Demonstração.

($\Rightarrow$) Sejam $d = \text{mdc}(f, f')$ um polinômio não constante e α um elemento de algum corpo M que contém K. Considere que $d(\alpha) = 0$. Então $f(\alpha) = f'(\alpha) = 0$. Logo, $f(x) = (x - \alpha)q(x)$ com $q \in M[x]$. Portanto, $f'(x) = q(x) + (x - \alpha)q'(x)$. Mas como $f'(\alpha) = 0$, então $q(\alpha) = 0$. Logo, $q(x) = (x-\alpha)r(x)$ com $r \in M[x]$ e $f(x) = (x-\alpha)^2 r(x)$, isto é, f possui raízes múltiplas.

($\Leftarrow$) Seja $\alpha \in L$ uma raiz de multiplicidade $m \geq 2$ de f, isto é, $f(x) = (x-\alpha)^m q(x)$ com $q \in L[x]$. Então, $f'(x) = m(x-\alpha)^{m-1}q(x)+(x-\alpha)^m q'(x)$, o que implica $f(\alpha) = f'(\alpha) = 0$. Logo, $\text{mdc}(f, f') \neq 1$, visto que $x - \alpha$ é divisor comum de f e f'. □

A demonstração do teorema seguinte pode ser encontrada em [1], Capítulo 8, T.8.2.

Teorema 3.35 (Teorema do Elemento Primitivo)**.** *Se $L : K$ é uma extensão de corpos finita e separável, então existe $\alpha \in L$ tal que $L = K(\alpha)$.*

3.5 Grupos de Galois

Alguns resultados desta seção serão apenas enunciados. As demonstrações podem ser encontradas em [1], Capítulos 6 e 9.

Definição 3.36. Seja L um corpo e considere a função $\sigma : L \to L$. Dizemos que σ é um **automorfismo** se satisfaz as seguintes condições:

(a) $\sigma(a + b) = \sigma(a) + \sigma(b)$, $\forall\, a, b \in L$;

(b) $\sigma(ab) = \sigma(a)\sigma(b)$, $\forall\, a, b \in L$;

(c) σ é bijetiva.

Se $L : K$ é uma extensão de corpos e $\sigma : L \to L$ é um automorfismo, então σ é dito um **K-automorfismo** se

(d) $\sigma(k) = k$, $\forall\, k \in K$.

Note que se σ é um automorfismo de corpos, então $\sigma(0) = \sigma(0 + 0) = \sigma(0) + \sigma(0) = 2\sigma(0)$, o que implica que $\sigma(0) = 0$. Note também que $\sigma(1) = \sigma(1 \cdot 1) = \sigma(1) \cdot \sigma(1)$, o que implica que $\sigma(1) = 1$, visto que σ é bijetiva. Se $L : K$ é uma extensão de corpos, então o conjunto G de todos os K-automorfismos de L forma um grupo com a operação composição. Este grupo tem um nome, conforme veremos na definição a seguir.

Definição 3.37. O **grupo de Galois** de uma extensão de corpos $L : K$ é o grupo de todos os K-automorfismos de L sob a operação de composição, e é denotado por $\text{Gal}(L : K)$.

Proposição 3.38. *Seja $f \in K[x]$ um polinômio irredutível sobre K. Se L é corpo de decomposição de f sobre K, então todo K-automorfismo $\sigma : L \to L$ permuta as raízes de $f(x) = 0$.*

Demonstração.

Seja $\alpha \in L$ tal que $f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i = 0$, e considere $\sigma : L \to L$ um K-automorfismo qualquer. Então:

$$f(\sigma(\alpha)) = \sum_{i=0}^{n} a_i \sigma(\alpha)^i = \sum_{i=0}^{n} \sigma(a_i)\sigma(\alpha^i) = \sigma\left(\sum_{i=0}^{n} a_i \alpha^i\right) = \sigma(f(\alpha)) = \sigma(0) = 0.$$

Isto conclui que $\sigma(\alpha)$ também é raiz de $f(x) = 0$. □

Definição 3.39. Sejam L um corpo e G um grupo de automorfismos de L. Definimos o conjunto L^G como

$$L^G = \{x \in L : \sigma(x) = x, \forall\, \sigma \in G\}.$$

Teorema 3.40 (Teorema de Artin)**.** *Sejam L um corpo e G um grupo finito de automorfismos de L. Então L^G é subcorpo de L e $[L : L^G] = |G|$.*

Definição 3.41. Seja $L : K$ uma extensão finita, normal e separável. Dizemos então que $L : K$ é uma **extensão galoisiana**.

Teorema 3.42. *Sejam $L : K$ uma extensão finita e $Gal(L : K)$ o respectivo grupo de Galois. Então as afirmações a seguir são equivalentes:*

(a) $L : K$ é uma extensão galoisiana;

(b) L é corpo de decomposição de um polinômio separável sobre K;

(c) $[L : K] = |Gal(L : K)|$;

(d) $L^{Gal(L:K)} = K$, isto é, K é o corpo fixado de $Gal(L : K)$;

(e) Existe um grupo G de K-automorfismos de L tal que $K = L^G$ e então, $G = Gal(L : K)$.

Proposição 3.43. *Sejam $f \in K[x]$ um polinômio com n raízes distintas e L corpo de decomposição de f sobre K. Então o grupo $Gal(L : K)$ é isomorfo à algum subgrupo de S_n.*

Demonstração.

Seja $X = \{\alpha_1, \ldots, \alpha_n\}$ o conjunto das raízes de f. Então $L = K(\alpha_1, \ldots, \alpha_n)$. Dado $\sigma \in \mathrm{Gal}(L : K)$, a Proposição 3.38 garante que $\sigma(X) = X$.

Defina a aplicação $\phi : \mathrm{Gal}(L:K) \to S_n$, dada por $\sigma \mapsto \sigma_X$, onde σ_X é a restrição de σ em X. Queremos mostrar que Φ é um homomorfismo injetivo.

Perceba que Φ é homomorfismo por definição. Para mostrar que ϕ é injetivo, considere $\sigma_X = \tau_X$, isto é, $\sigma(\alpha_i) = \tau(\sigma_i)$, $\forall\, i \in \{1, 2, \ldots, n\}$. Vamos mostrar que $\sigma = \tau$, ou seja, $\sigma(x) = \tau(x)$, $\forall\, x \in L$. Se $x \in L$, então $x = \sum_j c_j \alpha_1^{k_{j_1}} \alpha_2^{k_{j_2}} \cdots \alpha_n^{k_{j_n}}$. Temos:

$$\begin{aligned}
\sigma(x) &= \sigma\left(\sum_j c_j \alpha_1^{k_{j_1}} \alpha_2^{k_{j_2}} \cdots \alpha_n^{k_{j_n}}\right) = \sum_j \sigma(c_j \alpha_1^{k_{j_1}} \alpha_2^{k_{j_2}} \cdots \alpha_n^{k_{j_n}}) \\
&= \sum_j \sigma(c_j)\sigma(\alpha_1^{k_{j_1}})\sigma(\alpha_2^{k_{j_2}}) \cdots \sigma(\alpha_n^{k_{j_n}})) = \sum_j c_j \sigma(\alpha_1)^{k_{j_1}} \sigma(\alpha_2)^{k_{j_2}} \cdots \sigma(\alpha_n)^{k_{j_n}} \\
&= \sum_j c_j \tau(\alpha_1)^{k_{j_1}} \tau(\alpha_2)^{k_{j_2}} \cdots \tau(\alpha_n)^{k_{j_n}} = \sum_j \tau(c_j)\tau(\alpha_1^{k_{j_1}})\tau(\alpha_2^{k_{j_2}}) \cdots \tau(\alpha_n^{k_{j_n}})) \\
&= \sum_j \tau(c_j \alpha_1^{k_{j_1}} \alpha_2^{k_{j_2}} \cdots \alpha_n^{k_{j_n}}) = \tau\left(\sum_j c_j \alpha_1^{k_{j_1}} \alpha_2^{k_{j_2}} \cdots \alpha_n^{k_{j_n}}\right) \\
&= \tau(x).
\end{aligned}$$

Logo, ϕ é injetivo e, portanto, o grupo $\mathrm{Gal}(L:K)$ é isomorfo à algum subgrupo de S_n. □

Corolário 3.44. *Sejam $f \in K[x]$ um polinômio com n raízes distintas e L corpo de decomposição de f sobre K. Então $[L:K] \leq n!$.*

Demonstração.

Pela Proposição 3.43, temos que $\mathrm{Gal}(L:K)$ é isomorfo à algum subgrupo de S_n. Como $|S_n| = n!$, então $|\mathrm{Gal}(L:K)| = [L:K] \leq n!$. □

Exemplos 3.45. Vamos determinar os grupos de Galois das extensões de corpos a seguir.

1. $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$

   Solução.

   Perceba que $\mathbb{Q}(\sqrt{2})$ é corpo de decomposição de $f(x) = x^2 - 2$ sobre $\mathbb{Q}$. Como f é irredutível sobre $\mathbb{Q}$, então $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \partial(f) = 2$. A extensão $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ é galoisiana, pois é normal, finita e separável. Logo, $|\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})| = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

   Vamos agora determinar os elementos que pertencem ao grupo $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$. Sabemos que os $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\sqrt{2})$ devem permutar os zeros de f. Portanto os candidatos são:

σ	id	σ_1
$\sigma(\sqrt{2})$	$\sqrt{2}$	$-\sqrt{2}$

Note que $\sigma_1^2 = \sigma_1\sigma_1 = \text{id}$, pois $\sigma_1(\sigma_1(\sqrt{2})) = \sigma_1(-\sqrt{2}) = -\sigma_1(\sqrt{2}) = \sqrt{2}$.

Logo, segue que $\text{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) = \{\text{id}, \sigma_1\} \cong \mathbb{Z}_2$. □

2. $\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}$

Solução.

Perceba que $\mathbb{Q}(\sqrt{2}, i)$ é corpo de decomposição de $f(x) = (x^2+1)(x^2-2)$ sobre $\mathbb{Q}$. Logo, $\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}$ é uma extensão normal. Como f é separável, e $\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}$ é normal e finita, então $\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}$ é galoisiana. Pelo Teorema 3.16 (Lei da Torre), temos:

$$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})]}_{2, \text{ pois } i \notin \mathbb{Q}(\sqrt{2})} \cdot \underbrace{[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]}_{2} = 2 \cdot 2 = 4.$$

Disto temos $|\text{Gal}(\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q})| = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$. Os $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\sqrt{2}, i)$ são:

σ	id	σ_1	σ_2	σ_3
$\sigma(\sqrt{2})$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
$\sigma(i)$	i	i	$-i$	$-i$

Perceba que:

- $\sigma_1^2 = \text{id}$, visto que $\sigma_1^2(\sqrt{2}) = \sigma_1(\sigma_1(\sqrt{2})) = -\sigma_1(\sqrt{2}) = \sqrt{2}$, e $\sigma_1^2(i) = \sigma_1(\sigma_1(i)) = i$.
- $\sigma_2^2 = \text{id}$, visto que $\sigma_2^2(\sqrt{2}) = \sigma_2(\sigma_2(\sqrt{2}) = \sqrt{2}$, e $\sigma_2^2(i) = \sigma_2(\sigma_2(i)) = -\sigma_2(i) = i$.
- $\sigma_3^2 = \text{id}$, visto que $\sigma_3^2(\sqrt{2}) = \sigma_3(\sigma_3(\sqrt{2})) = -\sigma_3(\sqrt{2}) = \sqrt{2}$, e $\sigma_3^2(i) = \sigma_3(\sigma_3(i)) = -\sigma_3(i) = i$.

Logo, segue que $\text{Gal}(\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}) = \{\text{id}, \sigma_1, \sigma_2, \sigma_3\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. □

3. $\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}$, onde $\omega = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right)$

Solução.

Perceba que $\mathbb{Q}(\sqrt[3]{2}, \omega)$ é corpo de decomposição de $f(x) = x^3 - 2$ sobre $\mathbb{Q}$. Logo, $\mathbb{Q}(\sqrt[3]{2}, \omega)$ é uma extensão normal. Como f é separável, e $\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}$ é normal e finita, então $\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}$ é galoisiana. Pelo Teorema 3.16 (Lei da Torre), temos:

$$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})]}_{2, \text{ pois } \omega \notin \mathbb{Q}(\sqrt[3]{2})} \cdot \underbrace{[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]}_{3} = 2 \cdot 3 = 6.$$

Disto temos $|\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega):\mathbb{Q})| = [\mathbb{Q}(\sqrt[3]{2},\omega):\mathbb{Q}] = 6$ e segue que

$$\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \omega, \omega\sqrt[3]{2}, \omega(\sqrt[3]{2})^2\}$$

é base de $\mathbb{Q}(\sqrt[3]{2},\omega):\mathbb{Q}$.

Considere o $\mathbb{Q}$-automorfismo $\tau : \mathbb{Q}(\sqrt[3]{2},\omega) \to \mathbb{Q}(\sqrt[3]{2},\omega)$ dado por $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$ e $\tau(\omega) = \omega^2$. Considere também o $\mathbb{Q}$-automorfismo $\rho : \mathbb{Q}(\sqrt[3]{2},\omega) \to \mathbb{Q}(\sqrt[3]{2},\omega)$ dado por $\rho(\sqrt[3]{2}) = \omega\sqrt[3]{2}$ e $\rho(\omega) = \omega$. Temos:

- $\tau^2(\sqrt[3]{2}) = \tau(\tau(\sqrt[3]{2})) = \tau(\sqrt[3]{2}) = \sqrt[3]{2}$, e $\tau^2(\omega) = \tau(\tau(\omega)) = \tau(\omega^2) = \omega^4 = \omega$. Logo, $\tau^2 = \mathrm{id}$.
- $\rho^2(\sqrt[3]{2}) = \rho(\rho(\sqrt[3]{2})) = \rho(\omega\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$, e $\rho^2(\omega) = \rho(\rho(\omega)) = \rho(\omega) = \omega$.
- $\tau\rho(\sqrt[3]{2}) = \tau(\omega\sqrt[3]{2}) = \tau(\omega)\tau(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$, e $\tau\rho(\omega) = \tau(\omega) = \omega^2$.
- $\rho\tau(\sqrt[3]{2}) = \rho(\sqrt[3]{2}) = \omega\sqrt[3]{2}$, e $\rho\tau(\omega) = \rho(\omega^2) = \omega^2$.

Então, os $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\sqrt[3]{2},\omega)$ são:

σ	id	τ	ρ	$\rho\tau$	ρ^2	$\tau\rho$
$\sigma(\sqrt[3]{2})$	$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\omega\sqrt[3]{2}$	$\omega^2\sqrt[3]{2}$	$\omega^2\sqrt[3]{2}$
$\sigma(\omega)$	ω	ω^2	ω	ω^2	ω	ω^2

Logo, segue que $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega):\mathbb{Q}) \cong \langle\tau,\rho\rangle \cong S_3$. □

4. $\mathbb{Q}(\zeta):\mathbb{Q}$, onde $\zeta = \cos\left(\frac{2\pi}{7}\right) + i\,\mathrm{sin}\left(\frac{2\pi}{7}\right)$

Solução.

Note que $\zeta^7 = 1$, isto é, ζ é raiz do polinômio $p(x) = x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$. Perceba que $\mathbb{Q}(\zeta)$ é corpo de decomposição de $f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ sobre $\mathbb{Q}$. Como f é irredutível sobre $\mathbb{Q}$, então $[\mathbb{Q}(\zeta):\mathbb{Q}] = \partial(f) = 6$. A extensão $\mathbb{Q}(\zeta):\mathbb{Q}$ é galoisiana, pois é normal, finita e separável. Logo, $|\mathrm{Gal}(\mathbb{Q}(\zeta):\mathbb{Q})| = [\mathbb{Q}(\zeta):\mathbb{Q}] = 6$ e segue que $\{1,\zeta,\zeta^2,\zeta^3,\zeta^4,\zeta^5\}$ é base de $\mathbb{Q}(\zeta):\mathbb{Q}$.

Tome o $\mathbb{Q}$-automorfismo $\tau : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ dado por $\tau(\zeta) = \zeta^3$. Temos:

- $\tau^2(\zeta) = \tau(\tau(\zeta)) = \tau(\zeta^3) = \tau(\zeta)^3 = (\zeta^3)^3 = \zeta^9 = \zeta^7\cdot\zeta^2 = \zeta^2$.
- $\tau^3(\zeta) = \tau(\tau^2(\zeta)) = \tau(\zeta^2) = \tau(\zeta)^2 = (\zeta^3)^2 = \zeta^6$.
- $\tau^4(\zeta) = \tau(\tau^3(\zeta)) = \tau(\zeta^6) = \tau(\zeta)^6 = (\zeta^3)^6 = \zeta^{18} = \zeta^7\cdot\zeta^7\cdot\zeta^4 = \zeta^4$.
- $\tau^5(\zeta) = \tau(\tau^4(\zeta)) = \tau(\zeta^4) = \tau(\zeta)^4 = (\zeta^3)^4 = \zeta^{12} = \zeta^7\cdot\zeta^5 = \zeta^5$.

- $\tau^6(\zeta) = \tau(\tau^5(\zeta)) = \tau(\zeta^5) = \tau(\zeta)^5 = (\zeta^3)^5 = \zeta^{15} = \zeta^7 \cdot \zeta^7 \cdot \zeta = \zeta = \mathrm{id}\,.$

Então, os $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\zeta)$ são:

σ	id	τ	τ^2	τ^3	τ^4	τ^5
$\sigma(\zeta)$	ζ	ζ^3	ζ^2	ζ^6	ζ^4	ζ^5

Logo, segue que $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}) = \langle\tau\rangle \cong \mathbb{Z}_7^* \cong \mathbb{Z}_6$. □

5. $\mathbb{R}(x) : \mathbb{R}\left(x^2 + \frac{1}{x^2}\right)$

Solução.

Defina as aplicações $\rho : \mathbb{R}(x) \to \mathbb{R}(x)$ dada por $\rho(x) = -x$, e $\tau : \mathbb{R}(x) \to \mathbb{R}(x)$ dada por $\tau(x) = \dfrac{1}{x}$. Perceba que ρ e τ são $\mathbb{R}\left(x^2 + \frac{1}{x^2}\right)$-automorfismos e também que:

- $\rho^2 = \mathrm{id}$, visto que $\rho(\rho(x)) = \rho(-x) = x$.
- $\tau^2 = \mathrm{id}$, visto que $\tau(\tau(x)) = \tau(\frac{1}{x}) = x$.
- $\rho\tau = \tau\rho$, visto que $\rho(\tau(x)) = \rho(\frac{1}{x}) = -\frac{1}{x}$, $\tau(\rho(x)) = \tau(-x) = -\frac{1}{x}$.
- $(\rho\tau)^2 = \mathrm{id}$, visto que $\rho\tau(\rho\tau(x)) = \rho\tau(-\frac{1}{x}) = x$.

Portanto segue que $\langle\rho, \tau\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, e também que $\langle\rho, \tau\rangle$ é um grupo de automorfismos que fixa $\mathbb{R}\left(x^2 + \frac{1}{x^2}\right)$:

σ	id	ρ	τ	$\rho\tau$
$\sigma(x)$	x	$-x$	$\frac{1}{x}$	$-\frac{1}{x}$

Portanto, $|\mathrm{Gal}(\mathbb{R}(x) : \mathbb{R}\left(x^2 + \frac{1}{x^2}\right))| = [\mathbb{R}(x) : \mathbb{R}\left(x^2 + \frac{1}{x^2}\right)] = 4$ e concluímos que $\mathrm{Gal}(\mathbb{R}(x) : \mathbb{R}\left(x^2 + \frac{1}{x^2}\right)) = \{\mathrm{id}, \rho, \tau, \rho\tau\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. □

6. $\mathbb{R} : \mathbb{Q}$

Solução.

Note que $\mathbb{R} : \mathbb{Q}$ possui grau infinito e portanto não é uma extensão galoisiana.

Sejam $\sigma \in \mathrm{Gal}(\mathbb{R} : \mathbb{Q})$ e $a, b \in \mathbb{R}$. Como σ é homomorfismo, então $\sigma(a^2) = \sigma(a)^2$ e, portanto, σ leva reais positivos em reais positivos. Suponha que $a < b$. Como $\mathbb{Q}$ é denso em $\mathbb{R}$, então existe $u \in \mathbb{Q}$ tal que $a < u < b$. Temos:

$$u = \sigma(u) = \sigma(u - a + a) = \sigma(u - a) + \sigma(a) > \sigma(a);$$

$$u = \sigma(u) = \sigma(u - b + b) = \sigma(u + b) - \sigma(b) < \sigma(b).$$

Então $\sigma(a) < u < \sigma(b)$, isto é, $a < b \Rightarrow \sigma(a) < \sigma(b)$, $\forall\, a, b \in \mathbb{R}$.

