UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS BLUMENAU
LICENCIATURA EM MATEMÁTICA

Victor Afonso Garcia Schmitz

UM NORMAL ESTUDO SOBRE A TEORIA DE GALOIS

Blumenau
2022

Victor Afonso Garcia Schmitz

UM NORMAL ESTUDO SOBRE A TEORIA DE GALOIS

Trabalho de Conclusão de Curso de Graduação em Licenciatura em Matemática do Campus Blumenau da Universidade Federal de Santa Catarina para a obtenção do título de Licenciado em Matemática.
Orientador: Prof. Rafael Aleixo de Carvalho, Dr.

Blumenau
2022

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Schmitz, Victor
UM NORMAL ESTUDO SOBRE A TEORIA DE GALOIS / Victor Schmitz ; orientador, Rafael Aleixo de Carvalho, 2022.
141 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Campus Blumenau, Graduação em Matemática, Blumenau, 2022.

Inclui referências.

1. Matemática. 2. Teoria de Galois. I. Aleixo de Carvalho, Rafael. II. Universidade Federal de Santa Catarina. Graduação em Matemática. III. Título.

Victor Afonso Garcia Schmitz

UM NORMAL ESTUDO SOBRE A TEORIA DE GALOIS

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do Título de Licenciado em Matemática e aprovado em sua forma final pelo Curso de Licenciatura em Matemática.

Blumenau, 16 de dezembro de 2022.

Documento assinado digitalmente
Francis Felix Cordova Puma
Data: 28/12/2022 12:41:45-0300
CPF: ***.649.087-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Francis Felix Cordova, Dr.
Coordenador do Curso

Banca Examinadora:

Documento assinado digitalmente
Rafael Aleixo de Carvalho
Data: 28/12/2022 07:41:38-0300
CPF: ***.494.178-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Rafael Aleixo de Carvalho, Dr.
Orientador
Universidade Federal de Santa Catarina - UFSC

Documento assinado digitalmente
Felipe Vieira
Data: 28/12/2022 09:12:13-0300
CPF: ***.601.639-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Felipe Vieira, Dr.
Avaliador
Universidade Federal de Santa Catarina - UFSC

Prof. Jorge Luiz Deolindo Silva, Dr.
Avaliador
Universidade Federal de Santa Catarina - UFSC

AGRADECIMENTOS

Primeiramente, gostaria de agradecer à minha namorada, Janaína Stein, por seu suporte, tanto ao longo de minha graduação, quanto ao longo do meu TCC, para que eu me mantivesse constante em minhas atividades na graduação. Por sua compreensão em relação aos dias e noites que passei longe dela, escrevendo este trabalho e fazendo outras atividades necessárias para minha formação. Pelos momentos de lazer que passamos juntos, desde meu segundo semestre da graduação, que foi quando a conheci, que me relembraram inúmeras vezes que a vida é muito mais que a faculdade. Pelas nossas conquistas, que me fizeram ter certeza de que estamos no caminho certo. Ela, com certeza, é uma figura indispensável e insubstituível que está ao meu lado, e meu amor e gratidão por ter ela em minha vida é imensurável (ou, ao menos, não enumerável).

Agradeço à minha família, por me dar os recursos necessários para que eu pudesse fazer meu curso com tranquilidade, e sempre ter me apoiado na minha escolha de graduação.

Agradeço aos meus colegas por terem feito o período em que estávamos na faculdade, em aula, mais leve e divertido.

Agradeço a todos os docentes com que já tive o prazer de ter aulas, todos foram muito importantes à minha formação. Em especial, aos professores Francis Felix e Eleomar Cardoso, que ministraram as disciplinas de Análise. Ao professor Júlio Corrêa, que ministrou de forma excelente as matérias de Educação Matemática e, também, Filosofia da Matemática. À professora Laís Gereti, que foi de extrema ajuda nas disciplinas de Estágio Supervisionado. Ao professor Luís Rafael, que ministrou a disciplina de Métodos Numéricos. Ao professor Roger Beiling, que tive o prazer de ter aulas no início da graduação em Introdução ao Cálculo e Cálculo I, que sempre estimulou nosso

conhecimento matemático com exemplos muito interessantes em suas aulas, sempre fazendo referências às matérias posteriores que teríamos no curso. A professora Naiara Costa, por seu trabalho excepcional na disciplina de Geometrias Não-Euclidianas. Bruno Tadeu, que foi fundamental nos treinamentos das olimpíadas que realizamos em 2019-2020, e é o membro suplente da banca. Também, o professor Jorge Deolindo, que aceitou participar da banca desse trabalho, e sempre ouvi coisas boas sobre, apesar de nunca ter tido aula com ele.