Vamos agora mostrar que $|a - b| < \dfrac{1}{m} \Rightarrow |\sigma(a) - \sigma(b)| < \dfrac{1}{m}$, $\forall\, m \in \mathbb{Z}_+$. Pelo o que vimos anteriormente, temos:

$$-\frac{1}{m} = \sigma\left(-\frac{1}{m}\right) < \sigma(a - b) = \sigma(a) - \sigma(b) < \sigma\left(\frac{1}{m}\right) = \frac{1}{m}.$$

Logo $|a - b| < \dfrac{1}{m} \Rightarrow |\sigma(a) - \sigma(b)| < \dfrac{1}{m}$, $\forall\, m \in \mathbb{Z}_+$.
Por definição σ é contínua se $\forall\, \epsilon > 0$, $\exists\, \delta > 0$ tal que $|x - y| < \delta \Rightarrow |\sigma(a) - \sigma(b)| < \epsilon$.
Fixe $\epsilon > 0$, onde $\delta = \dfrac{1}{m} < \epsilon$, m inteiro. Se $|x - y| < \delta$, então pelo o que mostramos acima, segue que $|\sigma(x) - \sigma(y)| < \dfrac{1}{m} < \epsilon$. Logo σ é contínua.
Vamos agora provar que qualquer função σ contínua em $\mathbb{R}$ que fixa os elementos de $\mathbb{Q}$ é igual à identidade. Seja $x \in \mathbb{R}$ e $\epsilon > 0$. Como σ é contínua, $\exists\, 0 < \delta < \dfrac{\epsilon}{2}$ tal que $|x - y| < \delta \Rightarrow |\sigma(x) - \sigma(y)| < \dfrac{\epsilon}{2}$. Seja $\rho = \min\left(\dfrac{\epsilon}{2}, \delta\right)$ e seja $a \in \mathbb{Q}$ tal que $|x - a| < \rho$. Então:

$$|\sigma(x) - x| = |\sigma(x) - a + (a - x)| \leq |\sigma(x) - \sigma(a)| + |a - x| < \frac{\epsilon}{2} + \rho < \epsilon.$$

Logo $\sigma(x) = x$, $\forall\, x \in \mathbb{R}$, e segue que $\mathrm{Gal}(\mathbb{R} : \mathbb{Q}) = \{\mathrm{id}\}$. □

3.5.1 Teorema Fundamental de Galois

Definição 3.46. Seja $L : K$ uma extensão de corpos finita. Dizemos que M é um **corpo intermediário** de $L : K$ se M é subcorpo de L contendo K, ou seja, $L \supseteq M \supseteq K$.

Enunciaremos agora o Teorema Fundamental de Galois.

Teorema 3.47 (Teorema Fundamental de Galois)**.** *Seja $L : K$ uma extensão galoisiana.*

(a) A extensão $L : M$ é galoisiana e existe uma correspondência entre os subcorpos intermediários M de $L : K$ e os subgrupos H de $Gal(L : K)$, dada pela bijeção natural:

$$\begin{Bmatrix} \textit{subgrupos} \\ H \textit{ de } Gal(L : K) \end{Bmatrix} \quad \longleftrightarrow \quad \begin{Bmatrix} \textit{subcorpos intermediários} \\ M \textit{ de } L : K \end{Bmatrix}$$
$$H \quad \longmapsto \quad L^H$$
$$Gal(L : M) \quad \longleftarrow\!\shortmid \quad M.$$

(b) A extensão $M : K$ é galoisiana se, e somente se, $Gal(L : M)$ é subgrupo normal de $Gal(L : K)$. Nessas condições, vale $Gal(M : K) \cong \frac{Gal(L:K)}{Gal(L:M)}$ e $[M : K] = \frac{|Gal(L:K)|}{|Gal(L:M)|}$.

Vamos aplicar este teorema nos exemplos a seguir.

Exemplos 3.48. Dadas as extensões galoisianas a seguir, determinaremos os subgrupos do grupo de Galois e seus respectivos corpos intermediários.

1. $\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}$

   Solução.

   Vimos no item 2 dos Exemplos 3.45 que $\text{Gal}(\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}) = \{\text{id}, \sigma_1, \sigma_2, \sigma_3\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, onde os $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\sqrt{2}, i)$ são:

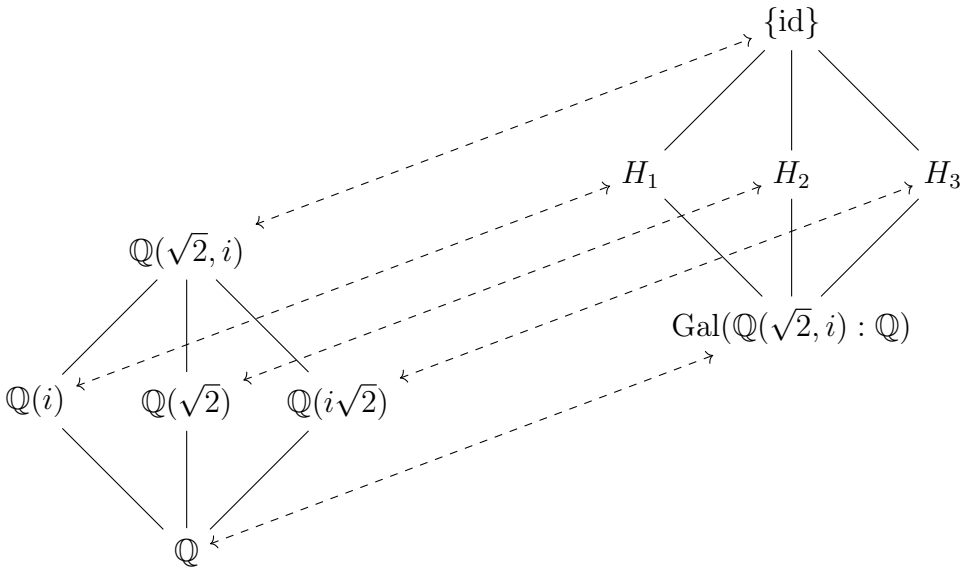
σ	id	σ_1	σ_2	σ_3
$\sigma(\sqrt{2})$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
$\sigma(i)$	i	i	$-i$	$-i$

   Vimos também que $\sigma_j^2 = \text{id}$ para $j \in \{1, 2, 3\}$. Logo, os subgrupos de $\text{Gal}(\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q})$ são $H_1 = \{\text{id}, \sigma_1\}$, $H_2 = \{\text{id}, \sigma_2\}$, $H_3 = \{\text{id}, \sigma_3\}$, $\{\text{id}\}$ e $\text{Gal}(\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q})$.

   Vamos então determinar os corpos intermediários associados a cada subgrupo. Se $L = \mathbb{Q}(\sqrt{2}, i)$, temos:

   - $L^{H_1} = \{x \in L : \sigma(x) = x, \forall\, \sigma \in H_1\} = \mathbb{Q}(i)$.
   - $L^{H_2} = \{x \in L : \sigma(x) = x, \forall\, \sigma \in H_2\} = \mathbb{Q}(\sqrt{2})$.
   - $L^{H_3} = \{x \in L : \sigma(x) = x, \forall\, \sigma \in H_3\} = \mathbb{Q}(i\sqrt{2})$.

   Podemos denotar a correspondência entre os subcorpos de $\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}$ e os subgrupos de $\text{Gal}(\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q})$ da seguinte maneira:



O subgrupo H_1 de $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},i):\mathbb{Q})$ é normal. Então, pelo Teorema 3.47 (Teorema Fundamental de Galois), $\mathbb{Q}(i):\mathbb{Q}$ é uma extensão galoisiana e $\mathrm{Gal}(\mathbb{Q}(i):\mathbb{Q}) \cong (\mathbb{Z}_2 \times \mathbb{Z}_2)/H_1 \cong \mathbb{Z}_2$.

Da mesma forma, H_2 é normal. Então, $\mathbb{Q}(\sqrt{2}):\mathbb{Q}$ é uma extensão galoisiana e $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}):\mathbb{Q}) \cong (\mathbb{Z}_2 \times \mathbb{Z}_2)/H_2 \cong \mathbb{Z}_2$.

Também, H_3 é normal. Então, $\mathbb{Q}(i\sqrt{2}):\mathbb{Q}$ é uma extensão galoisiana e $\mathrm{Gal}(\mathbb{Q}(i\sqrt{2}):\mathbb{Q}) \cong (\mathbb{Z}_2 \times \mathbb{Z}_2)/H_3 \cong \mathbb{Z}_2$. □

2. $\mathbb{Q}(\zeta):\mathbb{Q}$, onde $\zeta = \cos\left(\frac{2\pi}{7}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{7}\right)$

Solução.

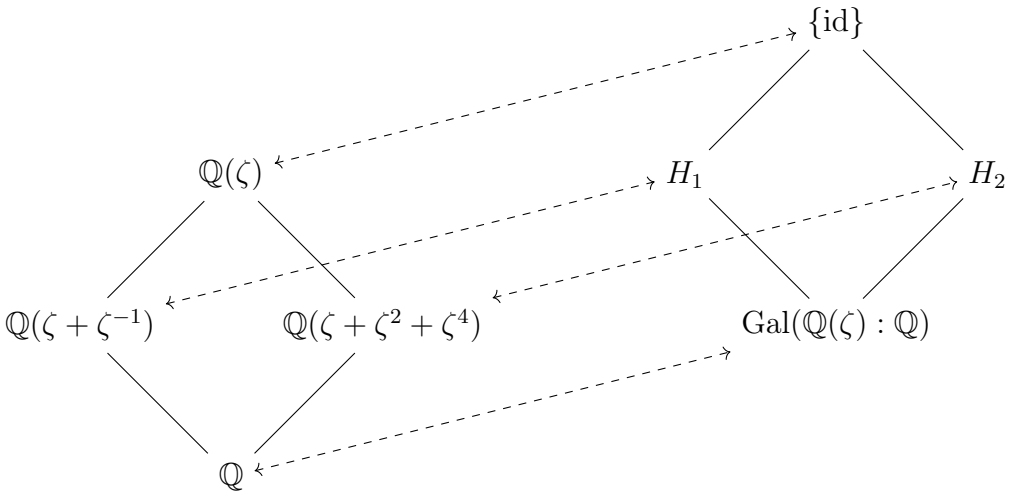
Vimos no item 4 dos Exemplos 3.45 que $\mathrm{Gal}(\mathbb{Q}(\zeta):\mathbb{Q}) = \langle\tau\rangle \cong \mathbb{Z}_7^* \cong \mathbb{Z}_6$, onde os $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\zeta)$ são:

σ	id	τ	τ^2	τ^3	τ^4	τ^5
$\sigma(\zeta)$	ζ	ζ^3	ζ^2	ζ^6	ζ^4	ζ^5

Os subgrupos de $\mathrm{Gal}(\mathbb{Q}(\zeta):\mathbb{Q})$ são $H_1 = \{\mathrm{id}, \tau^3\}$, $H_2 = \{\mathrm{id}, \tau^2, \tau^4\}$, $\{\mathrm{id}\}$ e $\mathrm{Gal}(\mathbb{Q}(\zeta):\mathbb{Q})$.

Vamos então determinar os corpos intermediários correspondentes a cada subgrupo. Se $L = \mathbb{Q}(\zeta)$, temos:

- $L^{H_1} = \{x \in L : \sigma(x) = x,\ \forall\, \sigma \in H_1\} = \mathbb{Q}(\zeta + \zeta^6) = \mathbb{Q}(\zeta + \zeta^{-1})$.
  Basta notar que $\tau^3(\zeta + \zeta^6) = \tau^3(\zeta) + (\tau^3(\zeta))^6 = \zeta^6 + \zeta$, ou seja, $\zeta + \zeta^6$ é fixado por τ^3.
- $L^{H_2} = \{x \in L : \sigma(x) = x,\ \forall\, \sigma \in H_2\} = \mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$.
  Basta notar que $\tau^2(\zeta + \zeta^2 + \zeta^4) = \tau^2(\zeta) + (\tau^2(\zeta))^2 + (\tau^2(\zeta))^4 = \zeta^2 + \zeta^4 + \zeta$ e $\tau^4(\zeta + \zeta^2 + \zeta^4) = \tau^4(\zeta) + (\tau^4(\zeta))^2 + (\tau^4(\zeta))^4 = \zeta^4 + \zeta + \zeta^2$, ou seja, $\zeta + \zeta^2 + \zeta^4$ é fixado por τ^2 e τ^4.



O subgrupo H_1 de $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$ é normal. Então, pelo Teorema 3.47 (Teorema Fundamental de Galois), $\mathbb{Q}(\zeta+\zeta^{-1}) : \mathbb{Q}$ é uma extensão galoisiana e $\mathrm{Gal}(\mathbb{Q}(\zeta+\zeta^{-1}) : \mathbb{Q}) \cong \mathbb{Z}_6/H_1 \cong \mathbb{Z}_3$.

Da mesma forma, H_2 é normal. Então, $\mathbb{Q}(\zeta+\zeta^2+\zeta^4) : \mathbb{Q}$ é uma extensão galoisiana e $\mathrm{Gal}(\mathbb{Q}(\zeta+\zeta^2+\zeta^4) : \mathbb{Q}) \cong \mathbb{Z}_6/H_2 \cong \mathbb{Z}_2$. □

3.6 Solubilidade de equações polinomiais por radicais

O nascimento da Teoria de Galois se deu por conta de uma questão matemática que estava aberta até o início do século XIX:

- Existe uma fórmula para encontrar as raízes de uma equação polinomial de grau maior ou igual a 5 em termos dos coeficientes desta equação, usando apenas operações básicas (adição, subtração, multiplicação, divisão) e raízes n-ésimas?

O Teorema de Abel-Ruffini prova que existem equações polinomiais no qual tal fórmula não existe. Mas a Teoria de Galois fornece uma resposta muito mais completa a esta pergunta, explicando o motivo de ser possível resolver todas as equações de grau quatro ou inferior, e o motivo de não ser possível para a maioria das equações de grau cinco ou superior. Além disso, fornece uma ferramenta de determinar se uma equação polinomial é solúvel por radicais.

Vamos estudar o conceito de grupo solúvel e, em seguida, estudaremos os critérios para determinar se uma equação é solúvel por radicais.

Alguns resultados desta seção serão apenas enunciados. As demonstrações podem ser encontradas em [1], Capítulos 12 e 13.

Definição 3.49. Um grupo G é dito **solúvel** se existe uma cadeia de grupos

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$$

tal que G_{i+1} é normal em G_i e os quocientes G_i/G_{i+1} são abelianos para $i = 0, 1, \ldots, n-1$.

Proposição 3.50. *Seja G um grupo.*

(a) Se G é solúvel e H é um subgrupo de G, então H é solúvel.

(b) Se N é um subgrupo normal de G e G é solúvel, então o grupo quociente G/N é solúvel.

(c) Se N é um subgrupo normal solúvel de G tal que o grupo quociente G/N é solúvel, então G é solúvel.

Proposição 3.51. *Se $n \geq 5$, então o grupo simétrico S_n não é solúvel.*

Definição 3.52. Uma extensão de corpos $L : K$ é dita **extensão radical** se existe uma cadeia de corpos

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = L$$

tal que $K_j = K_{j-1}(\alpha_j)$, onde $\alpha_j^{r_j} \in K_{j-1}$ e r_j são inteiros positivos para $j = 1, \ldots, n-1$.

Em especial, se $L = K(\alpha)$, onde $\alpha^n \in K$ para algum n inteiro positivo, dizemos que $L : K$ é uma **extensão radical simples**.

Definição 3.53. Dado $f \in K[x]$, dizemos que $f(x) = 0$ é **solúvel por radicais** sobre K se o corpo de decomposição de f sobre K está contido em uma extensão radical $L : K$. Dizemos que uma extensão $L : K$ é uma **extensão solúvel** se L é um subcorpo de uma extensão radical de K.

Teorema 3.54 (Teorema Casus Irreducibilis)**.** *Se $f(x) \in \mathbb{Q}[x]$ é um polinômio cúbico irredutível sobre $\mathbb{Q}$ com três zeros reais, então $f(x) = 0$ não é solúvel por radicais reais.*

Vamos ver alguns exemplos.

Exemplos 3.55.

1. A extensão $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ é radical simples.

   Solução.

   Note que $(\sqrt[3]{2})^3 = 2 \in \mathbb{Q}$. Então, pela Definição 3.52, segue que $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ é uma extensão radical simples. □

2. A extensão $\mathbb{Q}(\sqrt[5]{1+\sqrt{3}}) : \mathbb{Q}$ é radical.

   Solução.

   Note que $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt[5]{1+\sqrt{3}})$. Temos: $(\sqrt[5]{1+\sqrt{3}})^5 = 1+\sqrt{3} \in \mathbb{Q}(\sqrt{3})$, e $(\sqrt{3})^2 = 3 \in \mathbb{Q}$. Então, pela Definição 3.52, segue que $\mathbb{Q}(\sqrt[5]{1+\sqrt{3}}) : \mathbb{Q}$ é uma extensão radical. □

3. A extensão $\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}$, onde $\zeta = \cos\left(\frac{2\pi}{7}\right) + i \sin\left(\frac{2\pi}{7}\right)$, não é radical.

   Solução.

   Perceba que $\zeta + \zeta^{-1} = \zeta + \zeta^6 = 2\cos\left(\frac{2\pi}{7}\right)$. Então, $\mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(\cos\left(\frac{2\pi}{7}\right))$. Note também que ζ é raiz de

   $$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0.$$

Utilizando o fato que $\alpha = \cos\left(\frac{2\pi}{7}\right) = \frac{\zeta+\zeta^{-1}}{2}$, temos:

$$\begin{aligned} 0 = \sum_{j=0}^{6} \zeta^j &= \zeta^3 + \zeta^{-3} + \zeta^2 + \zeta^{-2} + \zeta + \zeta^{-1} + 1 \\ &= (\zeta + \zeta^{-1})^3 - 3(\zeta + \zeta^{-1}) + (\zeta + \zeta^{-1})^2 - 2 + (\zeta + \zeta^{-1}) + 1 \\ &= (\zeta + \zeta^{-1})^3 + (\zeta + \zeta^{-1})^2 - 2(\zeta + \zeta^{-1}) - 1 \\ &= (2\alpha)^3 + (2\alpha)^2 - 2(2\alpha) - 1 \\ &= 8\alpha^3 + 4\alpha^2 - 4\alpha - 1. \end{aligned}$$

Logo, $p(x) = 8x^3+4x^2-4x-1$ é um candidato a polinômio minimal de $\cos\left(\frac{2\pi}{7}\right)$ sobre $\mathbb{Q}$. Utilizando o Teorema 2.47 (critério redução módulo 3), concluímos que de fato p é o polinômio minimal. Os zeros de p são $\cos\left(\frac{2\pi}{7}\right)$, $\cos\left(\frac{4\pi}{7}\right)$, e $\cos\left(\frac{6\pi}{7}\right)$. Como as três raízes de $p(x) = 0$ são reais, então pelo Teorema 3.54 (Teorema Casus Irreducibilis) é impossível encontrar soluções para $p(x) = 0$ por radicais reais, ou seja, $p(x) = 0$ não é solúvel por radicais reais. Logo, pela Definição 3.53, $\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}$ não é uma extensão radical. □

Teorema 3.56. *Dado $f \in K[x]$, a equação $f(x) = 0$ é solúvel por radicais se, e somente se, o grupo de Galois de f sobre K é solúvel.*

Teorema 3.57 (Teorema de Weber)**.** *Sejam $K \subseteq \mathbb{R}$ um corpo e p um número primo. Se $f \in K[x]$ é um polinômio irredutível de grau p com exatamente duas raízes complexas não reais, então o grupo de Galois do corpo de decomposição de f sobre K é S_p.*

Demonstração.

Seja L o corpo de decomposição de f sobre K. Então a extensão $L : K$ é galoisiana e, portanto, $|\mathrm{Gal}(L : K)| = [L : K]$. Como f é irredutível, então f é separável, ou seja, possui todas as raízes distintas. Logo, os elementos de $\mathrm{Gal}(L : K)$ permutam as raízes de f, o que implica que $\mathrm{Gal}(L : K)$ é subgrupo de S_p.

Seja α uma raiz de f. Então $[K(\alpha) : K] = p$. Temos:

$$[L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K] = [L : K(\alpha)] \cdot p.$$

Logo $p \mid [L : K] = |\mathrm{Gal}(L : K)|$. Então pelo Teorema 2.19, existe $\sigma \in \mathrm{Gal}(L : K)$ tal que $\gamma = \sigma^p = \mathrm{id}_{\mathrm{Gal}(L:K)}$. Note que γ é um p-ciclo de $\mathrm{Gal}(L : K)$. Seja $\tau \in \mathrm{Gal}(L : K)$ o automorfismo que permuta as duas raízes complexas não reais e fixa as outras. Como γ é um ciclo e τ é uma transposição, então γ e τ geram o grupo S_p. Logo, $\mathrm{Gal}(L : K) \cong S_p$. □

Exemplos 3.58. Vamos verificar se as equações a seguir são solúveis por radicais sobre $\mathbb{Q}$.

1. $x^3 - 2 = 0$

   Solução.

   Seja $\omega = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right)$. Vimos no item 3 do Exemplo 3.45 que $\mathbb{Q}(\sqrt[3]{2}, \omega)$ é corpo de decomposição de $x^3 - 2$ sobre $\mathbb{Q}$, e que $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}) \cong S_3$. Pela Definição 3.49, para verificar se S_3 é solúvel, basta mostrar uma sequência de subgrupos normais cujo quociente seja abeliano. Tome a sequência de subgrupos normais:

   $$S_3 \supseteq \langle (123) \rangle \supseteq \{\mathrm{id}\}.$$

   Observe que $S_3/\langle (123) \rangle \cong \mathbb{Z}_2$ e $\langle (123) \rangle / \{\mathrm{id}\} \cong \mathbb{Z}_3$. Como $\mathbb{Z}_2$ e $\mathbb{Z}_3$ são abelianos, então S_3 é solúvel.

   Logo, pelo Teorema 3.56, como S_3 é solúvel, então $x^3 - 2 = 0$ é solúvel por radicais. □

2. $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$

   Solução.

   Seja $\zeta = \cos\left(\frac{2\pi}{7}\right) + i \sin\left(\frac{2\pi}{7}\right)$. Vimos no item 4 do Exemplo 3.45 que $\mathbb{Q}(\zeta)$ é corpo de decomposição de $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ sobre $\mathbb{Q}$, e que $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}) \cong \mathbb{Z}_6$. Pela Definição 3.49, para verificar se $\mathbb{Z}_6$ é solúvel, basta mostrar uma sequência de subgrupos normais cujo quociente seja abeliano. Tome a sequência de subgrupos normais:

   $$\mathbb{Z}_6 \supseteq \langle 2 \rangle \supseteq \{\mathrm{id}\}.$$

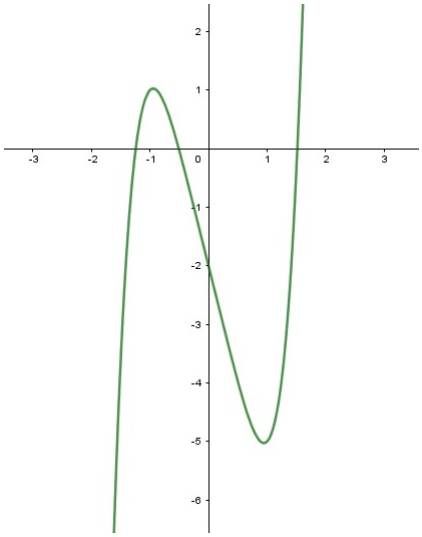
   Observe que $\mathbb{Z}_6/\langle 2 \rangle \cong \mathbb{Z}_2$ e $\langle 2 \rangle / \{\mathrm{id}\} \cong \mathbb{Z}_3$. Como $\mathbb{Z}_2$ e $\mathbb{Z}_3$ são abelianos, então $\mathbb{Z}_6$ é solúvel.

   Logo, pelo Teorema 3.56, como $\mathbb{Z}_6$ é solúvel, então $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$ é solúvel por radicais. □

3. $x^5 - 4x - 2 = 0$

   Solução.

   Seja $f(x) = x^5 - 4x - 2$. O polinômio f é irredutível sobre $\mathbb{Q}$ pelo Teorema 2.45 (Critério de Eisenstein) com $p = 2$. A derivada de f é $f'(x) = 5x^4 - 4$. Calculando $f'(x) = 0$, obtemos as raízes $x_1 = -\frac{\sqrt{2}}{\sqrt[4]{5}}$ e $x_2 = \frac{\sqrt{2}}{\sqrt[4]{5}}$. Logo, f possui dois pontos extremantes. Uma simples verificação nos diz que $f(x_1) > 0$, $f(x_2) < 0$, $\lim_{x \to +\infty} f(x) = +\infty$, e $\lim_{x \to -\infty} f(x) = -\infty$. Com isso, é possível esboçar o gráfico de f:



Portanto, f possui três zeros reais, o que implica que os outros dois são complexos não reais. Pelo Teorema 3.57, segue que o grupo de Galois do corpo de decomposição de f sobre $\mathbb{Q}$ é S_5. Como S_5 não é solúvel, então $f(x) = 0$ não é solúvel por radicais. □

Teorema 3.59 (Abel-Ruffini)**.** *Seja o polinômio*

$$f(x) = \prod_{i=1}^{n}(x - x_i) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n,$$

onde s_i são as funções elementares simétricas de $x_1, x_2, \ldots, x_n$, ou seja, $s_1 = \sum_{i=1}^{n} x_i$, $s_2 = \sum_{i=1}^{n}\sum_{j=1}^{n} x_ix_j$, ..., $s_n = \prod_{i=1}^{n} x_i$. Então $f(x) = 0$ não é solúvel por radicais se $n \geq 5$.

Demonstração.

Perceba que $K(x_1, \ldots, x_n)$ é corpo de decomposição de f sobre $K(s_1, \ldots, s_n)$. Seja $\sigma \in S_n$. Note que σ permuta as raízes $x_1, \ldots, x_n$ e, por conta disso, σ fixa cada s_j, $j \in \{1, 2, \ldots, n\}$.

Então temos a seguinte torre de corpos:

$$K(x_1, \ldots, x_n) \supseteq K(x_1, \ldots, x_n)^{S_n} \supseteq K(s_1, \ldots, s_n),$$

onde $K(x_1, \ldots, x_n)^{S_n} = \{x \in K(x_1, \ldots, x_n) : \sigma(x) = x, \forall\, \sigma \in S_n\}$.

Perceba que $[K(x_1, \ldots, x_n) : K(x_1, \ldots, x_n)^{S_n}] = |S_n| = n!$. Como $K(x_1, \ldots, x_n)$ é corpo de decomposição de f sobre $K(s_1, \ldots, s_n)$ e $\partial(f) = n$, então, pelo Corolário 3.44, $[K(x_1, \ldots, x_n) : K(s_1, \ldots, s_n)] \leq n!$. Logo, $K(x_1, \ldots, x_n)^{S_n} = K(x_1, \ldots, x_n)$.

Portanto, pelo Teorema 3.42, $\mathrm{Gal}(K(x_1, \ldots, x_n) : K(s_1, \ldots, s_n)) = S_n$. Se $n \geq 5$, pela Proposição 3.51, S_n não é solúvel. Agora aplicando o Teorema 3.56, concluimos que $f(x) = 0$ não é solúvel por radicais para $n \geq 5$. □

3.7 Problemas Clássicos da Matemática Grega

Os Problemas Clássicos da Matemática Grega são:

- a duplicação do cubo: dado um cubo, é possível construir outro cubo com o dobro do volume do cubo inicial, utilizando apenas régua e compasso?
- a quadratura do círculo: dado um círculo, é possível construir um quadrado com a mesma área do círculo dado, utilizando apenas régua e compasso?
- a trisecção do ângulo: é possível dividir um ângulo qualquer em três partes iguais, utilizando apenas régua e compasso?

Estes problemas ficaram em aberto por mais de vinte séculos, e apenas em 1837, o matemático Pierre Wantzel apresentou a prova da impossibilidade de duas destas construções: a duplicação do cubo e a trisecção do ângulo. Posteriormente, em 1882 Lindemann provou a impossibilidade da quadratura do círculo, ao demonstrar a transcendência do número π sobre o corpo dos números racionais.

Atualmente, conseguimos utilizar conceitos de extensões de corpos para provar esses resultados, como veremos a seguir.

Definição 3.60. Seja $X \subset \mathbb{R}^2$. Dizemos que um ponto P é **construtível** a partir de X se existe um inteiro n e uma sequência de pontos $(P_1, \ldots, P_n)$ com $P_n = P$ tal que para qualquer $i \in \{1, 2, \ldots, n\}$, $X_i = X \cup \{P_1, \ldots, P_{i-1}\}$ satisfaz uma das afirmações a seguir:

- existem 4 pontos $A, B, C, D \in X_i$ tal que P_i é o ponto de interseção entre as retas (AB) e (CD);
- existem 4 pontos $A, B, C, O \in X_i$ tal que P_i é um ponto de interseção entre a reta (AB) e a circunferência de centro O e raio CO;
- existem 4 pontos $O, M, O', M' \in X_i$ tal que P_i é um ponto de interseção entre a circunferência de centro O e raio OM e a a circunferência de centro O' e raio $O'M'$.

Aqui, a régua considerada não possui marcas, é apenas um instrumento que permite ligar dois pontos do plano. As circunferências são definidas por um centro dado e um ponto da circunferência dado.

Definição 3.61. Seja $X \subset \mathbb{R}$. Dizemos que um número real α é **construtível** a partir de X se α é abscissa de um ponto do plano que é construtível a partir dos pontos $(\xi, 0)$ com $\xi \in X$.

Proposição 3.62. *Seja $X \subset \mathbb{R}$ tal que $0, 1 \in X$. O conjunto $\mathscr{C}_X$ de todos os números reais que são construtíveis a partir de X satisfazem as seguintes propriedades:*

1. *Se* $\alpha, \beta \in \mathscr{C}_X$, *então* $\alpha+\beta, \alpha-\beta, \alpha\beta, \in \mathscr{C}_X$.

2. *Se* $\alpha, \beta \in \mathscr{C}_X$ *com* $\beta \neq 0$, *então* $\frac{\alpha}{\beta} \in \mathscr{C}_X$.

3. *Seja* $\alpha > 0$. *Se* $\alpha \in \mathscr{C}_X$, *então* $\sqrt{\alpha} \in \mathscr{C}_X$.

Um fato que decorre da proposição anterior é que o conjunto dos números reais construtíveis a partir de $\{0,1\}$ é um subcorpo de $\mathbb{R}$. Ser construtível a partir de $\{0,1\}$ é equivalente a ser construtível a partir de $\mathbb{Q}$.

A proposição seguinte descreve a estrutura algébrica das extensões de grau 2 e também justifica o fato destas extensões também serem chamadas de extensões quadráticas.

Proposição 3.63. *Sejam* K *um subcorpo de* $\mathbb{R}$ *e considere* $L : K$ *uma extensão de corpos de grau 2. Então existe* $\delta \in L \setminus K$ *tal que* $\delta^2 \in K$ *e* $L = K(\delta)$.

Demonstração.

Seja $\alpha \in L \setminus K$. Como $[L : K] = 2$, então o conjunto $\{1, \alpha\}$ é uma base da extensão $L : K$. Logo, o conjunto $\{1, \alpha, \alpha^2\}$ é linearmente dependente, o que implica que existem $a, b, c \in K$ não todos nulos tais que $a\alpha^2 + b\alpha + c = 0$. Como $\{1, \alpha\}$ é linearmente independente, então $a \neq 0$. Com isso,

$$\begin{aligned}
& a\alpha^2 + b\alpha + c = 0 \\
\Leftrightarrow \quad & a\left(\alpha + \frac{b}{2a}\right)^2 - \frac{b^2}{4a} + c = 0 \\
\Leftrightarrow \quad & a\left(\alpha + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a} \\
\Leftrightarrow \quad & \left(\alpha + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2} \\
\Leftrightarrow \quad & \left(\frac{2a\alpha + b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2} \\
\Leftrightarrow \quad & (2a\alpha + b)^2 = b^2 - 4ac.
\end{aligned}$$

Seja $\delta = 2a\alpha + b \in L \setminus K$. Então $\delta^2 = b^2 - 4ac \in K$. Como $\alpha = \dfrac{\delta - b}{2a}$, então $\{1, \delta\}$ é base de $L : K$ e, portanto, $L = K(\delta)$. □

Teorema 3.64 (Wantzel, 1837)**.** *Seja* K *um subcorpo de* $\mathbb{R}$. *Um número* $\alpha \in \mathbb{R}$ *é construtível a partir de* K *se, e somente se, existem* $n \in \mathbb{Z}$ *e uma cadeia de extensões de corpos*

$$\mathbb{R} \supseteq K_n \supseteq \cdots \supseteq K_1 \supseteq K$$

tais que para qualquer $i \in \{1, \ldots, n\}$, *temos* $[K_i : K_{i-1}] = 2$ *e* $\alpha \in K_n$.

A demonstração do teorema anterior pode ser encontrada em [2], Teorema 1.4.1.

Corolário 3.65. *Sejam K um subcorpo de $\mathbb{R}$ e $\alpha \in \mathbb{R}$ um número construtível a partir de K. Então α é algébrico sobre K e $[K(\alpha) : K] = 2^r$ para algum r inteiro positivo.*

Demonstração.

Considere a cadeia de extensões quadráticas abaixo tal que $\alpha \in K_n$:

$$\mathbb{R} \supseteq K_n \supseteq \cdots \supseteq K_1 \supseteq K.$$

Utilizando o Teorema 3.16 (Lei da Torre) recursivamente, obtemos:

$$[K_n : K] = [K_n : K_1] \cdot [K_1 : K] = [K_n : K_1] \cdot 2 = \cdots = 2^n.$$

Então, como $[K_n : K] = [K_n : K(\alpha)] \cdot [K(\alpha) : K] = 2^n$, segue que $[K(\alpha) : K] \mid 2^n$. Portanto α é algébrico sobre K e $[K(\alpha) : K] = 2^r$ para algum $r \leq n$ inteiro positivo. □

Vamos agora demonstrar a impossibilidade das construções dadas pelos Problemas Clássicos da Matemática Grega.

Teorema 3.66 (Duplicação do cubo)**.** *O número real $\sqrt[3]{2}$ não é construtível a partir de $\mathbb{Q}$.*

Demonstração.

Seja $p(x) = x^3 - 2$. Claramente $p(\sqrt[3]{2}) = 0$. Perceba que p é irredutível sobre $\mathbb{Q}$ pelo Teorema 2.45 (Critério de Eisenstein) tomando $p = 2$. Logo, p é o polinômio minimal de α sobre $\mathbb{Q}$ e segue que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Pelo Corolário 3.65, concluímos que α não é construtível. □

Teorema 3.67 (Quadratura do círculo)**.** *O número real $\sqrt{\pi}$ não é construtível a partir de $\mathbb{Q}$.*

Demonstração.

Suponha, por absurdo, que $\sqrt{\pi}$ é construtível. Então $\sqrt{\pi}$ é algébrico sobre $\mathbb{Q}$, o que implica que $\sqrt{\pi} \cdot \sqrt{\pi} = \pi$ é algébrico sobre $\mathbb{Q}$. Contradição, visto que π é transcendente sobre $\mathbb{Q}$. □

Para o problema da trissecção do ângulo, dada o ponto com coordenadas $(\cos(\alpha), \text{sen}(\alpha))$ na circunferência unitária, queremos construir o ponto com coordenadas $(\cos(\frac{\alpha}{3}), \text{sen}(\frac{\alpha}{3}))$.

Note que $\text{sen}(\alpha) \in \mathbb{Q}(\cos(\alpha))$, pois $\text{sen}^2(\alpha) = 1 - \cos^2(\alpha)$. Além disso, se $\cos(\frac{\alpha}{3})$ for construtível a partir de $\{0, 1, \cos(\alpha)\}$, então $\text{sen}(\frac{\alpha}{3})$ também será construtível. Então, poderemos trissectar o ângulo α se, e só se, $\cos(\frac{\alpha}{3})$ é construtível a partir de $\{0, 1, \cos(\alpha)\}$.

Pela fórmula do arco triplo, obtemos:

$$\begin{aligned} & \cos(\alpha) = 4\cos^3\left(\frac{\alpha}{3}\right) - 3\cos\left(\frac{\alpha}{3}\right) \\ \Leftrightarrow \quad & 2\cos(\alpha) = 8\cos^3\left(\frac{\alpha}{3}\right) - 6\cos\left(\frac{\alpha}{3}\right) \\ \Leftrightarrow \quad & 8\cos^3\left(\frac{\alpha}{3}\right) - 6\cos\left(\frac{\alpha}{3}\right) - 2\cos(\alpha) = 0 \\ \Leftrightarrow \quad & \left(2\cos\left(\frac{\alpha}{3}\right)\right)^3 - 3\left(2\cos\left(\frac{\alpha}{3}\right)\right) - 2\cos(\alpha) = 0. \end{aligned}$$

Logo, $2\cos(\frac{\alpha}{3})$ é raiz do polinômio $p(x) = x^3 - 3x - 2\cos(\alpha)$. Com isso, podemos enunciar o seguinte teorema:

Teorema 3.68 (Trissecção do ângulo)**.** *Seja $\alpha \in \mathbb{R}$. O número $\cos(\frac{\alpha}{3})$ é construtível a partir de $\{0, 1, \cos(\alpha)\}$ se, e somente se, o polinômio $p(x) = x^3 - 3x - 2\cos(\alpha)$ é redutível sobre $\mathbb{Q}(\cos(\alpha))$.*

Demonstração.

($\Rightarrow$) Se o polinômio $p(x) = x^3 - 3x - 2\cos(\alpha)$ é irredutível sobre $\mathbb{Q}(\cos(\alpha))$, então $[\mathbb{Q}(\cos(\alpha), \cos(\frac{\alpha}{3})) : \mathbb{Q}(\cos(\alpha))] = 3$. Pelo Corolário 3.65, concluímos que $\cos(\frac{\alpha}{3})$ não é construtível.

($\Leftarrow$) Se o polinômio $p(x) = x^3 - 3x - 2\cos(\alpha)$ é redutível sobre $\mathbb{Q}(\cos(\alpha))$, então $p = qr$ para polinômios não constantes $q, r \in \mathbb{Q}(\cos(\alpha))[x]$, onde $\partial(q) = 1$ e $\partial(r) = 2$. Logo, p possui raiz em $\mathbb{Q}(\cos(\alpha))$ e, como $\partial(q)$ e $\partial(r)$ são potências de 2, isto implica que todas raízes de p são construtíveis. □

Exemplos 3.69.

1. O ângulo $\dfrac{\pi}{3}$ é construtível com régua e compasso.

   Solução.

   Temos:

   $$p(x) = x^3 - 3x - 2\cos(\pi) = x^3 - 3x + 2 = (x-1)^2(x+2).$$

   Então p é redutível sobre $\mathbb{Q}(\cos(\frac{\pi}{3}))$, o que implica que $\cos(\frac{\pi}{3})$ é construtível. □

2. O ângulo $\dfrac{\pi}{9}$ não é construtível com régua e compasso.

   Solução.

   Como $\cos(\frac{\pi}{3}) = \frac{1}{2}$, é suficiente provar que o polinômio $p(x) = x^3 - 3x - 1$ é irredutível sobre $\mathbb{Q}$. Utilizando o Teorema 2.47 (critério redução módulo 2), concluímos que de fato p é irredutível sobre $\mathbb{Q}$, o que implica que $\cos(\frac{\pi}{9})$ não é construtível. □

Capítulo 4

Teoria de Picard-Vessiot

A Teoria de Picard-Vessiot teve início com Émile Picard e Ernest Vessiot no final do século XIX e tem como objetivo estudar extensões de corpos diferenciais geradas pelas soluções de equações diferenciais lineares.

Neste capítulo iremos fazer uma breve introdução da Teoria de Picard-Vessiot e abordar uma aplicação interessante desta teoria: a caracterização das funções que possuem primitiva elementar.

4.1 Corpos diferenciais

Definição 4.1. Seja A um anel. Uma **derivação** em A é um homomorfismo de grupos abelianos $D : A \to A$ que satisfaz a relação $D(ab) = aD(b) + bD(a),\ \forall\ a, b \in A$. Um **anel diferencial** é um anel munido de uma derivação. Quando o anel é um corpo, chamamos de **corpo diferencial**.

Observação 4. É comum denotar $a' = D(a)$, $a'' = D(D(a))$, e $\forall\ n \in \mathbb{N}$, $a^{(n)} = D^n(a)$.

Exemplos 4.2.

1. Qualquer anel A munido com a derivação $D(a) = 0\ \forall a \in A$ é um anel diferencial.

2. O anel das funções de classe C^∞ definidas no intervalo $I \subseteq \mathbb{R}$, munido com a derivação usual de funções $D(f) = f'$ é um anel diferencial.

3. O anel das funções reais analíticas definidas em um intervalo de $\mathbb{R}$, munido com a derivação usual, é um anel diferencial.

4. O anel das funções holomorfas tomadas em um aberto de $\mathbb{C}$, munido com a derivação usual $D(f) = f'$, é um anel diferencial.

5. O anel $K[x]$ dos polinômios em uma variável x e coeficientes no corpo K, munido com a derivação usual, é um anel diferencial.

6. O corpo $K(x)$ de todas as funções racionais em uma variável x e coeficientes no corpo K, munido com a derivação usual de funções racionais, é um corpo diferencial.

7. O corpo de funções meromorfas em um subconjunto aberto e conexo de $\mathbb{C}$, munido com a derivação usual, é um corpo diferencial.

Proposição 4.3. *Seja A um anel diferencial munido com a derivação D. Sejam $a, b \in A$. Então:*

(a) $D(1) = 0$.

(b) Para qualquer inteiro $n \geq 1$, $D(a^n) = na^{n-1}D(a)$.

(c) Para qualquer inteiro $n \geq 1$, $D^n(ab) = \sum_{k=0}^{n} \binom{n}{k} D^k(a)D^{n-k}(b)$.

(d) Se b é invertível, então $D\left(\frac{a}{b}\right) = \frac{bD(a)-aD(b)}{b^2}$. *Em particular,* $D\left(\frac{1}{b}\right) = -\frac{D(b)}{b^2}$.

Demonstração.