De forma ainda mais especial, agradeço aos professores Felipe Vieira e Rafael Aleixo que foram os professores que, com certeza, mais me ajudaram e influenciaram durante a graduação. Além de terem ministrado muitas matérias a mim, com o professor Aleixo ministrando as disciplinas de Álgebra Linear e Álgebra II, e o professor Vieira ministrando Álgebra I, que foram os principais motivos para que meu interesse em Álgebra tenha sido mais forte quando comparado às outras matérias.

Também foram os professores que me acolheram e orientaram desde o primeiro semestre de minha graduação, quando começamos os nossos encontros semanais de iniciação científica. Sem esses dois professores a minha formação e meu conhecimento teriam sido apenas uma fração do que é atualmente.

E, é claro, que, além do que foi mencionado até então, sou muito grato por ter o professor Aleixo como orientador. Ele que tomou a iniciativa para que eu estudasse álgebra desde cedo em minha graduação, iniciando o estudo de grupos em meu terceiro semestre, assim permitindo que eu desenvolvesse tópicos mais avançados em minhas iniciações científicas e, claro, nesse trabalho. Também, fez um trabalho fundamental com as recomendações de referências ao longo de minha graduação.

RESUMO

Este trabalho tem como principal objeto o desenvolvimento dos principais tópicos e aplicações da Teoria de Galois, geralmente presentes em um curso introdutório sobre o tema. Essa teoria consiste no estudo de corpos e suas extensões, a partir de um grupo associado a essa extensão, chamado de 'grupo de Galois'. O grupo de Galois de uma extensão permite criar uma ponte entre a Teoria de Corpos e a Teoria de Grupos, pode-se, então, derivar propriedades sobre os corpos a serem investigados, olhando apenas para seu grupo de Galois, e vice-versa. Não é, porém, qualquer extensão que tem acesso à essa poderosa ferramenta, as extensões que possuem uma relação útil com algum grupo precisam satisfazer duas condições: separabilidade e normalidade, e o estudo dessas condições é feito por meio dos morfismos entre extensões de corpos e os anéis de polinômios gerados por cada corpo. Uma vez que essas propriedades são bem estabelecidas, é possível utilizar as ferramentas desenvolvidas para diversas aplicações. Nesse trabalho, foi dada atenção à duas em específico: construções geométricas com régua e compasso, e a resolução de equações polinomiais.

Palavras-chave: Extensões de corpos. Teoria de Galois. Construções geométricas. Solubilidade por radicais

ABSTRACT

The main goal of this final paper is to develolp the key topics and applications of Galois Theory, which would be generally covered in an introductory course in the subject. This theory consists in the study of fields and their extensions, by making the use of groups that correspond with said extensions, called "Galois groups". The Galois group of an extension creates a bridge between the subjects of Field Theory and Group Theory, which enables the use of group properties to gather information about the corresponding field extension, and vice-versa. However, not all field extensions have access to this powerful tool, for there to be a useful relationship between an extension and a Galois group, the field extension must, first, satisfy two conditions: normality and sepparability, and the study of these two properties is done in terms of morphisms between field extensions and the properties of the polynomials rings made up by each field. Once these properties are well-established, its possible to use the theory that was develolped in many different applications. In this final paper, the attention was focused on two particular applications: geometric constructions with ruler and compass, and the solvability of polynomial equations in terms of radicals.

Keywords: Field extensions. Galois Theory. Geometric constructions. Solvability by radicals.

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho tem como objetivo geral apresentar os principais resultados e aplicações da Teoria de Galois, geralmente vistos em um curso introdutório sobre o tema.