(a) Aplicamos a derivação D em ambos os lados da igualdade $1 \cdot 1 = 1$. Temos:

$$\begin{aligned} & D(1 \cdot 1) = D(1) \\ \Leftrightarrow \quad & 1 \cdot D(1) + 1 \cdot D(1) = D(1) \\ \Leftrightarrow \quad & 2D(1) = D(1) \\ \Leftrightarrow \quad & D(1) = 0. \end{aligned}$$

(b) Vamos provar esta igualdade por indução em n. Para o caso base $n = 1$, temos:

$$1 \cdot a^{1-1} \cdot D(a) = a^0 D(a) = D(a^1).$$

Tomamos como hipótese de indução a seguinte igualdade:

$$D(a^k) = ka^{k-1}D(a), \ k \in \mathbb{N}^*.$$

Vamos mostrar que a igualdade continua satisfeita para $k + 1$:

$$\begin{aligned} D(a^{k+1}) &= D(a^k \cdot a) \\ &= a^k D(a) + aD(a^k) \\ &= a^k D(a) + a[ka^{k-1}D(a)] \\ &= a^k D(a) + ka^k D(a) \\ &= (k+1)a^k D(a). \end{aligned}$$

Logo, provamos por indução que para qualquer inteiro $n \geq 1$, $D(a^n) = na^{n-1}D(a)$.

(c) Novamente, vamos provar esta igualdade por indução em n. Para o caso base $n = 1$, temos:

$$\binom{1}{0} D^0(a)D^{1-0}(b) + \binom{1}{1} D^1(a)D^{1-1}(b) = aD(b) + bD(a) = D(ab) = D^1(ab).$$

Tomamos como hipótese de indução a seguinte igualdade:

$$D^n(ab) = \sum_{k=0}^{n} \binom{n}{k} D^k(a)D^{n-k}(b),\ n \in \mathbb{N}^*.$$

Vamos mostrar que a igualdade continua satisfeita para $n + 1$:

$$\begin{aligned}
D^{n+1}(ab) &= D(D^n(ab)) \\
&= D\left(\sum_{k=0}^{n} \binom{n}{k} D^k(a)D^{n-k}(b)\right) \\
&= \sum_{k=0}^{n} \binom{n}{k} D(D^k(a)D^{n-k}(b)) \\
&= \sum_{k=0}^{n} \binom{n}{k} (D^k(a)D^{n-k+1}(b) + D^{n-k}(b)D^{k+1}(a)) \\
&= \sum_{k=0}^{n} \binom{n}{k} D^k(a)D^{n-k+1}(b) + \sum_{k=0}^{n} \binom{n}{k} D^{k+1}(a)D^{n-k}(b) \\
&= \sum_{k=0}^{n} \binom{n}{k} D^k(a)D^{n-k+1}(b) + \sum_{k=1}^{n+1} \binom{n}{k-1} D^k(a)D^{n-k+1}(b) \\
&\overset{(*)}{=} \sum_{k=0}^{n+1} \binom{n+1}{k} D^k(a)D^{n-k+1}(b).
\end{aligned}$$

No passo $(*)$ foi utilizada a relação de Stifel: $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k},\ n \geq 1,\ k \geq 1$. Logo, provamos por indução que para qualquer inteiro $n \geq 1$, temos

$$D^n(ab) = \sum_{k=0}^{n} \binom{n}{k} D^k(a)D^{n-k}(b).$$

(d) Seja b invertível de forma que $\dfrac{ba}{b} = a$. Aplicando a derivação D em ambos os lados

desta igualdade, temos:

$$\begin{aligned} & D\left(\frac{ba}{a}\right) = D(a) \\ \Leftrightarrow \quad & D(b)\frac{a}{b} + bD\left(\frac{a}{b}\right) = D(a) \\ \Leftrightarrow \quad & bD\left(\frac{a}{b}\right) = D(a) - D(b)\frac{a}{b} \\ \Leftrightarrow \quad & D\left(\frac{a}{b}\right) = \frac{D(a)}{b} - \frac{D(b)a}{b^2} = \frac{bD(a) - D(b)a}{b^2}. \end{aligned}$$

Em particular,

$$D\left(\frac{1}{b}\right) = \frac{b \cdot D(1) - D(b) \cdot 1}{b^2} = -\frac{D(b)}{b^2}.$$

□

Definição 4.4. Um elemento de um anel diferencial é dito **constante** se sua derivada for nula. Se A é um anel diferencial, então $C_A = \{a \in A : a' = 0\}$ é o **conjunto dos elementos constantes** de A.

Proposição 4.5. *Seja A um anel diferencial. O conjunto C_A dos elementos constantes de A é um subanel de A. Se A é um corpo diferencial, então o conjunto C_A é um subcorpo de A, chamado de* ***corpo constante*** *de A.*

Demonstração.

Seja A um anel diferencial munido com a derivação D. Seja $a, b \in C_A$. Então $D(a) = D(b) = 0$. Note que $D(a+b) = D(a) + D(b) = 0 + 0 = 0$. Logo, $a + b \in C_A$. Da mesma forma, $D(ab) = aD(b) + bD(a) = a \cdot 0 + b \cdot 0 = 0$. Logo, $ab \in C_A$. Como $D(1) = 0$, então $1 \in C_A$. Portanto, C_A é subanel de A.

Caso A seja corpo diferencial, então para provar que C_A é subcorpo de A, basta provar que se $a, b \in C_A$ com $a \neq 0, b \neq 0$, então $ab^{-1} \in C_A$. Temos:

$$D(ab^{-1}) = aD(b^{-1}) + b^{-1}D(a) = aD\left(\frac{1}{b}\right) = a\left(-\frac{D(b)}{b^2}\right) = a \cdot 0 = 0.$$

Portanto, $ab^{-1} \in C_A$ e segue que C_A é subcorpo de A. □

Proposição 4.6. *Seja K um corpo de característica zero. Considere o anel diferencial $K[x]$ e o corpo diferencial $K(x)$, ambos munidos com a derivação usual. Então, $C_{K[x]} = C_{K(x)} = K$.*

Demonstração.

Seja $f \in K[x]$ tal que $f = \sum_{k=1}^{n} a_k x^k$. Então, $f' = \sum_{k=1}^{n} k a_k x^{k-1}$. Assuma que $f' = 0$. Então $ka_k = 0, \ \forall\, k \geq 1$, o que implica que $a_k = 0, \ \forall\, k \geq 1$. Logo, $f = a_0 \in K$ e, portanto, $C_{K[x]} = K$.

Considere agora $r \in K(x)$ tal que $r' = 0$. Seja $r = \dfrac{p}{q}$, onde $p, q \in K[x]$, $q \neq 0$ e $\text{mdc}(p, q) = 1$. Então

$$qr = p \Rightarrow (qr)' = p' \Rightarrow q'r + qr' = p' \Rightarrow q'r = p' \Rightarrow q'\frac{p}{q} = p' \in K[x].$$

Suponha, por absurdo, que $\partial q \geq 1$. Como $\text{mdc}(p, q) = 1$, então sabemos que $q \nmid p$ e, portanto, necessariamente $q \mid q'$. Mas como $\partial q' < \partial q$, então $\dfrac{q'}{q} \notin K[x]$, o que implica que $p' \notin K[x]$. Contradição! Portanto, q é constante. Logo, $q' = 0$ o que implica que $p' = 0$. Segue que p é constante também e portanto $r = \dfrac{p}{q}$ é constante. Concluímos que $C_{K(x)} = K$. □

Definição 4.7. Sejam A um anel diferencial e I um ideal de A. Então I é um **ideal diferencial** de A se $a' \in I, \forall\, a \in I$.

Definição 4.8. Um **homomorfismo diferencial** $f : A \to B$ de anéis diferenciais é um homomorfismo de anéis $f : A \to B$ tal que $f(a') = f(a)',\ \forall\, a \in A$.

Proposição 4.9. *Seja $f : A \to B$ um homomorfismo diferencial de anéis. Então* $\ker(f)$ *é um ideal diferencial de A e o isomorfismo $\overline{f} : A/\ker(f) \to \text{Im}(f)$ é um isomorfismo diferencial.*

Demonstração.

Seja $a \in \ker(f)$. Então $f(a') = f(a)' = (0)' = 0$, o que implica que $a' \in \ker(f)$ e, portanto, $\ker(f)$ é um ideal diferencial.

Dado $a \in A$ arbitrário, temos $\overline{f}(\overline{a})' = f(a)' = f(a') = \overline{f}(\overline{a'}) = \overline{f}(\overline{a}')$. Logo, $\overline{f}$ é um isomorfismo diferencial. □

Proposição 4.10. *Sejam A um anel diferencial e I um ideal diferencial de A. Então existe uma única derivação do anel quociente A/I tal que a projeção canônica $\pi : A \to A/I$ é um homomorfismo diferencial.*

Demonstração.

Considere que o anel A está munido da derivação D. Como D e π são homomorfismos de grupos, então a composta $\pi \circ D : A \to A/I$ também é homomorfismo de grupos. Como I é ideal diferencial de A, então $D(I) \subseteq I$. Portanto, se $a \in I$, então $(\pi \circ D)(a) = \pi(D(a)) = \overline{D(a)} = \overline{0}$. Defina a aplicação $\overline{D} : A/I \to A/I$ dada por $\overline{D}(\overline{a}) = \pi(D(a))$. Vamos mostrar que $\overline{D}$ está bem definida, ou seja, dados $a_1, a_2 \in A/I$ tais que $\overline{a_1} = \overline{a_2}$,

então $\overline{D}(\overline{a_1}) = \overline{D}(\overline{a_2})$. Note que $\overline{a_1} = \overline{a_2}$ implica que $a_1 - a_2 \in I$. Temos:

$$\begin{aligned}
& \overline{D}(\overline{a_1 - a_2}) = \overline{0} \\
\Leftrightarrow \quad & \pi(D(a_1 - a_2)) = \overline{0} \\
\Leftrightarrow \quad & \pi(D(a_1) - D(a_2)) = \overline{0} \\
\Leftrightarrow \quad & \pi(D(a_1)) - \pi(D(a_2)) = \overline{0} \\
\Leftrightarrow \quad & \pi(D(a_1)) = \pi(D(a_2)) \\
\Leftrightarrow \quad & \overline{D}(\overline{a_1}) = \overline{D}(\overline{a_2}).
\end{aligned}$$

Logo, $\overline{D}$ está bem definida. Mostraremos agora que $\overline{D}$ define uma derivação em A/I. Temos:

$$\begin{aligned}
\overline{D}(\overline{a_1 + a_2}) &= \pi(D(a_1 + a_2)) \\
&= \pi(D(a_1) + D(a_2)) \\
&= \pi(D(a_1)) + \pi(D(a_2)) \\
&= \overline{D}(\overline{a_1}) + \overline{D}(\overline{a_2}). \\
\overline{D}(\overline{a_1 a_2}) &= \pi(D(a_1 a_2)) \\
&= \pi(a_1 D(a_2) + a_2 D(a_1)) \\
&= \pi(a_1)\pi(D(a_2)) + \pi(a_2)\pi(D(a_1)) \\
&= \overline{a_1}\,\overline{D}(\overline{a_2}) + \overline{a_2}\,\overline{D}(\overline{a_1}).
\end{aligned}$$

Portanto, $\overline{D}$ define uma derivação em A/I. Considere as derivações $\overline{D}$ e $\widetilde{D}$ de forma que o diagrama abaixo seja comutativo.

$$\begin{array}{ccc}
A & \xrightarrow{D} & A \\
{\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\
A/I & \xrightarrow{\overline{D},\,\widetilde{D}} & A/I
\end{array}$$

Então $\widetilde{D}(\pi(a)) = \overline{D}(\pi(a)) = \pi(D(a)) \Rightarrow \widetilde{D}(\widetilde{a}) = \overline{D}(\overline{a})$, $\forall\, a \in A \Rightarrow \widetilde{D} = \overline{D}$. Isto prova a unicidade de $\overline{D}$ e completa a demonstração. □

Proposição 4.11. *Seja A um anel diferencial. Assuma que A é domínio de integridade e seja $K = \operatorname{Frac} A$. Então existe uma única derivação D em K que coincide com a derivação de A.*

Demonstração.

Para $a, b \in A$, temos $\left(\dfrac{a}{b}\right)' = \dfrac{a'b - ab'}{b^2}$. Para $\dfrac{a}{b} \in K$, defina $D\left(\dfrac{a}{b}\right) = \dfrac{a'b - ab'}{b^2}$, e

então há unicidade. Vamos verificar que esta fórmula não depende da escolha do representante e que define uma derivação em K. Para qualquer $c \in A^*$, temos:

$$\begin{aligned} D\left(\frac{ac}{bc}\right) &= \frac{(ac)'bc - ac(bc)'}{(bc)^2} \\ &= \frac{(a'c + ac')bc - ac(b'c + bc')}{b^2c^2} \\ &= \frac{a'bc^2 + abcc' - ab'c^2 - abcc'}{b^2c^2} \\ &= \frac{a'b - ab'}{b^2} \\ &= D\left(\frac{a}{b}\right). \end{aligned}$$

Logo, a derivação de $\frac{a}{b} \in K$ é independente da escolha do representante. Agora, dados $\frac{a}{b}, \frac{c}{d} \in K$ temos:

$$\begin{aligned} D\left(\frac{a}{b} + \frac{c}{d}\right) &= D\left(\frac{ad + bc}{bd}\right) \\ &= \frac{(ad + bc)'bd - (ad + bc)(bd)'}{(bd)^2} \\ &= \frac{(a'd + ad' + b'c + bc')bd - (ad + bc)(b'd + bd')}{b^2d^2} \\ &= \frac{a'bd^2 + abdd' + bb'cd + b^2c'd - ab'd^2 - abdd' - bb'cd - b^2cd'}{b^2d^2} \\ &= \frac{a'b - ab'}{b^2} + \frac{c'd - cd'}{d^2} \\ &= D\left(\frac{a}{b}\right) + D\left(\frac{c}{d}\right). \\ D\left(\frac{a}{b} \cdot \frac{c}{d}\right) &= D\left(\frac{ac}{bd}\right) \\ &= \frac{(ac)'bd - ac(bd)'}{(bd)^2} \\ &= \frac{(a'c + ac')bd - ac(b'd + bd')}{b^2d^2} \\ &= \frac{a'bcd + abc'd - ab'cd - abcd'}{b^2d^2} \\ &= \frac{(a'b - ab')cd + (c'd - cd')ab}{b^2d^2} \\ &= \frac{(a'b - ab')c}{b^2d} + \frac{(c'd - cd')a}{bd^2} \\ &= \left(\frac{a'b - ab'}{b^2}\right) \cdot \left(\frac{c}{d}\right) + \left(\frac{c'd - cd'}{d^2}\right) \cdot \left(\frac{a}{b}\right) \\ &= D\left(\frac{a}{b}\right) \cdot \left(\frac{c}{d}\right) + D\left(\frac{c}{d}\right) \cdot \left(\frac{a}{b}\right). \end{aligned}$$

Isto mostra que de fato, $D\left(\frac{a}{b}\right) = \frac{a'b - ab'}{b^2}$ define uma derivação em K. □

4.2 Extensões diferenciais

Definição 4.12. Uma extensão de corpos $L : K$ é dita **extensão diferencial de corpos** se a restrição da derivação de L em K for igual à derivação de K.

Teorema 4.13. *Sejam K um corpo diferencial e $L : K$ uma extensão algébrica finita separável. Então a derivação de K se estende de forma única para L. Além disso, todo K-automorfismo de L é diferencial.*

Demonstração.

Se $L : K$ é uma extensão finita, então $L = K(\alpha)$ para algum $\alpha \in L$, pelo Teorema 3.35 (Teorema do Elemento Primitivo). Seja $p(x) = \sum_{j=0}^{n} a_j x^j$ o polinômio minimal de α sobre K. Então $L \cong K[x]/\langle p \rangle$. Suponha que existe uma derivação D_L em L que estende a derivação D de K. Se aplicarmos a derivação D_L em $p(\alpha) = 0$, temos:

$$\begin{aligned} D_L(p(\alpha)) &= D_L\left(\sum_{j=0}^{n} a_j \alpha^j\right) \\ &= \sum_{j=0}^{n} (D(a_j)\alpha^j + j a_j \alpha^{j-1} D_L(\alpha)) \\ &= \left(\sum_{j=0}^{n} D(a_j)\alpha^j\right) + \left(\sum_{j=0}^{n} j a_j \alpha^{j-1}\right) D_L(\alpha) \\ &= p^D(\alpha) + p'(\alpha) D_L(\alpha) \\ &= 0. \end{aligned}$$

Denotamos por p^D o polinômio obtido ao aplicar D nos coeficientes de p.

Como $\partial(p') < \partial(p)$ e p é separável, então $p' \neq 0$. Logo $p'(\alpha) \neq 0$, pois p é o polinômio minimal de α. Então $D_L(\alpha) = -\dfrac{p^D(\alpha)}{p'(\alpha)}$, o que implica que a derivação de K se estende de forma única para L.

Para mostrar que tal derivação de fato existe, utilizaremos a Proposição 4.10. Precisamos mostrar que existe uma derivação em $K[x]$ tal que o ideal $\langle p \rangle$ é diferencial. Como p é separável, então p e p' são coprimos. Com isso, podemos estender a derivação de K para $K[x]$ da seguinte forma: $\overline{D}(x) = -p^D(x)h(x)$ para $h(x) \in K[x]$ tal que

$h(x)p'(x) \equiv 1 (\mathrm{mod}\, p(x))$. Dado $q(x) \in K[x]$ tal que $h(x)p'(x) = 1 + q(x)p(x)$, temos:

$$\begin{aligned}\overline{D}(p(x)) &= p^D(x) + p'(x)\overline{D}(x)\\ &= p^D(x) + p'(x)(-p^D(x)h(x))\\ &= p^D(x)(1 - p'(x)h(x))\\ &= p^D(x)(1 - 1 - q(x)p(x))\\ &= -p^D(x)q(x)p(x).\end{aligned}$$

Portanto, $\langle p \rangle$ é um ideal diferencial de $K[x]$ e segue que $L \cong K[x]/\langle p \rangle$ é um corpo diferencial.

Se σ é um K-automorfismo de L, então $\sigma^{-1}D_L\sigma$ é também uma derivação de L que estende a derivação de K. Como a derivação é única, então $\sigma^{-1}D_L\sigma = D_L$, e portanto, $D_L\sigma = \sigma D_L$, o que prova que σ é um automorfismo diferencial. □

O teorema acima também é válido se assumirmos a extensão $L : K$ não finita.

4.3 Equações diferenciais lineares homogêneas

Seja K um corpo diferencial. Uma equação diferencial linear homogênea de ordem n sobre K é da forma:

$$\mathcal{L}(y) = y^{(n)} + a_{(n-1)}y^{(n-1)} + \cdots + a_2y'' + a_1y' + a_0y = 0,\ a_i \in K.$$

Toda equação diferencial linear homogênea de ordem n sobre K pode ser representada também como uma equação diferencial matricial de primeira ordem da forma:

$$Y' = AY,\ A \in \mathrm{GL}_n(K).$$

Então f é solução da equação $\mathcal{L}(y) = 0$ se, e somente se, $(f, f', \ldots, f^{(n-2)}, f^{(n-1)})^T$ satisfaz a equação $Y' = AY$, ou seja,

$$\begin{pmatrix} f \\ f' \\ \vdots \\ f^{(n-2)} \\ f^{(n-1)} \end{pmatrix}' = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-1} \end{pmatrix} \begin{pmatrix} f \\ f' \\ \vdots \\ f^{(n-2)} \\ f^{(n-1)} \end{pmatrix}$$

Vamos definir uma estrutura para o conjunto de soluções da equação $\mathcal{L}(y) = 0$.

Lema 4.14. *Seja K um corpo diferencial munido da derivação D. Então $D : K \to K$ é um operador linear sobre C_K.*

Demonstração.

Dados $a \in C_K$ e $f, g \in K$, temos

$$D(af+g) = D(af) + D(g) = aD(f) + f\underbrace{D(a)}_{=0} + D(g) = aD(f) + D(g).$$

Portanto D é um operador linear sobre C_K. □

Lema 4.15. *Sejam K um corpo diferencial e $Y_1, \ldots, Y_m$ soluções de $Y' = AY$, $A \in GL_n(K)$. Se $\{Y_1, \ldots, Y_m\}$ é linearmente independente sobre C_K, então $\{Y_1, \ldots, Y_m\}$ também é linearmente independente sobre K.*

Demonstração.

Vamos provar por indução em m.

Para o caso base $m = 1$, suponha que $\{Y_1\}$ é linearmente independente sobre C_K. Então $Y_1 \neq 0$. Logo $\{Y_1\}$ é linearmente independente sobre K.

Pela hipótese de indução, assumiremos que $\{Y_1, \ldots, Y_{m-1}\}$ é linearmente independente sobre K.

Considere a equação $\sum_{j=1}^{m} a_j Y_j = 0$, $a_j \in K$, $a_m \neq 0$. Como K é corpo, podemos assumir $a_m = 1$. Derivando a equação, temos:

$$\begin{aligned}
& \left(\sum_{j=1}^{m} a_j Y_j\right)' = 0 \\
\Rightarrow \quad & (a_1'Y_1 + a_1Y_1') + (a_2'Y_2 + a_2Y_2') + \cdots + (a_{m-1}'Y_{m-1} + a_{m-1}Y_{m-1}') + Y_m' = 0 \\
\Rightarrow \quad & (a_1'Y_1 + a_2'Y_2 + \cdots + a_{m-1}'Y_{m-1}) + (a_1Y_1' + a_2Y_2' + \cdots + a_{m-1}Y_{m-1}' + Y_m') = 0 \\
\Rightarrow \quad & (a_1'Y_1 + a_2'Y_2 + \cdots + a_{m-1}'Y_{m-1}) + A\underbrace{(a_1Y_1 + a_2Y_2 + \cdots + a_{m-1}Y_{m-1} + Y_m)}_{=0} = 0 \\
\Rightarrow \quad & \sum_{j=1}^{m-1} a_j'Y_j = 0 \\
\overset{(*)}{\Rightarrow} \quad & a_j' = 0.
\end{aligned}$$

No passo $(*)$ utilizamos a hipótese de indução. Logo, $a_1, \ldots, a_{m-1} \in C_K$ e segue que $\{f_1, \ldots, f_m\}$ é linearmente dependente sobre C_K, o que é contradição.

Portanto, $\{f_1, \ldots, f_m\}$ é linearmente independente sobre K. □

Proposição 4.16. *Sejam K um corpo diferencial e $\mathcal{L}(y) = 0$ uma equação diferencial linear homogênea de ordem n sobre K. O conjunto $V_{\mathcal{L}} = \{f \in K : \mathcal{L}(f) = 0\}$ é um espaço vetorial sobre C_K de dimensão menor ou igual a n.*

Demonstração.

Note que mostrar que $V_{\mathcal{L}}$ é um espaço vetorial sobre C_K de dimensão menor ou igual a n é equivalente a mostrar que o conjunto V de soluções $Y \in K^n$ da equação diferencial $Y' = AY$, $A \in \mathrm{GL}_n(K)$ é um espaço vetorial sobre C_K de dimensão menor ou igual a n.

Seja D a derivação de K. Pelo Lema 4.14, a derivação D é um operador linear sobre C_K. Então a aplicação $\varphi : K^n \to K^n$ dada por $\varphi(Y) = Y' - AY$ é linear sobre C_K e, portanto, $\ker(\varphi)$ é um espaço vetorial sobre C_K. Note que $\ker(\varphi) = V$, pois é o conjunto de soluções de $Y' = AY$.

Falta agora mostrar que $\dim_{C_K}(V) \leq n$. Sejam $Y_1, Y_2, \ldots, Y_n, Y_{n+1} \in V$. Claramente $\{Y_1, \ldots, Y_{n+1}\}$ é linearmente dependente sobre K, pois $\dim_K(K^n) = n$. Então, pelo Lema 4.15, segue que $\{Y_1, \ldots, Y_{n+1}\}$ é linearmente dependente sobre C_K. Logo, $\dim_{C_K}(V) \leq n$. □

Definição 4.17. Seja K um corpo diferencial. O **Wronskiano** de n elementos $f_1, \ldots, f_n \in K$ é dado pelo determinante da **matriz wronskiana**:

$$\mathcal{W}(f_1, \ldots, f_n) = \det \begin{pmatrix} f_1 & f_2 & \cdots & f_n \\ f_1' & f_2' & \cdots & f_n' \\ \vdots & \vdots & & \vdots \\ f_1^{(n-1)} & f_2^{(n-1)} & \cdots & f_n^{(n-1)} \end{pmatrix}.$$

Proposição 4.18. *Seja K um corpo diferencial. Os elementos $f_1, \ldots, f_n \in K$ são linearmente dependentes sobre C_K se, e somente se, $\mathcal{W}(f_1, \ldots, f_n) = 0$.*

Demonstração.

($\Rightarrow$) Seja D a derivação de K. Pelo Lema 4.14, a derivação D é um operador linear sobre C_K.

Note que se $\{f_1, \ldots, f_n\}$ é linearmente dependente sobre C_K, então as colunas da matriz wronskiana de $f_1, \ldots, f_n$ também são linearmente dependentes sobre C_K, pois a derivação D é um operador linear sobre C_K. Então, $\mathcal{W}(f_1, \ldots, f_n) = 0$.

($\Leftarrow$) Vamos mostrar por indução em n. Para $n = 1$ é trivial. Assuma que $\mathcal{W}(f_1, \ldots, f_n) = 0$. Se $\mathcal{W}(f_2, \ldots, f_n) = 0$, nossa hipótese de indução garante que $\{f_2, \ldots, f_n\}$ é linearmente dependente sobre C_K. Assuma que $\mathcal{W}(f_2, \ldots, f_n) \neq 0$. Como $\mathcal{W}(f_1, \ldots, f_n) = 0$, então as colunas da matriz wronskiana de $f_1, \ldots, f_n$ satisfazem uma relação de dependência linear não trivial com coeficientes em K, digamos

$$\sum_{j=1}^{n} a_j f_j^{(k)} = 0,\ 0 \leq k \leq n-1,\ a_j \in K. \quad (*)$$

Como $\mathcal{W}(f_2, \ldots, f_n) \neq 0$, então $a_1 \neq 0$ e podemos assumir, sem perda de generalidade,

que $a_1 = 1$, pois K é corpo. Derivando a equação $(*)$, temos:

$$\begin{aligned}
& \left(\sum_{j=1}^{n} a_j f_j^{(k)}\right)' = 0 \\
\Rightarrow \quad & f_1^{(k+1)} + (a_2 f_2^{(k+1)} + a_2' f_2^{(k)}) + \cdots + (a_n f_n^{(k+1)} + a_n' f_n^{(k)}) = 0 \\
\Rightarrow \quad & \underbrace{(f_1^{(k+1)} + a_2 f_2^{(k+1)} + \cdots + a_n f_n^{(k+1)})}_{= 0 \text{ por } (*)} + (a_2' f_2^{(k)} + \cdots + a_n' f_n^{(k)}) = 0 \\
\Rightarrow \quad & \sum_{j=2}^{n} a_j' f_j^{(k)} = 0.
\end{aligned}$$

Obtemos então um sistema linear homogêneo de equações em $a_2', \ldots, a_n'$ com determinante $\mathcal{W}(f_2, \ldots, f_n) \neq 0$, o que implica que $a_2' = a_3' = \cdots = a_n' = 0$. Portanto, $a_2, a_3, \ldots, a_n \in C_K$. Como $a_1 = 1$, então $a_j \in C_K$, $1 \leq j \leq n$. Logo, $\{f_1, \ldots, f_n\}$ é linearmente dependente sobre C_K. □

Exemplos 4.19. Vamos verificar se os conjuntos a seguir são linearmente independentes sobre $\mathbb{C}$ utilizando o Wronskiano.

1. $\{1, x^3\}$, $K = \mathbb{C}(x)$

   Solução.

   Calculando o Wronskiano de $\{1, x^3\}$, temos:

   $$\mathcal{W}(1, x^3) = \begin{vmatrix} 1 & x^3 \\ 0 & 3x^2 \end{vmatrix} = 3x^2 \neq 0.$$

   Logo $\{1, x^3\}$ é um conjunto linearmente independente sobre $\mathbb{C}$. □

2. $\{x^2 + 1, x^2, 1\}$, $K = \mathbb{C}(x)$

   Solução.

   Calculando o Wronskiano de $\{x^2 + 1, x^2, 1\}$, temos:

   $$\mathcal{W}(x^2 + 1, x^2, 1) = \begin{vmatrix} x^2 + 1 & x^2 & 1 \\ 2x & 2x & 0 \\ 2 & 2 & 0 \end{vmatrix} = 4x - 4x = 0.$$

   Logo $\{x^2 + 1, x^2, 1\}$ é um conjunto linearmente dependente sobre $\mathbb{C}$. □

3. $\{\text{sen}(2x), \cos(x)\,\text{sen}(x)\}$, $K = \mathbb{C}(x, \cos x, \text{sen}\, x)$

Solução.

Como $\text{sen}(2x) = 2\cos(x)\,\text{sen}(x)$, é fácil ver que $\{\text{sen}(2x), \cos(x)\,\text{sen}(x)\}$ é linearmente dependente sobre $\mathbb{C}$. Veja abaixo que o Wronskiano de $\{\text{sen}(2x), \cos(x)\,\text{sen}(x)\}$ se anula.

$$\begin{aligned}\mathcal{W}(\text{sen}(2x), \cos(x)\,\text{sen}(x)) &= \begin{vmatrix} \text{sen}(2x) & \cos(x)\,\text{sen}(x) \\ 2\cos(2x) & \cos^2(x) - \text{sen}^2(x) \end{vmatrix} \\ &= \text{sen}(2x)(\cos^2(x) - \text{sen}^2(x)) - 2\cos(2x)\cos(x)\,\text{sen}(x) \\ &= \text{sen}(2x)\cos(2x) - \cos(2x)\,\text{sen}(2x) \\ &= 0.\end{aligned}$$

□

4.4 Extensões de Picard-Vessiot

Vimos na Teoria de Galois clássica que uma extensão de corpos $L : K$ é normal se, e só se, L é corpo de decomposição de um polinômio $f \in K[x]$. De maneira similar, construiremos uma extensão minimal de corpos diferenciais onde uma equação diferencial linear homogênea de ordem n admite n soluções linearmente independentes.

Definição 4.20. Sejam $L : K$ uma extensão diferencial e $f_1, \ldots, f_n \in L$ soluções linearmente independentes sobre C_K da equação diferencial linear $\mathcal{L}(y) = 0$ de ordem n. Então $\{f_1, \ldots, f_n\}$ é dito **conjunto fundamental de soluções** de $\mathcal{L}(y) = 0$ em L.

Definição 4.21. Seja $\mathcal{L}(y) = 0$ uma equação diferencial linear de ordem n com coeficientes em um corpo diferencial K. Então o menor corpo que contém tanto K quanto as soluções de $\mathcal{L}(y) = 0$ é denotado por $E_{\mathcal{L}}$ e é dito **corpo de decomposição diferencial** de $\mathcal{L}$.

Definição 4.22. Sejam $L : K$ uma extensão diferencial e $\mathcal{L}(y) = 0$ uma equação diferencial linear de ordem n sobre K. Assuma que C_K é algebricamente fechado de característica zero. Dizemos que a extensão $L : K$ é uma **extensão de Picard-Vessiot** de $\mathcal{L}(y) = 0$ se:

(a) $L = K(f_1, \ldots, f_n)$, onde $\{f_1, \ldots, f_n\}$ é um conjunto fundamental de soluções de $\mathcal{L}(y) = 0$ em L;

(b) O corpo constante de L é C_K, isto é, $C_L = C_K$.

Vejamos alguns exemplos.

Exemplos 4.23. Vamos determinar a extensão de Picard-Vessiot de $\mathcal{L}(y) = 0$ para cada item abaixo. A derivação em cada item é a usual.

1. $\mathcal{L}(y) = y' - \dfrac{1}{x}y$ com coeficientes em $\mathbb{C}(x)$

   Solução.

   As soluções de $\mathcal{L}(y) = 0$ são as funções $y(x) = cx$, com $c \in \mathbb{C}$. Logo $\{x\}$ é um conjunto fundamental de soluções de $\mathcal{L}(y) = 0$ em $E_{\mathcal{L}}$. Portanto $E_{\mathcal{L}} = \mathbb{C}(x)$, e segue que a extensão de Picard-Vessiot de $\mathcal{L}(y) = 0$ é $\mathbb{C}(x) : \mathbb{C}(x)$. □

2. $\mathcal{L}(y) = y'' - 2y$ com coeficientes em $\mathbb{C}(x)$

   Solução.

   As soluções de $\mathcal{L}(y) = 0$ são as funções $y(x) = c_1 e^{\sqrt{2}x} + c_2 e^{-\sqrt{2}x}$, com $c_1, c_2 \in \mathbb{C}$. Calculando o Wronskiano do conjunto $\{e^{\sqrt{2}x}, e^{-\sqrt{2}x}\}$, temos:

   $$\mathcal{W}(e^{\sqrt{2}x}, e^{-\sqrt{2}x}) = \begin{vmatrix} e^{\sqrt{2}x} & e^{-\sqrt{2}x} \\ \sqrt{2}e^{\sqrt{2}x} & -\sqrt{2}e^{-\sqrt{2}x} \end{vmatrix} = -2\sqrt{2} \neq 0.$$

   Logo $\{e^{\sqrt{2}x}, e^{-\sqrt{2}x}\}$ é um conjunto linearmente independente e, portanto, é um conjunto fundamental de soluções de $\mathcal{L}(y) = 0$ em $E_{\mathcal{L}}$.

   Portanto $E_{\mathcal{L}} = \mathbb{C}(x, e^{\sqrt{2}x}, e^{-\sqrt{2}x})$, e segue que a extensão de Picard-Vessiot de $\mathcal{L}(y) = 0$ é $\mathbb{C}(x, e^{\sqrt{2}x}, e^{-\sqrt{2}x}) : \mathbb{C}(x)$. □

O teorema a seguir garante que qualquer equação diferencial linear admite uma única extensão de Picard-Vessiot, a menos de K-isomorfismos diferenciais. A demonstração deste teorema não será abordada neste trabalho, mas pode ser encontrada em [3], Teorema 3.3.

Teorema 4.24. *Seja K um corpo diferencial, onde C_K é algebricamente fechado. Seja também $\mathcal{L}(y) = 0$ uma equação diferencial linear de ordem n definida sobre K. Então existe uma extensão de Picard-Vessiot $L : K$ para $\mathcal{L}(y) = 0$ que é única a menos de K-isomorfismo diferencial.*

Se C_K é algebricamente fechado, então a extensão de Picard-Vessiot $L : K$ de $\mathcal{L}(y) = 0$ pode ser construída da seguinte maneira:

1. Seja $\{f_1, \ldots, f_n\}$ o conjunto fundamental de soluções de $\mathcal{L}(y) = 0$. Defina os elementos $f_{ij} = f_j^{(i)}, 0 \leq i \leq n-1, 1 \leq j \leq n$.

2. Obtenha o anel de polinômios em n^2 indeterminadas $K[f_{ij}, 0 \leq i \leq n-1, 1 \leq j \leq n]$.

3. Considere o subconjunto S de $K[f_{ij}]$ tal que $(\mathcal{W}(f_1, \ldots, f_n))^n \in S$ para qualquer $n \geq 0$ inteiro. Defina o anel $R = S^{-1}K[f_{ij}] = \{ab^{-1} : a \in K[f_{ij}], b \in S\} \subseteq \text{Frac}(K[f_{ij}])$.

4. Como qualquer ideal diferencial maximal P de R é um ideal primo, então o quociente R/P é um domínio de integridade. Se $L = \text{Frac}(R/P)$, então $L : K$ é de Picard-Vessiot.

4.5 Grupos de Galois diferenciais

Vimos que na Teoria de Galois clássica podemos associar um grupo de Galois a uma extensão de corpos. Da mesma maneira, veremos que podemos associar um grupo de Galois diferencial a uma extensão diferencial de corpos.

Definição 4.25. O **grupo de Galois diferencial** de uma extensão diferencial de corpos $L : K$ é o grupo de todos os K-automorfismos diferenciais de L sob a operação de composição, isto é, o conjunto dos automorfismos $\sigma : L \to L$ tais que

1. para qualquer $x \in K$, temos que $\sigma(x) = x$.

2. para qualquer $y \in L$, temos que $\sigma(y)' = \sigma(y')$.

Denotamos este grupo por $\text{Gal}^D(L : K)$.

Lembre-se que na teoria clássica, vimos que uma extensão $L : K$ é galoisiana se $L^{\text{Gal}(L:K)} = \{x \in L : \sigma(x) = x, \forall \sigma \in \text{Gal}(L : K)\} = K$. Isto nos permite aproveitar todo o poder do Teorema Fundamental de Galois. Como iremos enunciar a versão diferencial análoga deste teorema, faz sentido verificar que o mesmo vale para extensões de Picard-Vessiot em frente a seu grupo de Galois diferencial. Para isso, necessitaremos do lema a seguir, cuja demonstração pode ser encontrada em [3], Proposição 3.7 (a).

Lema 4.26. *Se $L : K$ é uma extensão de Picard-Vessiot para a equação diferencial linear $\mathcal{L}(y) = 0$ e $x \in L \setminus K$, então existe um K-automorfismo diferencial $\sigma : L \to L$ tal que $\sigma(x) \neq x$.*

Teorema 4.27. *Sejam $L : K$ uma extensão de Picard-Vessiot e $Gal^D(L : K)$ o respectivo grupo de Galois diferencial. Então $L^{Gal^D(L:K)} = K$, isto é, K é o corpo fixado de $Gal^D(L : K)$.*

Demonstração.

É imediato da Definição 4.25 que $K \subseteq L^{\text{Gal}^D(L:K)}$. Para a inclusão reversa, considere $x \in L^{\text{Gal}^D(L:K)}$ e suponha, por absurdo, que $x \in L \setminus K$. Pelo Lema 4.26, existe um K-automorfismo diferencial $\sigma : L \to L$ tal que $\sigma(x) \neq x$, o que contradiz o fato de x pertencer à $L^{\text{Gal}^D(L:K)}$. Logo, $L^{\text{Gal}^D(L:K)} = K$. □

Vimos que na Teoria de Galois clássica a ação de um grupo de Galois no corpo de decomposição de um polinômio é determinada pela maneira que ele permuta as raízes (que é um conjunto finito de n elementos), já que as raízes geram o corpo de decomposição. Por isso, um grupo de Galois pode ser naturalmente identificado com um subgrupo de S_n.

Da mesma forma, a ação de um grupo de Galois diferencial de uma equação diferencial linear homogênea na extensão de Picard-Vessiot é determinada pela maneira que ele move as soluções fundamentais (que agora forma um espaço vetorial sobre C_K de dimensão n), já que as soluções fundamentais geram a extensão de Picard-Vessiot. Veremos agora que um grupo de Galois diferencial pode ser naturalmente identificado com um subgrupo de $\mathrm{GL}_n(C_K)$.

Proposição 4.28. *Sejam $L : K$ uma extensão de Picard-Vessiot da equação diferencial linear homogênea $\mathcal{L}(y) = 0$ de ordem n e $Gal^D(L : K)$ o respectivo grupo de Galois diferencial. O grupo $Gal^D(L : K)$ é isomorfo à algum subgrupo de $GL_n(C_K)$.*

Demonstração.

Sejam $\{f_1, \ldots, f_n\}$ o conjunto fundamental de soluções de $\mathcal{L}(y) = 0$ em L e $\sigma \in \mathrm{Gal}^D(L : K)$. Como σ é um K-automorfismo diferencial de L, então $\sigma(f_1), \ldots, \sigma(f_n)$ são soluções de $\mathcal{L}(y) = 0$. Como $\{f_1, \ldots, f_n\}$ é uma base para o espaço vetorial das soluções de $\mathcal{L}(y) = 0$, então temos

$$\sigma(f_j) = \sum_{i=1}^{n} c_{ij} f_i,\ 1 \leq j \leq n,\ c_{ij} \in C_K.$$

Defina a aplicação $\phi : \mathrm{Gal}^D(L : K) \to \mathrm{GL}_n(C_K)$ dada por $\phi(\sigma) = (c_{ij})$. Vamos mostrar que ϕ é um homomorfismo de grupos injetivo.

Seja $\sigma_1, \sigma_2 \in \mathrm{Gal}^D(L : K)$ tais que $\sigma_1(f_j) = \sum_{i=1}^{n} c_{ij} f_i$ e $\sigma_2(f_j) = \sum_{i=1}^{n} d_{ij} f_i$, onde $1 \leq j \leq n$. Então:

$$\begin{aligned}
(\sigma_1 \circ \sigma_2)(f_j) &= \sigma_1(\sigma_2(f_j)) \\
&= \sigma_1 \left(\sum_{k=1}^{n} d_{kj} f_k \right) \\
&= \sum_{k=1}^{n} d_{kj} \sigma_1(f_k) \\
&= \sum_{k=1}^{n} d_{kj} \sum_{i=1}^{n} c_{ik} f_i \\
&= \sum_{i=1}^{n} \sum_{k=1}^{n} c_{ik} d_{kj} f_i.
\end{aligned}$$

Com isso, concluímos:

$$\phi(\sigma_1 \circ \sigma_2) = \left(\sum_{k=1}^{n} c_{ik} d_{kj} \right) = (c_{ij}) \cdot (d_{ij}) = \phi(\sigma_1) \cdot \phi(\sigma_2).$$

Para provar que ϕ é injetora, basta mostrar que $\ker \phi = \{\mathrm{id}\}$. Temos:

$$\phi(\sigma) = \mathrm{id} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \Leftrightarrow \sigma(f_j) = f_j,\ 1 \leq j \leq n \Leftrightarrow \sigma = \mathrm{id}\,.$$

Disto segue que $\ker \phi = \{\mathrm{id}\}$. Logo ϕ é injetora, e portanto o grupo $\mathrm{Gal}^D(L : K)$ é isomorfo à algum subgrupo de $\mathrm{GL}_n(C_K)$. □

Na Teoria de Galois clássica, se $L : K$ era uma extensão galoisiana, então $|\mathrm{Gal}(L : K)| = [L : K]$. Mas na Teoria de Picard-Vessiot, como C_K é infinito, então um grupo de Galois diferencial de uma extensão de Picard-Vessiot também pode ter ordem infinita, como veremos nos exemplos a seguir.

Exemplos 4.29. Vamos determinar o grupo de Galois diferencial de $\mathcal{L}(y) = 0$ para cada item abaixo. A derivação em cada item é a usual.