O estudo foi realizado a partir de livros didáticos que abordavam a Teoria de Galois, e foram utilizados tanto livros desenvolvidos por autores nacionais, quanto internacionais. A partir dos conteúdos desses livros, buscou-se fazer uma síntese dos temas abordados, assim como o desenvolvimento de alguns pontos que foram não estavam bem desenvolvidos. As principais fontes, aqui, foram [4] e [2], que influenciaram, majoritariamente, a escrita dos capítulos 2, 3, e 6. Para alguns resultados auxiliares dos capítulos 4, 5 e 6, foram usados também os textos [1] e [3], respectivamente.

A teoria de Galois consiste, basicamente, no estudo dos corpos e suas extensões a partir de suas simetrias, isto é, seu grupo de automorfismos. Isso permite traçar um paralelo entre a Teoria de Corpos e a Teoria de Grupos, permitindo assim utilizar as ferramentas de ambas a teorias para o estudo das propriedades dos corpos.

Esse trabalho é divido em 5 partes. A primeira parte é o Capítulo 2, que contém o desenvolvimento do maquinário necessário para o estudo aprofundado de extensões e suas propriedades. É desenvolvido os conceitos de extensões algébricas e finitas, o conceito de polinômio minimal de elementos algébricos e morfismos entres extensões.

Uma vez que essas propriedades básicas sobre extensões de corpos estão estabelecidas, é feito um estudo da Teoria de Galois no Capítulo 3. Nesse capítulo é feito o estudo de duas propriedades de extensões: normalidade e separabilidade. Essas propriedades garantem que a correspondência entre a Teoria de Corpos e a Teoria de Grupos ocorra de forma “bem comportada”.

As extensões que são normais e separáveis são ditas ser galoisianas e são as extensões mais importantes neste trabalho. Cada extensão galoisiana está relacionada a um chamado "grupo de Galois", que é o grupo de automorfismos dessa extensão. Em extensões galoisianas, as propriedades da extensão são refletidas nas propriedades de seu grupo de Galois, e vice-versa. Esse fato é chamado de "O Teorema Fundamental da Teoria de Galois", que é a principal ferramenta que será utilizado posteriormente ao Capítulo 3.

No Capítulo 4 é feito um estudo detalhado sobre um tipo específico de extensões galoisianas, que são as chamadas "extensões ciclotômicas". Essas extensões são importantes pois tem uma propriedade particular: elas têm grupo de Galois abeliano. Elas não são as únicas extensões galoisianas cujo grupo de Galois é abeliano (nesse caso a extensão é chamada de abeliana), porém são, de certa forma, as mais fundamentais. Além disso, elas nos dão uma maneira geral de construir extensões abelianas que funciona com (quase) qualquer corpo, o que é uma particularidade das extensões ciclotômicas (outras construções conhecidas de extensões abelianas geralmente requerem hipóteses extras no corpo original), e são de grande importância nos capítulos posteriores.

Os Capítulos 5 e 6 apresentam algumas aplicações clássicas da Teoria de Galois. O Capítulo 5 é uma aplicação dessa teoria na classificação dos números e pontos construtíveis por régua e compasso. Essa classificação leva a muitos resultados interessantes na geometria, como a caracterização dos polígonos regulares construtíveis.

O Capítulo 6, por fim, é uma aplicação da Teoria de Galois à resolução d equações polinomiais de grau 3, assim como a demonstração do conhecido fato de que não existe fórmula para a resolução de equações polinomiais de grau maior ou igual a 5.

Para os pré-requisitos, assume-se, aqui, que o leitor já tenha

um conhecimento básico sobre alguns tópicos abordados em uma graduação em licenciatura em matemática, sendo eles:

- Álgebra Linear (equivalente a um curso de um semestre, que mostra as principais propriedades de espaços vetoriais de dimensão finita e as transformações lineares entre eles).
- Cálculo e análise (derivadas e conjuntos enumeráveis).
- Álgebra (equivalente a dois cursos introdutórios, que contém os básicos sobre grupos, anéis e corpos, e, em particular, anéis de polinômios, critérios de irredutibilidade de polinômios, domínios euclidianos, principais, de fatoração única, e o primeiro Teorema de Sylow).
- Teoria dos Números (fatorações primas, propriedades do mmc, mdc, e funções aritméticas, em particular, a função totiente de Euler).
- Teoria dos Conjuntos (propriedades de imagens diretas, inversas, operações com conjuntos)
- Conjuntos parcialmente ordenados (diagramas de Hasse, Lema de Zorn)
- Noções básicas de Teoria das Categorias (definição de diagramas comutativos apenas, que pode ter sido abordada em uma aula de álgebra), nota-se aqui que, nos diagramas comutativos, morfismos injetores são denotadas por $\hookrightarrow$ e sobrejetores por $\twoheadrightarrow$. Além, no caso em que não há símbolo acompanhado da flecha $\hookrightarrow$ nos diagramas, assume-se que o morfismo correspondente é a inclusão.