1. $\mathcal{L}(y) = y' - y$ com coeficientes em $\mathbb{C}(x)$

   Solução.

   As soluções de $\mathcal{L}(y) = 0$ são as funções $y(x) = ce^x$, com $c \in \mathbb{C}$. Logo $\{e^x\}$ é um conjunto fundamental de soluções de $\mathcal{L}(y) = 0$ em $E_{\mathcal{L}}$.

   Note que um elemento α de $E_{\mathcal{L}}$ é da forma:

   $$\alpha = \sum_{i=a}^{n} \sum_{j=b}^{m} a_{ij} b_{ij} x^i (e^x)^j,\ a, b, n, m \in \mathbb{Z},\ a_{ij}, b_{ij} \in \mathbb{C}.$$

   Concluímos que $E_{\mathcal{L}} = \mathbb{C}(x, e^x)$ e, portanto, a extensão de Picard-Vessiot de $\mathcal{L}(y) = 0$ é $\mathbb{C}(x, e^x) : \mathbb{C}(x)$. Vamos agora determinar $\mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x))$.

   Um automorfismo $\sigma \in \mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x))$, além de fixar os elementos de $\mathbb{C}(x)$, deve satisfazer $\sigma(e^x) = ce^x$ para algum $c \in \mathbb{C}^*$. A escolha de c determina o automorfismo. Perceba que e^x é transcendente sobre $\mathbb{C}(x)$ e, portanto, não há outras restrições algébricas na escolha de $c \in \mathbb{C}^*$. Logo, $\mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x)) \cong \mathbb{C}^*$. □

2. $\mathcal{L}(y) = y' - \dfrac{1}{15x}y$ com coeficientes em $\mathbb{C}(x)$, onde $y : I \subseteq \mathbb{R} \to \mathbb{C}$

Solução.

As soluções de $\mathcal{L}(y) = 0$ são as funções $y(x) = c\sqrt[15]{x}$, com $c \in \mathbb{C}$. Logo $\{\sqrt[15]{x}\}$ é um conjunto fundamental de soluções de $\mathcal{L}(y) = 0$ em $E_{\mathcal{L}}$.

Note que um elemento α de $E_{\mathcal{L}}$ é da forma:

$$\alpha = \sum_{i=a}^{n}\sum_{j=b}^{m} a_{ij}b_{ij}x^i(\sqrt[15]{x})^j,\ a, b, n, m \in \mathbb{Z},\ a_{ij}, b_{ij} \in \mathbb{C}.$$

Concluímos que $E_{\mathcal{L}} = \mathbb{C}(x, \sqrt[15]{x})$ e, portanto, a extensão de Picard-Vessiot de $\mathcal{L}(y) = 0$ é $\mathbb{C}(x, \sqrt[15]{x}) : \mathbb{C}(x)$. Vamos agora determinar $\mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x))$.

Um automorfismo $\sigma \in \mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x))$, além de fixar os elementos de $\mathbb{C}(x)$, deve satisfazer $\sigma(\sqrt[15]{x}) = c\sqrt[15]{x}$ para algum $c \in \mathbb{C}^*$. A escolha de c determina o automorfismo. Perceba que $\sqrt[15]{x}$ é algébrico sobre $\mathbb{C}(x)$ e, portanto, há uma restrição algébrica na escolha de $c \in \mathbb{C}^*$. Teremos $c^{15} = 1$, pois

$$c^{15}x = (c\sqrt[15]{x})^{15} = (\sigma(\sqrt[15]{x}))^{15} = \sigma(x) = x.$$

Seja $\zeta = \cos\left(\frac{2\pi}{15}\right) + i\,\mathrm{sin}\left(\frac{2\pi}{15}\right)$. Os $\mathbb{C}(x)$-automorfismos de $E_{\mathcal{L}}$ são:

σ	id	σ_1	σ_2	$\cdots$	σ_{14}
$\sigma(\sqrt[15]{x})$	$\sqrt[15]{x}$	$\zeta\sqrt[15]{x}$	$\zeta^2\sqrt[15]{x}$	$\cdots$	$\zeta^{14}\sqrt[15]{x}$

Logo, $\mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x)) \cong \mathbb{Z}_{15}$. □

3. $\mathcal{L}(y) = y'' - \dfrac{1}{x}y'$ com coeficientes em $\mathbb{C}(x)$

Solução.

As soluções de $\mathcal{L}(y) = 0$ são as funções $y(x) = c_1 + c_2x^2$, com $c_1, c_2 \in \mathbb{C}$. Calculando o Wronskiano do conjunto $\{1, x^2\}$, temos:

$$\mathcal{W}(1, x^2) = \begin{vmatrix} 1 & x^2 \\ 0 & 2x \end{vmatrix} = 2x \neq 0.$$

Logo $\{1, x^2\}$ é um conjunto linearmente independente e, portanto, é um conjunto fundamental de soluções de $\mathcal{L}(y) = 0$ em $E_{\mathcal{L}}$.

Portanto $E_{\mathcal{L}} = \mathbb{C}(x, x^2) = \mathbb{C}(x)$, e segue que a extensão de Picard-Vessiot de $\mathcal{L}(y) = 0$ é $\mathbb{C}(x) : \mathbb{C}(x)$. Vamos agora determinar $\mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x))$.

Note que dado $\sigma \in \mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x))$, então σ fixa os elementos de $\mathbb{C}(x)$. Logo, $\mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x)) = \{\mathrm{id}\}$. □

4. $\mathcal{L}(y) = y'' + \dfrac{1}{x}y'$ com coeficientes em $\mathbb{C}(x)$, onde $y : I \subseteq \mathbb{R} \to \mathbb{C}$

Solução.

As soluções de $\mathcal{L}(y) = 0$ são as funções $y(x) = c_1 + c_2 \ln x$, com $c_1, c_2 \in \mathbb{C}$. Calculando o Wronskiano de $\{1, \ln x\}$, temos:

$$\mathcal{W}(1, \ln x) = \begin{vmatrix} 1 & \ln x \\ 0 & \frac{1}{x} \end{vmatrix} = \frac{1}{x} \neq 0.$$

Logo $\{1, \ln x\}$ é um conjunto linearmente independente e, portanto, é um conjunto fundamental de soluções de $\mathcal{L}(y) = 0$ em $E_{\mathcal{L}}$.

Note que um elemento α de $E_{\mathcal{L}}$ é da forma:

$$\alpha = \sum_{i=a}^{n} \sum_{j=b}^{m} a_{ij} b_{ij} x^i (\ln x)^j,\ a, b, n, m \in \mathbb{Z},\ a_{ij}, b_{ij} \in \mathbb{C}.$$

Concluímos que $E_{\mathcal{L}} = \mathbb{C}(x, \ln x)$ e, portanto, a extensão de Picard-Vessiot de $\mathcal{L}(y) = 0$ é $\mathbb{C}(x, \ln x) : \mathbb{C}(x)$. Vamos agora determinar $\mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x))$.

Um automorfismo $\sigma \in \mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x))$, além de fixar os elementos de $\mathbb{C}(x)$, deve satisfazer $\sigma(\ln x) = z + w \ln x$, com $w \neq 0$. A escolha de (z, w) determina o automorfismo. Seja o conjunto

$$S = \left\{ \begin{pmatrix} 1 & z \\ 0 & w \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C}) : w \neq 0 \right\}.$$

Defina a aplicação

$$\begin{array}{rccl} \Phi : & S & \to & \mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x)) \\ & \begin{pmatrix} 1 & z \\ 0 & w \end{pmatrix} & \mapsto & \sigma : E_{\mathcal{L}} \to E_{\mathcal{L}} \\ & & & f \mapsto \sigma(f) \end{array}$$

Queremos mostrar que Φ é um isomorfismo de grupos.

Seja $\sigma_1, \sigma_2 \in \mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x))$ tais que $\sigma_1(\ln x) = z_1 + w_1 \ln x$ e $\sigma_2(\ln x) = z_2 + w_2 \ln x$.

Então:

$$\begin{aligned}(\sigma_1 \circ \sigma_2)(\ln x) &= \sigma_1(\sigma_2(\ln x)) \\ &= \sigma_1(z_2 + w_2 \ln x) \\ &= \sigma_1(z_2) + \sigma_1(w_2)\sigma_1(\ln x) \\ &= z_2 + w_2(z_1 + w_1 \ln x) \\ &= (z_2 + z_1 w_2) + (w_1 w_2) \ln x.\end{aligned}$$

Com isso, concluímos:

$$\Phi\left(\begin{pmatrix}1 & z_1\\ 0 & w_1\end{pmatrix}\cdot\begin{pmatrix}1 & z_2\\ 0 & w_2\end{pmatrix}\right) = \Phi\begin{pmatrix}1 & z_2+z_1w_2\\ 0 & w_1w_2\end{pmatrix} = \sigma_1\circ\sigma_2 = \Phi\begin{pmatrix}1 & z_1\\ 0 & w_1\end{pmatrix}\cdot\Phi\begin{pmatrix}1 & z_1\\ 0 & w_1\end{pmatrix}.$$

Note que Φ é sobrejetora por definição. Para provar que Φ é injetora, basta mostrar que $\ker\Phi = \{\mathrm{id}\}$. Temos:

$$\Phi\begin{pmatrix}1 & z\\ 0 & w\end{pmatrix} = \mathrm{id} \Leftrightarrow z = 0,\ w = 1.$$

Logo Φ é injetora, e portanto bijetora. Segue então que Φ é um isomorfismo, ou seja, $\mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x)) \cong S$. □

5. $\mathcal{L}(y) = y'' + y$ com coeficientes em $\mathbb{C}(x)$

Solução.

As soluções de $\mathcal{L}(y) = 0$ são as funções $y(x) = c_1 \cos x + c_2 \operatorname{sen} x$, com $c_1, c_2 \in \mathbb{C}$. Calculando o Wronskiano de $\cos x, \operatorname{sen} x$, temos:

$$\mathcal{W}(\cos x, \operatorname{sen} x) = \begin{vmatrix}\cos x & \operatorname{sen} x\\ -\operatorname{sen} x & \cos x\end{vmatrix} = \cos^2 x + \operatorname{sen}^2 x = 1 \neq 0.$$

Logo $\{\cos x, \operatorname{sen} x\}$ é um conjunto linearmente independente e, portanto, é um conjunto fundamental de soluções de $\mathcal{L}(y) = 0$ em $E_{\mathcal{L}}$.

Note que um elemento α de $E_{\mathcal{L}}$ é da forma:

$$\alpha = \sum_{i=a}^{n}\sum_{j=b}^{m}\sum_{k=c}^{l} a_{ijk}b_{ijk}c_{ijk}x^i(\cos x)^j(\operatorname{sen} x)^k,\ a,b,c,n,m,l \in \mathbb{Z},\ a_{ijk}, b_{ijk}, c_{ijk} \in \mathbb{C}.$$

Concluímos que $E_{\mathcal{L}} = \mathbb{C}(x, \cos x, \operatorname{sen} x)$ e, portanto, a extensão de Picard-Vessiot de $\mathcal{L}(y) = 0$ é $\mathbb{C}(x, \cos x, \operatorname{sen} x) : \mathbb{C}(x)$. Vamos agora determinar $\mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x))$.

Dado $\sigma \in \mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x))$, suponha que $\sigma(\operatorname{sen} x) = a \operatorname{sen} x + b \cos x$, e $\sigma(\cos x) = c \operatorname{sen} x + d \cos x$, para $a, b, c, d \in \mathbb{C}$. Então:

$$\begin{aligned} c \operatorname{sen} x + d \cos x &= \sigma(\cos x) \\ &= \sigma(\operatorname{sen}(x)') \\ &= \sigma(\operatorname{sen} x)' \\ &= (a \operatorname{sen} x + b \cos x)' \\ &= a \cos x - b \operatorname{sen} x. \end{aligned}$$

Logo, $d = a$ e $c = -b$. Então um automorfismo $\sigma \in \mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x))$, além de fixar os elementos de $\mathbb{C}(x)$, deve satisfazer $\sigma(\cos x) = a \cos x - b \operatorname{sen} x$, e $\sigma(\operatorname{sen} x) = b \cos x + a \operatorname{sen} x$. Também temos a seguinte restrição que se origina da equação $\operatorname{sen}^2 x + \cos^2 x = 1$:

$$\begin{aligned} a^2 + b^2 &= (a^2 + b^2)(\operatorname{sen}^2 x + \cos^2 x) \\ &= a^2 \operatorname{sen}^2 x + a^2 \cos^2 x + b^2 \operatorname{sen}^2 x + b^2 \cos^2 x \\ &= (b \cos x + a \operatorname{sen} x)^2 + (a \cos x - b \operatorname{sen} x)^2 \\ &= \sigma(\operatorname{sen} x)^2 + \sigma(\cos x)^2 \\ &= \sigma(\operatorname{sen}^2 x) + \sigma(\cos^2 x) \\ &= \sigma(\operatorname{sen}^2 x + \cos^2 x) \\ &= \sigma(1) \\ &= 1. \end{aligned}$$

Seja o conjunto

$$S = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C}) : a^2 + b^2 = \det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = 1 \right\}.$$

Defina a aplicação

$$\begin{array}{rccl} \Phi : & S & \to & \mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x)) \\ & \begin{pmatrix} a & -b \\ b & a \end{pmatrix} & \mapsto & \sigma : E_{\mathcal{L}} \to E_{\mathcal{L}} \\ & & & f \mapsto \sigma(f) \end{array}$$

Queremos mostrar que Φ é um isomorfismo de grupos. Seja $\sigma_1, \sigma_2 \in \mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x))$ tais que $\sigma_1(\cos x) = a_1 \cos x - b_1 \operatorname{sen} x$, $\sigma_1(\operatorname{sen} x) = b_1 \cos x + a_1 \operatorname{sen} x$, $\sigma_2(\cos x) =$

$a_2 \cos x - b_2 \operatorname{sen} x$, e $\sigma_2(\operatorname{sen} x) = b_2 \cos x + a_2 \operatorname{sen} x$. Então:

$$\begin{aligned}(\sigma_1 \circ \sigma_2)(\cos x) &= \sigma_1(\sigma_2(\cos x)) \\ &= \sigma_1(a_2 \cos x - b_2 \operatorname{sen} x) \\ &= \sigma_1(a_2)\sigma_1(\cos x) - \sigma_1(b_2)\sigma_1(\operatorname{sen} x) \\ &= a_2(a_1 \cos x - b_1 \operatorname{sen} x) - b_2(b_1 \cos x + a_1 \operatorname{sen} x) \\ &= (a_1 a_2 - b_1 b_2)\cos x - (a_2 b_1 + a_1 b_2)\operatorname{sen} x.\end{aligned}$$

$$\begin{aligned}(\sigma_1 \circ \sigma_2)(\operatorname{sen} x) &= \sigma_1(\sigma_2(\operatorname{sen} x)) \\ &= \sigma_1(b_2 \cos x + a_2 \operatorname{sen} x) \\ &= \sigma_1(b_2)\sigma_1(\cos x) + \sigma_1(a_2)\sigma_1(\operatorname{sen} x) \\ &= b_2(a_1 \cos x - b_1 \operatorname{sen} x) + a_2(b_1 \cos x + a_1 \operatorname{sen} x) \\ &= (a_1 b_2 + a_2 b_1)\cos x + (a_1 a_2 - b_1 b_2)\operatorname{sen} x.\end{aligned}$$

Com isso, concluímos:

$$\begin{aligned}\Phi\left(\begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix}\right) &= \Phi \begin{pmatrix} a_1 a_2 - b_1 b_2 & -(a_1 b_2 + a_2 b_1) \\ a_1 b_2 + a_2 b_1 & a_1 a_2 - b_1 b_2 \end{pmatrix} \\ &= \sigma_1 \circ \sigma_2 \\ &= \Phi \begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} \cdot \Phi \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix}.\end{aligned}$$

Note que Φ é sobrejetora por definição. Para provar que Φ é injetora, basta mostrar que $\ker \Phi = \{\mathrm{id}\}$. Temos:

$$\Phi \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \mathrm{id} \Leftrightarrow a = 1,\ b = 0.$$

Logo Φ é injetora, e portanto bijetora. Segue então que Φ é um isomorfismo, ou seja, $\mathrm{Gal}^D(E_{\mathcal{L}} : \mathbb{C}(x)) \cong S$. □

4.5.1 Teorema Fundamental de Picard-Vessiot

Finalmente a cereja do bolo: o Teorema Fundamental de Picard-Vessiot! Antes iremos dar algumas definições.

Definição 4.30. Um **grupo algébrico linear** é um subgrupo $G \subseteq \mathrm{GL}_n(C_K)$ que é um conjunto de zeros de um sistema de polinômios em n^2 variáveis com coeficientes em C_K.

Definição 4.31. Um subgrupo $H \subseteq G$ é dito **Zariski-fechado** se H é um grupo algébrico linear.

Vimos na Proposição 4.28 que dada uma extensão de Picard-Vessiot $L : K$ associada à equação diferencial linear homogênea $\mathcal{L}(y) = 0$ de ordem n, o grupo $\mathrm{Gal}^D(L : K)$ é isomorfo à algum subgrupo de $\mathrm{GL}_n(C_K)$. Agora afirmaremos mais: $\mathrm{Gal}^D(L : K)$ também é um conjunto de zeros de um sistema de polinômios em n^2 variáveis com coeficientes em C_K. Pela Definição 4.30, segue que $\mathrm{Gal}^D(L : K)$ é um grupo algébrico linear.

Enunciaremos agora o Teorema Fundamental de Picard-Vessiot, cuja demonstração pode ser encontrada em [3], Teorema 5.1. Na Teoria de Galois clássica dada uma extensão galoisiana $L : K$, existe uma correspondência entre os subcorpos de L que contém K e os subgrupos de $\mathrm{Gal}(L : K)$. De maneira semelhante, na Teoria de Picard-Vessiot dada uma extensão de Picard-Vessiot $L : K$, existe uma correspondência entre os subcorpos diferenciais de L que contém K e os subgrupos Zariski-fechados de $\mathrm{Gal}^D(L : K)$.

Teorema 4.32 (Teorema Fundamental de Picard-Vessiot)**.** *Seja $L : K$ uma extensão de Picard-Vessiot.*

(a) A extensão $L : M$ é de Picard-Vessiot e existe uma correspondência entre os subcorpos intermediários M de $L : K$ e os subgrupos Zariski-fechados H de $Gal^D(L : K)$, dada pela bijeção natural:

$$\begin{array}{ccc} \left\{\begin{array}{c} \textit{subgrupos Zariski-fechados} \\ H \textit{ de } Gal^D(L:K) \end{array}\right\} & \longleftrightarrow & \left\{\begin{array}{c} \textit{subcorpos diferenciais} \\ \textit{intermediários } M \textit{ de } L:K \end{array}\right\} \\ H & \longmapsto & L^H \\ Gal^D(L:M) & \longleftarrow & M. \end{array}$$

(b) A extensão $M : K$ é de Picard-Vessiot se, e somente se, $Gal^D(L : M)$ é subgrupo normal de $Gal^D(L : K)$. Nessas condições, vale $Gal^D(M : K) \cong \frac{Gal^D(L:K)}{Gal^D(L:M)}$.

Vamos aplicar este teorema nos exemplos a seguir.

Exemplos 4.33. Vamos determinar os subgrupos do grupo de Galois e seus respectivos corpos intermediários para cada item abaixo. A derivação em cada item é a usual.

1. $\mathcal{L}(y) = y' - y$ com coeficientes em $\mathbb{C}(x)$

   Solução.

   Vimos no item 1 dos Exemplos 4.29 que $\mathcal{L}(y) = y' - y = 0$, definida sobre $\mathbb{C}(x)$, está associada à extensão de Picard-Vessiot $\mathbb{C}(x, e^x) : \mathbb{C}(x)$ e $\mathrm{Gal}^D(\mathbb{C}(x, e^x) : \mathbb{C}(x)) \cong \mathbb{C}^*$.

   Os subgrupos Zariski-fechados de $\mathbb{C}^*$ são os grupos gerados pelas raízes de $x^n - 1 = 0$ para cada $n \in \mathbb{N}^*$, isto é, $\mu_n = \{\cos\left(\frac{2k\pi}{n}\right) + i \sin\left(\frac{2k\pi}{n}\right) : k = 1, 2, \ldots, n\}$.