Nesse trabalho, os símbolos $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ são reservados aos conjuntos dos números naturais, inteiros, racionais, reais e complexos, respectivamente. Além disso, 0 não é considerado um número natural.

2 EXTENSÕES DE CORPOS

2.1 EXTENSÕES ALGÉBRICAS E TRANSCENDENTES

Iniciaremos nosso estudo definindo precisamente o que é uma extensão de corpos.

Definição 2.1. Seja L um corpo e K um subcorpo de L. Nessas condições, L é dito ser uma extensão de K, e a configuração dos corpos como um todo é dita ser uma extensão de corpos, denotada por L/K.

Perceba que uma "extensão de corpos" não é uma estrutura algébrica. Ela representa, apenas, a relação de subcorpo entre os corpos L e K. Ou seja, o símbolo L/K não representa um corpo.

Definição 2.2. Se $C \subseteq L$ é um subconjunto qualquer, denotamos por $K[C]$ o menor subanel de L que contém C e K simultaneamente. Mais precisamente, $K[C]$ é a intersecção de todos os subanéis de L que contém C.

De forma similar, $K(C)$ é a intersecção de todos os subcorpos de L que contém K e C simultaneamente. Caso $C = \{\theta_1, \ldots, \theta_n\}$, o uso das chaves é dispensado. Nesse caso, pode-se escrever esse corpo explicitamente desta maneira

$$K(\theta_1, \ldots, \theta_n) = \{f(\theta_1, \ldots, \theta_n) : f \in K(x_1 \ldots, x_n)\}.$$

Aqui, $K(x_1, \ldots, x_n)$ é o corpo das expressões racionais em n variáveis, e $f(\theta_1, \ldots, \theta_n)$ é a expressão racional $f(x_1, \ldots, x_n)$ avaliada na n-upla $(\theta_1, \ldots, \theta_n)$.

Na notação dessa definição, caso em que C é um conjunto finito, digamos $C = \{\theta_1, \ldots, \theta_n\}$, denotamos $K[C]$ por $K[\theta_1, \ldots, \theta_n]$. Além disso, $K[\theta_1, \ldots, \theta_n]$ pode ser explicitamente escrito da seguinte forma

$$K[\theta_1, \ldots, \theta_n] = \{f(\theta_1, \ldots, \theta_n) : f \in K[x_1, \ldots, x_n]\},$$

onde $K[x_1, \ldots, x_n]$ é o anel de polinômios em n variáveis com coeficientes em K, e $f(\theta_1, \ldots, \theta_n)$ é o polinômio $f(x_1, \cdots, x_n)$ avaliado na n-upla $(\theta_1, \cdots, \theta_n)$.

Se D é um domínio de integridade, denotaremos por $\mathrm{Frac}(D)$ seu corpo de frações. E, caso $\phi : A \to B$ seja um morfismo entre anéis ou grupos, $\mathrm{Ker}(\phi)$ denota o núcleo desse morfismo.

Proposição 2.3. Seja L/K uma extensão de corpos e C um subconjunto qualquer de L. Então, $K(C) = \mathrm{Frac}(K[C])$.

Demonstração. Considere o morfismo $\phi : \mathrm{Frac}(K[C]) \to K(C)$, definido por $\phi(\frac{a}{b}) = ab^{-1}$.

Perceba que ϕ é injetora. De fato, caso $\phi(\frac{a}{b}) = 0$, teríamos que $ab^{-1} = 0$. Isso ocorre apenas se $a = 0$, visto que $b^{-}1 \neq 0$. Podemos, a partir disso, concluir que $\mathrm{Ker}(\phi) = \{0\}$, onde $\mathrm{Ker}(\phi)$ representa o núcleo da aplicação ϕ. Segue então que ϕ é injetora.