Seja $L = \mathbb{C}(x, e^x)$. Os corpos intermediários $L \supseteq M_n \supseteq \mathbb{C}(x)$ são dados por $M_n = L^{\mu_n} = \{x \in L : \sigma(x) = x, \forall\, \sigma \text{ identificado com um elemento de } \mu_n\} = \mathbb{C}(x, e^{nx})$, pois identificando σ com um elemento de μ_n, temos:

$$\sigma(e^{nx}) = (\sigma(e^x))^n = (ce^x)^n = c^n e^{nx} = e^{nx}.$$

Seja $m \in \mathbb{N}^*$ tal que $m \mid n$. Então podemos denotar a correspondência entre os subcorpos de $\mathbb{C}(x, e^x) : \mathbb{C}(x)$ e os subgrupos Zariski-fechados de $\mathrm{Gal}^D(\mathbb{C}(x, e^x) : \mathbb{C}(x))$ da seguinte maneira:

$$\begin{array}{ccc}
\mathbb{C}(x, e^x) & \longleftrightarrow & \{\mathrm{id}\} \\
| & & | \\
\mathbb{C}(x, e^{mx}) & \longleftrightarrow & \mu_m \\
| & & | \\
\mathbb{C}(x, e^{nx}) & \longleftrightarrow & \mu_n \\
| & & | \\
\mathbb{C}(x) & \longleftrightarrow & \mathbb{C}^*
\end{array}$$

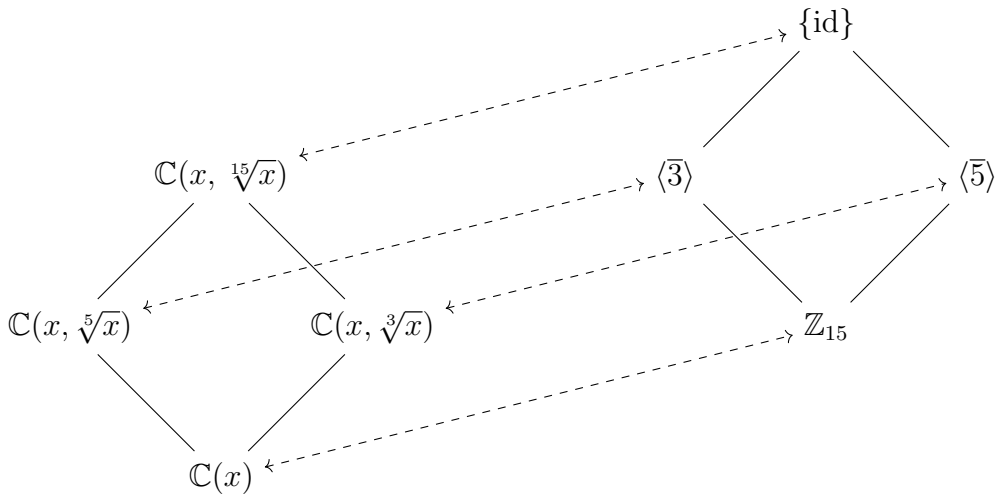
Como $\mathbb{C}^*$ é abeliano, então μ_n é subgrupo normal de $\mathbb{C}^*$ para todo $n \in \mathbb{N}^*$. Portanto, pelo Teorema 4.32 (Teorema Fundamental de Picard-Vessiot), $\mathbb{C}(x, e^{nx}) : \mathbb{C}(x)$ é uma extensão de Picard-Vessiot da equação $y' - ny = 0$ para cada $n \in \mathbb{N}^*$ com o grupo de Galois diferencial $\mathrm{Gal}^D(\mathbb{C}(x, e^{nx}) : \mathbb{C}(x)) \cong \mathbb{C}^*/\mu_n$. □

2. $\mathcal{L}(y) = y' - \dfrac{1}{15x} y$ com coeficientes em $\mathbb{C}(x)$, onde $y : I \subseteq \mathbb{R} \to \mathbb{C}$

Solução.

Vimos no item 2 dos Exemplos 4.29 que $\mathcal{L}(y) = y' - \dfrac{1}{15x} y = 0$, definida sobre $\mathbb{C}(x)$, está associada à extensão de Picard-Vessiot $\mathbb{C}(x, \sqrt[15]{x}) : \mathbb{C}(x)$ e $\mathrm{Gal}^D(\mathbb{C}(x, \sqrt[15]{x}) : \mathbb{C}(x)) \cong \mathbb{Z}_{15}$.

Os subgrupos $\langle \overline{3} \rangle$ e $\langle \overline{5} \rangle$ de $\mathbb{Z}_{15}$ são finitos e, portanto, Zariski-fechados. Podemos denotar a correspondência entre os subcorpos de $\mathbb{C}(x, \sqrt[15]{x}) : \mathbb{C}(x)$ e os subgrupos Zariski-fechados de $\mathrm{Gal}^D(\mathbb{C}(x, \sqrt[15]{x}) : \mathbb{C}(x))$ da seguinte maneira:



O subgrupo $\langle\overline{5}\rangle$ de $\mathbb{Z}_{15}$ é normal. Então, pelo Teorema 4.32 (Teorema Fundamental de Picard-Vessiot), $\mathbb{C}(x, \sqrt[3]{x}) : \mathbb{C}(x)$ é uma extensão de Picard-Vessiot da equação $y' - \frac{1}{3x}y = 0$ com o grupo de Galois diferencial $\mathrm{Gal}^D(\mathbb{C}(x, \sqrt[3]{x}) : \mathbb{C}(x)) \cong \mathbb{Z}_{15}/\langle\overline{5}\rangle \cong \mathbb{Z}_3$.

Da mesma forma, $\langle\overline{3}\rangle$ é subgrupo normal de $\mathbb{Z}_{15}$. Então, pelo Teorema 4.32 (Teorema Fundamental de Picard-Vessiot), $\mathbb{C}(x, \sqrt[5]{x}) : \mathbb{C}(x)$ é uma extensão de Picard-Vessiot da equação $y' - \frac{1}{5x}y = 0$ com o grupo de Galois diferencial $\mathrm{Gal}^D(\mathbb{C}(x, \sqrt[5]{x}) : \mathbb{C}(x)) \cong \mathbb{Z}_{15}/\langle\overline{3}\rangle \cong \mathbb{Z}_5$. □

4.6 Integração em termos de funções elementares

Nesta seção, apresentaremos um teorema de Joseph Liouville que caracteriza funções que possuem primitiva elementar. Liouville provou esses resultados por volta do ano de 1830, mas foi apenas na metade do século XX que Ostrowski reformulou o teorema de Liouville no cenário da álgebra de corpos diferenciais. Posteriormente, esta teoria deu surgimento ao algoritmo de Risch, que é usado para computar integrais indefinidas, quando possível.

Antes de tudo, o que são funções elementares?

Definição 4.34. O **conjunto das funções elementares** E é o menor conjunto de funções $f : I \subseteq \mathbb{R} \to \mathbb{C}$, tal que:

(a) Todos os polinômios estão em E.

(b) As funções exponencial e logaritma estão em E.

(c) As funções seno e cosseno estão em E.

(d) E é fechado sob as operações de adição, subtração, multiplicação, divisão e composição (apenas para uma quantidade finita de operações).

Perceba que pela Definição 4.34, funções elementares são funções de uma variável cujos termos são constantes, algébricos, exponenciais ou logaritmos. Funções trigonométricas e inversas trigonométricas definidas em uma região (conjunto aberto e conexo) do plano complexo também são elementares, pois são compostas por exponenciais ou logaritmos. A integral de uma função racional de uma variável real é elementar, pois é combinação linear de logaritmos, arcotangentes e funções racionais.

Nesse estudo, queremos evitar todas as funções multivaloradas. Para isso, trabalharemos apenas com funções $f : I \subseteq \mathbb{R} \to \mathbb{C}$.

Definição 4.35. Seja $L : K$ uma extensão diferencial e seja $a \in K$. Um elemento $\alpha \in L$ é um **logaritmo** do elemento a se $a \neq 0$ e $\alpha' = \dfrac{a'}{a}$. Um elemento $\alpha \in L$ é uma **exponencial** do elemento a se $\alpha \neq 0$ e se $a' = \dfrac{\alpha'}{\alpha}$.

Definição 4.36. Seja K um corpo diferencial. Uma extensão diferencial $L : K$ é dita **extensão liouvilliana** (ou **extensão diferencial elementar**) se existem elementos $\alpha_1, \ldots, \alpha_n \in L$ tais que

1. $L = K(\alpha_1, \ldots, \alpha_n)$.
2. $C_L = C_K$.
3. Para qualquer $j \in \{1, 2, \ldots, n\}$, uma das três propriedades a seguir valem:
   (a) α_j é algébrico sobre $K(\alpha_1, \ldots, \alpha_{j-1})$.
   (b) α_j é um logaritmo de um elemento não nulo de $K(\alpha_1, \ldots, \alpha_{j-1})$.
   (c) α_j é uma exponencial de um elemento de $K(\alpha_1, \ldots, \alpha_{j-1})$.

Uma observação importante é que extensões liouvillanas não são necessariamente de Picard-Vessiot. Considere a extensão $K(\tau, \alpha) : K$ tal que τ é logaritmo de um elemento não nulo de K e α é algébrico sobre $K(\tau)$, sendo $p(x) = x^2 + \tau^2 - 1$ o polinômio minimal de α sobre $K(\tau)$. Então $K(\tau, \alpha) : K$ é um exemplo de extensão liouvilliana que não é de Picard-Vessiot.

Definição 4.37. Seja $p \in K[x]$ um polinômio mônico irredutível. Para qualquer $f \in K(x)^*$, definimos a **ordem** de f em relação ao polinômio p como sendo o expoente de p quando escrevemos f como produto de polinômios irredutíveis de $K[x]$ e de inversos de polinômios irredutíveis de $K[x]$, vezes um elemento de K, e denotamos por $\mathrm{ord}_p(f)$.

Exemplos 4.38. Determinaremos $\mathrm{ord}_p(f)$ nos casos a seguir.

1. $f(x) = \dfrac{2x-1}{x^3(2x^2+2)(x-3)}$ e $p(x) = x^2+1$

   Solução.

   Perceba que

$$\begin{aligned} f(x) &= \frac{2x-1}{x^3(2x^2+2)(x-3)} \\ &= (2x-1)x^{-3}(2x^2+2)^{-1}(x-3)^{-1} \\ &= 2^{-1}(2x-1)x^{-3}(x^2+1)^{-1}(x-3)^{-1}. \end{aligned}$$

   Como o expoente do fator $p(x) = x^2+1$ em f é -1, segue que $\mathrm{ord}_p(f) = -1$. □

2. $f(x) = \dfrac{(x^2+1)(2x-1)}{x^3(2x^2+2)(x-3)}$ e $p(x) = x^2+1$

   Solução.

   Perceba que

$$\begin{aligned} f(x) &= \frac{(x^2+1)(2x-1)}{x^3(2x^2+2)(x-3)} \\ &= (x^2+1)(2x-1)x^{-3}(2x^2+2)^{-1}(x-3)^{-1} \\ &= 2^{-1}\cancel{(x^2+1)}(2x-1)x^{-3}\cancel{(x^2+1)^{-1}}(x-3)^{-1} \\ &= 2^{-1}(2x-1)x^{-3}(x-3)^{-1}. \end{aligned}$$

   Como o fator $p(x) = x^2+1$ em f se cancelou, então o expoente do fator $p(x) = x^2+1$ em f é zero e segue que $\mathrm{ord}_p(f) = 0$. □

Iremos agora enunciar e provar o Teorema de Liouville-Ostrowski e o Critério de Liouville que caracterizam funções com primitivas elementares. Para demonstrar o Teorema de Liouville-Ostrowski, iremos analisar um caso mais simples na proposição seguinte para depois fazermos um processo de indução.

Proposição 4.39. *Sejam $K(\alpha) : K$ uma extensão liouvilliana e $f \in K$ tais que $f = v' + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i}$ com $c_i \in C_{K(\alpha)}$ e $u_1, \ldots, u_n, v \in K(\alpha)$. Então f admite uma expressão similar em K, isto é, existem $\tilde{c_i} \in C_K$ e $\tilde{u_1}, \ldots, \tilde{u_n}, \tilde{v} \in K$ tais que*

$$f = \tilde{v}' + \sum_{i=1}^{n} \tilde{c_i} \frac{\tilde{u_i}'}{\tilde{u_i}}.$$

Demonstração.

Vamos separar esta demonstração em três casos.

Caso 1: α é algébrico sobre K.

Seja $L \supset K$ um fecho galoisiano[1] da extensão algébrica $K(\alpha) : K$ de forma que $L : K$ seja uma extensão diferencial munida da derivação de $K(\alpha) : K$. Sejam $\sigma \in \mathrm{Gal}(L : K)$ e $y \in L$, $y \neq 0$. Temos:

$$\sigma\left(\frac{y'}{y}\right) = \frac{\sigma(y')}{\sigma(y)} = \frac{\sigma(y)'}{\sigma(y)}.$$

Como $f \in K$, então $\sigma(f) = f$, $\forall\, \sigma \in \mathrm{Gal}(L : K)$. Temos: $f = \dfrac{1}{[L : K]} \displaystyle\sum_{\sigma \in \mathrm{Gal}(L:K)} \sigma(f)$. Considere que $[L : K] = m$ e $\mathrm{Gal}(L : K) = \{\sigma_1, \sigma_2, \ldots, \sigma_m\}$. Reescrevendo a expressão de f acima, temos:

$$\begin{aligned}
f &= \frac{1}{m}\sum_{j=1}^{m} \sigma_j(f) \\
&= \frac{1}{m}\sum_{j=1}^{m} \sigma_j\left(v' + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i}\right) \\
&= \frac{1}{m}\sum_{j=1}^{m} \left[\sigma_j(v') + \sigma_j\left(\sum_{i=1}^{n} c_i \frac{u_i'}{u_i}\right)\right] \\
&= \frac{1}{m}\sum_{j=1}^{m} \left[\sigma_j(v)' + \sum_{i=1}^{n} c_i \sigma_j\left(\frac{u_i'}{u_i}\right)\right] \\
&= \frac{1}{m}\sum_{j=1}^{m} \left[\sigma_j(v)' + \sum_{i=1}^{n} c_i \frac{\sigma_j(u_i)'}{\sigma_j(u_i)}\right] \\
&= \frac{1}{m}\left(\sum_{j=1}^{m} \sigma_j(v)' + \sum_{i=1}^{n} c_i \sum_{j=1}^{m} \frac{\sigma_j(u_i)'}{\sigma_j(u_i)}\right) \\
&= \frac{1}{m}\sum_{j=1}^{m} \sigma_j(v)' + \sum_{i=1}^{n} \frac{c_i}{m} \cdot \frac{\sum_{j=1}^{m} \sigma_j(u_i)' \prod_{k=1, j\neq k}^{m} \sigma_k(u_i)}{\prod_{j=1}^{m} \sigma_j(u_i)}.
\end{aligned}$$

Defina $\tilde{v} = \dfrac{1}{m}\displaystyle\sum_{j=1}^{m} \sigma_j(v)$, $\tilde{c_i} = \dfrac{c_i}{m}$ e $\tilde{u_i} = \displaystyle\prod_{j=1}^{m} \sigma_j(u_i)$. Note que estes elementos são fixados pelos automorfismos de $\mathrm{Gal}(L : K)$ e, portanto, $\tilde{v}, \tilde{c_i}, \tilde{u_i} \in K$, $\forall\, i \in \{1, 2, \ldots, n\}$.

Então, segue que

$$f = \tilde{v}' + \sum_{i=1}^{n} \tilde{c_i} \frac{\tilde{u_i}'}{\tilde{u_i}}.$$

[1]Seja $L : K$ uma extensão de corpos. A menor extensão galoisiana $N : K$ que contém L (ou seja, $N \supset L \supset K$) é chamada de **fecho galoisiano**.

Caso 2: α é transcendente sobre K, e é um logaritmo.

Suponha que α é logaritmo de $a \in K^*$. Então $\alpha' = \frac{a'}{a}$. Vamos expandir as derivadas logarítmicas na fórmula $f = v' + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i}$. Temos:

$$f = v' + \sum_{i=1}^{n} c_i \left(\frac{a_i'}{a_i} + \sum_{j=1}^{k_i} k_{ij} \frac{\pi_{ij}'}{\pi_{ij}} \right) = v' + \sum_{i=1}^{n} c_i \frac{a_i'}{a_i} + \sum_{i=1}^{n} c_i \sum_{j=1}^{k_i} k_{ij} \frac{\pi_{ij}'}{\pi_{ij}}, \quad (*)$$

onde $a_i \in K^*$, $c_i, k_{ij} \in C_K$ e $\pi_{ij} \in K[x]$ com π_{ij} mônicos irredutíveis sobre K. Como $v \in K(\alpha)$, então podemos escrever v na forma $v = \dfrac{p(\alpha)}{r(\alpha)\pi(\alpha)^k}$, onde $p, r, \pi \in K[x]$ com π mônico irredutível sobre K, p, r, π primos entre si e $k \in \mathbb{N}^*$.

Segue que $\mathrm{ord}_\pi(v) = -k \leq -1$. Derivando v, temos:

$$\begin{aligned} v' &= \frac{p(\alpha)'\alpha' r(\alpha)\pi(\alpha)^k - p(\alpha)[r(\alpha)'\alpha'\pi(\alpha)^k + k r(\alpha)\pi(\alpha)^{k-1}\pi(\alpha)'\alpha']}{[r(\alpha)\pi(\alpha)^k]^2} \\ &= \frac{\alpha'\pi(\alpha)^{k-1}[p(\alpha)' r(\alpha)\pi(\alpha) - p(\alpha) r(\alpha)'\pi(\alpha) - k p(\alpha) r(\alpha)\pi(\alpha)']}{r(\alpha)^2\pi(\alpha)^{2k}} \\ &= \frac{\alpha'[p(\alpha)' r(\alpha)\pi(\alpha) - p(\alpha) r(\alpha)'\pi(\alpha) - k p(\alpha) r(\alpha)\pi(\alpha)']}{r(\alpha)^2\pi(\alpha)^{k+1}}. \end{aligned}$$

Como π é mônico irredutível, então π e π' são primos entre si. Portanto, $\mathrm{ord}_\pi(v') = -(k+1) = -k - 1 \leq -2$. Como $c_i \dfrac{a_i'}{a_i} \in K$ e $\pi \notin K$, então $\mathrm{ord}_\pi \left(c_i \frac{a_i'}{a_i} \right) = 0$. Como π e π' são primos entre si, então

$$\mathrm{ord}_\pi \left(c_i \sum_{j=1}^{k_i} k_{ij} \frac{\pi_{ij}'}{\pi_{ij}} \right) = 0, \text{ se } \pi \neq \pi_{ij}, \forall\, i, j, \text{ ou}$$

$$\mathrm{ord}_\pi \left(c_i \sum_{j=1}^{k_i} k_{ij} \frac{\pi_{ij}'}{\pi_{ij}} \right) = -1, \text{ se } \pi = \pi_{ij}, \text{ para algum } i, j.$$

Mas $\mathrm{ord}_\pi(f) = 0$, pois $f \in K$, o que faz ser impossível dessa soma ser igual à f. Então, $v \in K[\alpha]$.

Como $\partial(\pi(\alpha)') < \partial(\pi(\alpha))$, a equação $(*)$ é decomposição em frações parciais da função racional $f \in K$. Como tal decomposição é única e $\dfrac{\pi_{ij}'}{\pi_{ij}} \notin K$, então esses termos se anulam e segue que:

$$f = v' + \sum_{i=1}^{n} c_i \frac{a_i'}{a_i}.$$

Portanto $v' = f - \sum_{i=1}^{n} c_i \dfrac{a_i'}{a_i} \in K$, o que implica que $\partial(v') = 0$. Logo, $v = c\alpha + d$, para

$c, d \in K$ e $c' = 0$. Então:

$$\begin{aligned} f &= v' + \sum_{i=1}^{n} c_i \frac{a_i'}{a_i} \\ &= c'\alpha + c\alpha' + d' + \sum_{i=1}^{n} c_i \frac{a_i'}{a_i} \\ &= c\alpha' + d' + \sum_{i=1}^{n} c_i \frac{a_i'}{a_i} \\ &= c\frac{a'}{a} + d' + \sum_{i=1}^{n} c_i \frac{a_i'}{a_i} \\ &= d' + \left(c\frac{a'}{a} + \sum_{i=1}^{n} c_i \frac{a_i'}{a_i} \right). \end{aligned}$$

Esta expressão é da forma esperada, e conclui a demonstração para este caso.

Caso 3: α é transcendente sobre K, e é uma exponencial.