Para ver que ϕ é sobrejetora, perceba que $\phi(\mathrm{Frac}(K[C]))$ é um subcorpo de $K(C)$, visto que é isomorfo a $\mathrm{Frac}(K[C])$, pois ϕ é injetora. Por outro lado, $K(C)$ é, por definição, a intersecção de todos os corpos que contém K e C simultaneamente, e $\phi(\mathrm{Frac}(K[C]))$ contém esses conjuntos, pois são formados pelas imagens dos elementos da forma $\frac{x}{1}$ onde $x \in K$ ou $x \in C$. Assim, $K(C)$ deve estar contido, por definição, em $\phi(\mathrm{Frac}(K))$, portanto $K(C) = \phi(\mathrm{Frac}(K[C]))$, provando, assim, a sobrejetividade de ϕ. □

Exemplo 2.4. Todo corpo K admite pelo menos uma extensão. Basta considerar o corpo de expressões racionais em uma variável $K(x)$. Assim temos a extensão $K(x)/K$.

Exemplo 2.5. Seja K um corpo, L uma extensão de K, e $\alpha \in K$ um elemento ‘ ´sem raiz quadrada” em K, porém “com raiz quadrada” em

L. Em termos mais precisos, $\beta^2 \neq \alpha$ para qualquer $\beta \in K$, e existe um elemento $\sqrt{\alpha} \in L$ onde $(\sqrt{\alpha})^2 = \alpha$.

Afirmamos que $K(\sqrt{\alpha}) = \{x + y\sqrt{\alpha} : x, y \in K\}$. Ainda mais, $\{1, \sqrt{\alpha}\}$ são linearmente independentes sobre K e, portanto, formam uma base de $K(\sqrt{\alpha})$ se visto como um K-espaço vetorial.

Vamos, primeiro, mostrar a igualdade entre os conjuntos. A inclusão $\supseteq$ é clara, pela definição de $K(\sqrt{\alpha})$. Para a inclusão oposta, note que $\{x + y\sqrt{\alpha} : x, y \in K\}$, que denotaremos por M, é um subcorpo de L.

Com efeito, é claro que $0, 1 \in K(\sqrt{\alpha})$, e as operações de soma e produto são fechadas em M, visto que, para quaisquer $a_1, a_2, b_1, b_2 \in K$,

$$(a_1 + b_1\sqrt{\alpha}) + (a_2 + b_2\sqrt{\alpha}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{\alpha} \in M,$$
$$(a_1 + b_1\sqrt{\alpha})(a_2 + b_2\sqrt{\alpha}) = (a_1a_2 + \alpha b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{\alpha} \in M.$$

Além disso, para quaisquer $a, b \in K$, o oposto de $a + b\sqrt{\alpha}$ é $(-a) + (-b)\sqrt{\alpha}$, que está em M. Também, caso $b \neq 0$, o inverso de $a + b\sqrt{\alpha}$ é dado por $\frac{a-b\sqrt{\alpha}}{a^2-\alpha b^2}$ (perceba que, caso $b = 0$ e $a \neq 0$, a existência do inverso multiplicativo de $a + b\sqrt{\alpha}$ é trivial, pois $a \in K$).

A verificação desses fatos é imediata, basta operar os elementos. Só precisamos garantir que $a^2 - \alpha b^2 \neq 0$ para que $\frac{a-b\sqrt{\alpha}}{a^2-\alpha b^2}$ esteja bem definido. Isso, de fato, ocorre, pois se tivéssemos $a^2 - \alpha b^2 = 0$, teríamos que $\alpha = (a/b)^2$. Mas isso é um absurdo, visto que $a/b \in K$, e α não tem raiz quadrada nesse corpo.

Ou seja, se $(a, b) \neq (0, 0)$, $a + b\sqrt{\alpha}$ tem elemento inverso em $\{x + y\sqrt{\alpha} : x, y \in K\}$, logo também é não nulo, o que mostra a independência linear de 1 e $\sqrt{\alpha}$. Portanto, tal conjunto é um corpo, e como $K(\sqrt{\alpha})$ é o menor subcorpo de L que contém tanto K como $\sqrt{\alpha}$, devemos ter que $K(\sqrt{\alpha}) \subseteq \{x + y\sqrt{\alpha} : x, y \in K\}$. Como já mostramos a inclusão oposta anteriormente, a igualdade está provada.