Suponha que α é uma exponencial, ou seja, $\alpha' = a'\alpha$ para algum $a \in K^*$. Assim como o caso anterior, vamos expandir as derivadas logarítmicas na fórmula $f = v' + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i}$. Temos:

$$f = v' + \sum_{i=1}^{n} c_i \left(\frac{a_i'}{a_i} + \sum_{j=1}^{k_i} k_{ij} \frac{\pi_{ij}'}{\pi_{ij}} \right) = v' + \sum_{i=1}^{n} c_i \frac{a_i'}{a_i} + \sum_{i=1}^{n} c_i \sum_{j=1}^{k_i} k_{ij} \frac{\pi_{ij}'}{\pi_{ij}}, \quad (**)$$

onde $a_i \in K^*$, $c_i, k_{ij} \in C_K^*$ e $\pi_{ij} \in K[x]$ com π_{ij} mônicos irredutíveis sobre K.
Consequentemente, temos:

$$f = v' + \sum_{i=1}^{n} c_i \frac{a_i'}{a_i} + \sum_{i=1}^{n} c_i \sum_{j=1}^{k_i} k_{ij} \left(a' + \frac{\pi_{ij}^D(\alpha) + a'\alpha\pi_{ij}'(\alpha) - a'\pi_{ij}(\alpha)}{\pi_{ij}(\alpha)} \right). \quad (***)$$

Se $\pi_{ij} \neq x$ para algum $i \in \{1, 2, \ldots, n\}$ e $j \in \{1, 2, \ldots, k_i\}$, e $\mathrm{ord}_{\pi_{ij}}(v) < 0$, então $\mathrm{ord}_{\pi_{ij}}(v') \leq -2$, pois as raízes da derivada de um polinômio separável são distintas das raízes do polinômio em si. Mas $\mathrm{ord}_{\pi_{ij}}$ do lado direito da igualdade $(***)$ é maior ou igual à -1. Isto mostra que $\mathrm{ord}_{\pi_{ij}}(v) \geq 0$ se $\pi_{ij} \neq x$, ou seja, podemos escrever $v = \sum_{j=r}^{s} v_j \alpha^j$ para $v_j \in K, r, s \in \mathbb{Z}$. Com isso,

$$v' = \sum_{j=r}^{s} (v_j'\alpha^j + v_j j\alpha^{j-1}\alpha') = \sum_{j=r}^{s} (v_j'\alpha^j + v_j j\alpha^{j-1}a'\alpha) = \sum_{j=r}^{s} (v_j' + ja'v_j)\alpha^j.$$

Agora observe que para qualquer π_{ij}, temos

$$\partial(\pi_{ij}^D(x) + a'x\pi'_{ij}(x) - a'\pi_{ij}(x)) < \partial(\pi_{ij}(x)).$$

Como $f \in K$, a unicidade da decomposição em frações parciais implica que podemos omitir as somas com π_{ij} no denominador. Seja $c = \sum_{i=1}^{n}\sum_{j=1}^{k_i} c_i k_{ij}$. Então trabalhando a equação $(**)$ temos:

$$f = \sum_{j=r}^{s}(v'_j + ja'v_j)\alpha^j + ca' + \sum_{i=1}^{n} c_i\frac{a'_i}{a_i}.$$

Como $f \in K$, basta tomarmos apenas a potência nula de α:

$$f = v'_0 + ca' + \sum_{i=1}^{n} c_i\frac{a'_i}{a_i} = (v_0 + ca)' + \sum_{i=1}^{n} c_i\frac{a'_i}{a_i}.$$

Esta expressão é da forma esperada, e conclui a demonstração para este caso.

□

Teorema 4.40 (Teorema de Liouville-Ostrowski; Liouville, 1835; Ostrowski, 1946)**.** *Sejam K um corpo diferencial de característica zero e $f \in K$. Se f possui uma primitiva em uma extensão liouvilliana $L : K$, então existem $n \geq 0$ inteiro, $c_1, \ldots, c_n \in C_K$ e $u_1, \ldots, u_n, v \in K$ tais que*

$$f = v' + \sum_{i=1}^{n} c_i\frac{u'_i}{u_i}.$$

Demonstração.

Suponha que f tem primitiva na extensão liouvilliana $L = K(\alpha_1, \ldots, \alpha_m) : K$. Sabemos que vale a seguinte cadeia de corpos diferenciais:

$$L = K(\alpha_1, \ldots, \alpha_m) \supseteq K(\alpha_1, \ldots, \alpha_{m-1}) \supseteq \cdots \supseteq K(\alpha_1, \alpha_2) \supseteq K(\alpha_1) \supseteq K.$$

Aplicando a Proposição 4.39 na extensão

$$K(\alpha_1, \ldots, \alpha_j) = K(\alpha_1, \ldots, \alpha_{j-1})(\alpha_j) \supseteq K(\alpha_1, \ldots, \alpha_{j-1})$$

para cada $j \in \{1, 2, \ldots, m\}$ de forma decrescente, concluímos que existem $n \geq 0$ inteiro, $c_1, \ldots, c_n \in C_K$ e $u_1, \ldots, u_n, v \in K$ tais que

$$f = v' + \sum_{i=1}^{n} c_i\frac{u'_i}{u_i}.$$

□

Lema 4.41. *Seja $g \in \mathbb{C}(x)$ não constante. Então e^g é transcendente sobre $\mathbb{C}(x)$.*

Demonstração.

Suponha, por absurdo, que e^g possui um polinômio minimal sobre $\mathbb{C}(x)$, isto é,

$$e^{ng} + \sum_{j=0}^{n-1} a_j e^{jg} = 0.$$

Derivando esta equação, obtemos

$$\begin{aligned} & \left(e^{ng} + \sum_{j=0}^{n-1} a_j e^{jg} \right)' = 0 \\ \Leftrightarrow \quad & ng' e^{ng} + \sum_{j=0}^{n-1} (a_j' + j a_j g') e^{jg} = 0 \\ \Leftrightarrow \quad & e^{ng} + \sum_{j=0}^{n-1} \left(\frac{a_j' + j a_j g'}{n g'} \right) e^{jg} = 0. \end{aligned}$$

Como o polinômio minimal é único, então $\dfrac{a_j' + j a_j g'}{n g'} = a_j$ e portanto, $a_j(n-j)g' = a_j'$ para todo $j \in \{0, 1, \ldots, n-1\}$. Como $e^{ng} \neq 0$, então algum a_j é não nulo. Logo, temos $(n-j)g' = \dfrac{a_j'}{a_j}$. Também sabemos que a_j não é constante, pois caso ele fosse, teríamos $g' = 0$, o que contradiz o fato de g não ser constante.

Escreva $a_j = \dfrac{p(x)}{q(x)}$, onde $p(x), q(x) \in \mathbb{C}[x]$. Então,

$$\frac{a_j'}{a_j} = \frac{p(x)'q(x) - p(x)q(x)'}{q(x)^2} \cdot \frac{q(x)}{p(x)} = \frac{p(x)'q(x) - p(x)q(x)'}{p(x)q(x)} = \frac{p(x)'}{p(x)} - \frac{q(x)'}{q(x)}.$$

Sabemos que p e q não são ambos constantes, então suponha que $\dfrac{p(x)'}{p(x)}$ é não nulo. Fatorando $p(x)$, obtemos $p(x) = \prod_{k=1}^{d} (x - r_k)^{s_k}$, onde d é a quantidade de raízes distintas de $p(x)$, $d \leq \partial(p(x))$. Temos:

$$\frac{p(x)'}{p(x)} = \frac{(\prod_{k=1}^{d} (x - r_k)^{s_k})'}{\prod_{k=1}^{d} (x - r_k)^{s_k}} = \sum_{k=1}^{d} \frac{s_k (x - r_k)^{s_k - 1}}{(x - r_k)^{s_k}} = \sum_{k=1}^{d} \frac{s_k}{x - r_k}.$$

De forma semelhante, temos:

$$\frac{a_j'}{a_j} = \sum_{m=1}^{c} \frac{s_m}{x - r_m}.$$

Portanto, g' e g devem ter $x - r_m$ como fator em seus denominadores para qualquer m. Logo, $g(x) = h(x)(x - r_m)^{-c}$, onde $x - r_m \nmid h(x)$ e $c > 0$. A derivada de $g(x)$ é $g'(x) = -c \cdot h(x)(x - r_m)^{-(c+1)} + h'(x)(x - r_m)^c$. Esta expressão claramente não pode ter $\dfrac{s_m}{x - r_m}$ como único termo em sua expansão em frações parciais, e portanto $(n-j)g' \neq \dfrac{a'_j}{a_j}$, o que é contradição. Isto prova que e^g é transcendente sobre $\mathbb{C}(x)$. □

Teorema 4.42 (Critério de Liouville)**.** *Sejam f e g duas funções racionais em $\mathbb{C}(x)$. Assuma que $f \neq 0$ e que g não é constante. Então fe^g possui uma primitiva em uma extensão liouvilliana de $\mathbb{C}(x, e^g)$ se, e somente se, existe $a \in \mathbb{C}(x)$ tal que $f = a' + ag'$, ou seja,*

$$\int fe^g \, dx = ae^g.$$

Demonstração.

($\Rightarrow$) Suponha que fe^g possui uma primitiva em uma extensão diferencial elementar de $\mathbb{C}(x, e^g)$. Pelo Teorema 4.40, temos:

$$fe^g = v' + \sum_{i=1}^{n} c_i \frac{u'_i}{u_i},$$

para $c_1, \ldots, c_n \in \mathbb{C}$ e $u_1, \ldots, u_n, v \in \mathbb{C}(x, e^g)$.

Seja $\alpha = e^g$. Pelo Lema 4.41, α é transcendente sobre $\mathbb{C}(x)$ e, portanto, $\dfrac{\alpha'}{\alpha} = g' \in \mathbb{C}(x)$. Então podemos pensar em u_i e v como funções racionais na variável α e coeficientes em $\mathbb{C}(x)$ e aplicar os mesmos argumentos utilizados na demonstração do Caso 3 da Proposição 4.39. Desta forma, há duas possibilidades para cada $i \in \{1, 2, \ldots, n\}$: $u_i = \alpha$ ou $u_i \in \mathbb{C}(x)$. Também, o denominador de v é uma potência de α e podemos escrever $v = \sum_{j=r}^{s} v_j \alpha^j$ para $v_j \in \mathbb{C}(x), r, s \in \mathbb{Z}$. Logo,

$$f \cdot \alpha = \sum_{j=r}^{s} (v'_j + jg'v_j)\alpha^j + cg' + \sum_{i=1}^{n} c_i \frac{u'_i}{u_i}.$$

Comparando os coeficientes de α em cada lado, obtemos que $f = v'_1 + g'v_1$.
Portanto, existe $a \in \mathbb{C}(x)$ tal que $f = a' + ag'$, pois basta tomar $a = v_1$.
($\Leftarrow$) Observe que se $f = a' + ag'$ para algum $a \in \mathbb{C}(x)$, então $fe^g = (ae^g)'$, pois

$$(ae^g)' = a'e^g + ae^g g' = e^g(a' + ag') = fe^g.$$

□

Veremos a seguir exemplos de funções que não admitem primitiva elementar.

Exemplos 4.43.

1. A função $f_1(x) = e^{cx^2}$, $c \in \mathbb{C}^*$ não possui primitiva elementar.

   Solução.

   Seja $c \in \mathbb{C}^*$ arbitrário. Suponha, por absurdo, que $f_1(x) = e^{cx^2}$ possui primitiva elementar. Então, pelo Teorema 4.42, $\int e^{cx^2}\,dx = ae^{cx^2}$ para algum $a \in \mathbb{C}(x)$, isto é, $1 = a' + 2cxa$. Considere $a = \dfrac{p}{q}$, com $p, q \in \mathbb{C}[x]$ primos entre si e $q \neq 0$. Então:

$$\begin{aligned}
& 1 = a' + 2cxa \\
\Leftrightarrow \quad & 1 = \frac{p'q - pq'}{q^2} + 2cx\frac{p}{q} \\
\Leftrightarrow \quad & 1 = \frac{p'q - pq' + 2cxpq}{q^2} \\
\Leftrightarrow \quad & q^2 = p'q - pq' + 2cxpq \qquad (*) \\
\Leftrightarrow \quad & q^2 - p'q - 2cxpq = -pq' \\
\Leftrightarrow \quad & q(q - p' - 2cxp) = -pq'. \qquad (**)
\end{aligned}$$

   Assuma que $\partial(q) > 0$. Então a equação $q = 0$ possui uma raiz α de multiplicidade r ($r > 0$). Como p e q são primos entre si, então $p(\alpha) \neq 0$. Logo, analisando a igualdade $(**)$, α é um zero de multiplicidade $\geq r$ de $q(q - p' - 2cxp)$, mas é um zero de multiplicidade $r - 1$ de $-pq'$. Isto é uma contradição, o que implica que $\partial(q) = 0$.

   Suponha que $q = 1$. Então de $(**)$, obtemos:

$$\begin{aligned}
& q(q - p' - 2cxp) = -pq' \\
\Leftrightarrow \quad & 1(1 - p' - 2cxp) = 0 \\
\Leftrightarrow \quad & p' + 2cxp = 1. \qquad (***)
\end{aligned}$$

   Como $p \in \mathbb{C}[x]$, então $\partial(2cxp) > \partial(p')$ e $\partial(2cxp) > 0$. Logo, analisando a igualdade $(***)$, concluímos que $\partial(p' + 2cxp) > \partial(1)$, o que é uma contradição. Portanto, não existe um polinômio p que satisfaz $(***)$, o que implica que não existe função racional que satisfaz $(*)$. Disto, obtemos então que $f_1(x) = e^{cx^2}$ não possui primitiva elementar. □

2. A função $f_2(x) = \dfrac{e^{cx}}{x}$, $c \in \mathbb{C}^*$ não possui primitiva elementar.

   Solução.

   Seja $c \in \mathbb{C}^*$ arbitrário. Suponha, por absurdo, que $f_2(x) = \dfrac{e^{cx}}{x}$ possui primitiva elementar. Então, pelo Teorema 4.42 tomando $f = \dfrac{1}{x}$ e $g = cx$ (onde $g' = c$), existe $a \in \mathbb{C}(x)$ tal que $\dfrac{1}{x} = a' + ac$. Assuma que a possui decomposição em frações parciais. Obviamente, nenhum termo de a' é igual a $\dfrac{1}{x}$, pois $\displaystyle\int \frac{1}{x}\,dx = \ln x + c$, onde c é constante. Logo a parcela $\dfrac{1}{x}$ deve estar presente em ac e, portanto, $\left(\dfrac{1}{x}\right)' = -\dfrac{1}{x^2}$ deve estar presente em $a'c$, o que implica que $-\dfrac{1}{cx^2}$ deve estar presente em a'. Então, a parcela $\dfrac{1}{cx^2}$ deve estar em ac para cancelar $-\dfrac{1}{cx^2}$ e, portanto, $\left(\dfrac{1}{cx^2}\right)' = -\dfrac{2}{cx^3}$ deve estar presente em $a'c$, o que implica que $-\dfrac{2}{c^2x^3}$ deve estar presente em a'. Pelo mesmo argumento, a parcela $\dfrac{2}{c^2x^3}$ deve estar em ac para cancelar $-\dfrac{2}{c^2x^3}$. Esta regressão continua infinitamente, o que é impossível. Logo, $f_2(x) = \dfrac{e^{cx}}{x}$ não possui primitiva elementar. □

3. A função $f_3(x) = x^2e^{x^2}$ não possui primitiva elementar.

   Solução.

   Resolvendo a integral pela técnica de integração por partes, obtemos:

$$\int x^2e^{x^2}\,dx = \frac{xe^{x^2}}{2} - \frac{1}{2}\int e^{x^2}\,dx.$$

   Vimos anteriormente que $f_1(x) = e^{cx^2}$, $c \in \mathbb{C}^*$ não possui primitiva elementar. Em especial, e^{x^2} não possui primitiva elementar. Portanto, $f_3(x) = x^2e^{x^2}$ também não possui primitiva elementar. □

4. A função $f_4(x) = \dfrac{1}{\ln x}$ não possui primitiva elementar.

   Solução.

   Se $u = \ln x$, então $x = e^u$, e $\displaystyle\int \frac{1}{\ln x}\,dx = \int \frac{e^u}{u}\,du$. Vimos anteriormente que $f_2(x) = \dfrac{e^{cx}}{x}$, $c \in \mathbb{C}^*$ não possui primitiva elementar. Em especial, $\dfrac{e^u}{u}$ não possui primitiva elementar. Logo, $f_4(x) = \dfrac{1}{\ln x}$ também não possui primitiva elementar. □

5. A função $f_5(x) = \dfrac{\operatorname{sen} x}{x}$ não possui primitiva elementar.

Solução.

Sabemos que $\operatorname{sen}(x) = \dfrac{e^{ix} - e^{-ix}}{2i}$. Então, $\operatorname{sen}(iu) = \dfrac{e^{-u} - e^{u}}{2i}$. Tomando a substituição $x = iu$, segue que $\frac{dx}{du} = i$. Então:

$$\int \frac{\operatorname{sen} x}{x}\, dx = \int \frac{\operatorname{sen}(iu)}{u}\, du = \frac{1}{2i} \int \frac{e^{-u} - e^{u}}{u}\, du.$$

Então basta mostrarmos que $\displaystyle\int \frac{e^{-x} - e^{x}}{x}\, dx$ não é elementar.

Suponha que $\dfrac{e^{-x} - e^{x}}{x}$ possui uma primitiva em uma extensão diferencial elementar de $\mathbb{C}(x, e^x)$. Pelo Teorema 4.40, temos:

$$\frac{e^{-x} - e^{x}}{x} = v' + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i},$$

para $c_1, \ldots, c_n \in \mathbb{C}$ e $u_1, \ldots, u_n, v \in \mathbb{C}(x, e^x)$.

Seja $\alpha = e^x$. Sabemos que α é transcendente sobre $\mathbb{C}(x)$ e, portanto, $\dfrac{\alpha'}{\alpha} = x' = 1$. Então podemos pensar em u_i e v como funções racionais na variável α e coeficientes em $\mathbb{C}(x)$ e aplicar os mesmos argumentos utilizados na demonstração do Caso 3 da Proposição 4.39. Desta forma, há duas possibilidades para cada $i \in \{1, 2, \ldots, n\}$: $u_i = \alpha$ ou $u_i \in \mathbb{C}(x)$. Também, o denominador de v é uma potência de α e podemos escrever $v = \displaystyle\sum_{j=r}^{s} v_j \alpha^j$ para $v_j \in \mathbb{C}(x), r, s \in \mathbb{Z}$. Logo,

$$\frac{\alpha^{-1} - \alpha}{x} = \sum_{j=r}^{s} (v_j' + j v_j)\alpha^j + c + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i}.$$

Comparando os coeficientes de α em cada lado, obtemos que

$$\frac{1}{x}(\alpha^{-1} - \alpha) = (v_{-1}' - v_{-1})\alpha^{-1} + (v_1' + v_1)\alpha.$$

Portanto, deduzimos que $\dfrac{1}{x} = v_{-1}' - v_{-1}$, o que é impossível como vimos no item 2 dos Exemplos 4.43. □

6. A função $f_6(x) = \ln(\operatorname{arcsen} x)$ não possui primitiva elementar.

   Solução.

   Se $x = \operatorname{sen}\theta$, então $\dfrac{dx}{d\theta} = \cos\theta$. Aplicando esta substituição e resolvendo a integral pela técnica de integração por partes, obtemos:

$$\int \ln(\operatorname{arcsen} x)\, dx = \int \ln(\theta)\cos(\theta)\, d\theta = \ln(\theta)\operatorname{sen}(\theta) - \int \frac{\operatorname{sen}\theta}{\theta}\, d\theta.$$

   Vimos anteriormente que $f_5(x) = \dfrac{\operatorname{sen} x}{x}$ não possui primitiva elementar. Portanto, $f_6(x) = \ln(\operatorname{arcsen} x)$ também não possui primitiva elementar. □

Referências

[1] BRZEZINSKI, J. **Galois Theory through Exercises.** Springer, 2018.

[2] CHAMBERT-LOIR, A. **A field guide to algebra.** New York: Springer, 2005.

[3] CRESPO, T.; HAJTO, Z. **Introduction to Differential Galois Theory.** Cracow: Wydawnictwo PK, 2007.

[4] DUMMIT, D.; FOOTE, R. **Abstract algebra.** 3. ed. Hoboken: John Wiley & Sons, 2004.

[5] ESCOFIER, J. **Galois theory.** New York: Springer, 2001.

[6] GALOIS, E. **The Last Mathematical Testament of Galois.** Tradução de: SINGH, A. R. Disponível em: `https://www.ias.ac.in/article/fulltext/reso/004/10/0093-0100`. Acesso em: 29 nov. 2021.

[7] GONÇALVES, A. **Introdução à álgebra.** 5. ed. Rio de Janeiro: IMPA, 2015.

[8] JAYARAM V. **Proving the non-existence of elementary anti-derivatives for certain elementary functions.** 2017.

[9] MACTUTOR history of mathematics archive. Disponível em: `https://mathshistory.st-andrews.ac.uk/` Acesso em: 29 nov. 2021.

[10] MEAD, D. G. Integration. **The American Mathematical Monthly,** v. 68, n. 2, p. 152-156, fev. 1961.

[11] PIERPONT, J. **Early History of Galois Theory of Equations.** 1898. Disponível em: `https://projecteuclid.org/download/pdf_1/euclid.bams/1183415320`. Acesso em: 29 nov. 2021.

[12] ROSENLICHT, M. Integration in Finite Terms. **The American Mathematical Monthly,** v. 79, n. 9, p. 963-972, nov. 1972.

[13] SIMON, B. **An introduction to differential galois theory.** 2015. Disponível em: `http://math.sfsu.edu/serkan/expository/bruceSimonExpository.pdf`. Acesso em: 29 nov. 2021.

[14] SIU, M. Integration in Finite Terms: From Liouville's Work to the Calculus Classroom of Today. In: CALINGER R. **Vita Mathematica: Historical Research and Integration with Teaching.** Mathematical Association of America Notes and Reports, n. 40, 1996, p. 321-330.

[15] STEWART, I. **Galois theory.** 3. ed. Boca Raton: Chapman & Hall/CRC, 2004.

[16] TENGAN, E.; BORGES, H. **Álgebra comutativa em quatro movimentos.** Rio de Janeiro: IMPA, 2015.

[17] WOOD, A. **Non-linear Differential Galois Theory.** 2017.

[18] WU, J. **Galois Correspondence and Liouvillian Extensions.** Disponível em: `https://www.uni-due.de/~hm0002/Lehre/Galois_Correspondence_and_Liouvillian_Extensions-2.pdf`. Acesso em: 29 nov. 2021.