Definição 2.6. Extensões de corpos que são geradas a partir da adjunção de uma raiz quadrada são chamadas de extensões quadráticas, e o corpo gerado é dito ser um corpo quadrático.

Mais geralmente, extensões que fazem a adjunção de alguma raiz n-ésima de um elemento são chamadas de extensões radicais n-ésimas.

Extensões radicais serão a nossa fonte mais rica de exemplos e terão um papel fundamental quando estudarmos, no Capítulo 6, a solubilidade de equações polinomiais por meio de fórmulas que envolvem a extração de radicais.

Exemplo 2.7. Afirmamos que

$$\mathbb{Q}(\sqrt{3},\sqrt{5}) = \{a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15} : a, b, c, d \in \mathbb{Q}\}$$

Com efeito, pelo Exemplo 2.5, sabemos que $\{1, \sqrt{3}\}$ forma uma base de $\mathbb{Q}(\sqrt{3})$ como $\mathbb{Q}$-espaço vetorial. Perceba, também, que $\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$, pois caso contrário, teríamos que existem $a, b \in \mathbb{Q}$ onde

$$(a+b\sqrt{3})^2 = 5 \implies (a^2+3b^2)+(2ab)\sqrt{3} = 5 \implies \begin{cases} .a^2 + 3b^2 = 5 \\ 2ab = 0 \end{cases}$$

A segunda igualdade nos diz que $a = 0$ ou $b = 0$, entretanto, ambos os casos são impossíveis: se $a = 0$, então $3b^2 = 5 \implies b = \sqrt{15}/3 \notin \mathbb{Q}$, por outro lado, se $b = 0$, teríamos que $a^2 = 5 \implies a = \sqrt{5} \notin \mathbb{Q}$. Ou seja, ambas as opções nos levam a absurdos.

Assim, também pelo Exemplo 2.5, $\{1, \sqrt{5}\}$ forma uma base de $\mathbb{Q}(\sqrt{3},\sqrt{5})$ como $\mathbb{Q}(\sqrt{3})$-espaço vetorial, portanto

$$\begin{aligned} \mathbb{Q}(\sqrt{3},\sqrt{5}) &= \{x + y\sqrt{5} : x, y \in \mathbb{Q}(\sqrt{3})\} \\ &= \{(a + b\sqrt{3}) + (c + d\sqrt{3})\sqrt{5} : a, b, c, d \in \mathbb{Q}\} \\ &= \{a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15} : a, b, c, d \in \mathbb{Q}\}. \end{aligned}$$

Ainda mais, $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$ forma uma base de $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ como $\mathbb{Q}$-espaço vetorial. De fato, já mostramos que ele é gerado pelas combinações $\mathbb{Q}$-lineares desses elementos. Para mostrar a independência linear sobre $\mathbb{Q}$, perceba que

$$\begin{aligned} a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15} = 0 &\iff (a + b\sqrt{3}) + (c + d\sqrt{3})\sqrt{5} = 0 \\ &\iff \begin{cases} a + b\sqrt{3} = 0 \\ c + d\sqrt{3} = 0, \end{cases} \\ &\iff a = b = c = d = 0, \end{aligned}$$

o que mostra a independência linear.

Exemplo 2.8. Vamos achar uma descrição da extensão do racionais $\mathbb{Q}(\sqrt{1+\sqrt{2}})$. Para isso, considere a cadeia de corpos

$$\mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right) \supseteq \mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}.$$

Primeiramente, note que a inclusão $\mathbb{Q}(\sqrt{1+\sqrt{2}}) \supseteq \mathbb{Q}(\sqrt{2})$ realmente se verifica, já que $\sqrt{2} = (\sqrt{1+\sqrt{2}})^2 - 1 \in \mathbb{Q}(\sqrt{1+\sqrt{2}})$.

Como já sabemos, o corpo $\mathbb{Q}(\sqrt{2})$ é um $\mathbb{Q}$-espaço vetorial de dimensão 2, com base $\{1, \sqrt{2}\}$. A partir disso, veja que $\sqrt{1+\sqrt{2}} \notin \mathbb{Q}(\sqrt{2})$, pois

$$\begin{aligned} (a + b\sqrt{2})^2 = 1 + \sqrt{2} &\iff (a^2 + 2b^2) + (2ab)\sqrt{2} = 1 + \sqrt{2} \\ &\iff \begin{cases} a^2 + 2b^2 = 1 \\ 2ab = 1. \end{cases} \end{aligned}$$

Isolando $b = 1/(2a)$ e substituindo na primeira equação, obtemos a equação $a^2 + \frac{1}{2a^2} = 1$, que equivale a $2(a^2)^2 - 2a^2 + 1 = 0$. Essa é uma equação de segundo grau de variável a^2. Resolvendo ela, obtemos que $a^2 = 1 \pm i$, porém isso não é possível para $a \in \mathbb{Q}(\sqrt{2})$,

visto que qualquer número real, quando elevado ao quadrado, não pode ser complexo.

Assim, pelo Exemplo 2.5, $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ tem base, como $\mathbb{Q}(\sqrt{2})$-espaço vetorial, igual a $\{1, \sqrt{1+\sqrt{2}}\}$. Portanto, seguindo o mesmo raciocínio do Exemplo 2.7,

$$\begin{aligned}
&\mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right) \\
&= \left\{ x + y\sqrt{1+\sqrt{2}} : x, y \in \mathbb{Q}(\sqrt{2}) \right\} \\
&= \left\{ (a+b\sqrt{2}) + (c+d\sqrt{2})\sqrt{1+\sqrt{2}} : a, b, c, d \in \mathbb{Q} \right\} \\
&= \left\{ a + b\sqrt{2} + c\sqrt{1+\sqrt{2}} + d\sqrt{2+2\sqrt{2}} : a, b, c, d \in \mathbb{Q} \right\}.
\end{aligned}$$

Além disso, $\left\{1, \sqrt{2}, \sqrt{1+\sqrt{2}}, \sqrt{2+2\sqrt{2}}\right\}$ é uma base desse corpo quando visto como $\mathbb{Q}$-espaço vetorial. A verificação é feita de forma análoga à que foi feita no Exemplo 2.7.

Vamos estudar agora as estruturas algébricas das extensões de corpos, começando pela definição de algebricidade para elementos e extensões.

Definição 2.9. Seja L/K uma extensão de corpos e $\theta \in L$.

(i) θ é dito ser algébrico sobre K se ele é raiz de algum polinômio não nulo $f(x) \in K[x]$, caso contrário, ele é dito ser um elemento transcendente sobre K.

(ii) L/K é dita ser uma extensão algébrica se todo elemento de L é algébrico sobre K e, caso contrário, uma extensão transcendente.

Elementos algébricos sobre um corpo K podem ser entendidos como elementos "não muito estranhos" ao corpo, que satisfazem algum

tipo de relação polinomial com os elementos de K. As extensões algébricas de K, também, podem ser vistas como extensões que adicionam apenas raízes de alguns polinômios com coeficientes em K.

Exemplo 2.10. A extensão $K(x)/K$ é transcendente para qualquer K. Com efeito, o monômio $x \in K(x)$ claramente não é raiz de nenhum polinômio não nulo de $K[x]$, pela igualdade, aparentemente óbvia, $f(x) = f(x) \neq 0$ (aqui, o lado esquerdo representa a avaliação do polinômio f no elemento x, enquanto o lado direito representa a expressão polinomial) para qualquer $f(x) \in K[x] \setminus \{0\}$. Ou seja, o monômio x é um elemento transcente explícito.

Exemplo 2.11. Toda extensão quadrática $K(\sqrt{\alpha})/K$ é algébrica, pois cada elemento $a + b\sqrt{\alpha} \in K(\sqrt{\alpha})$ é raiz do polinômio $(x-a)^2 - \alpha b^2 \in K[x]$. Em particular, a extensão $\mathbb{C}/\mathbb{R}$ é algébrica, visto que $\mathbb{C} = \mathbb{R}(\sqrt{-1})$.

Exemplo 2.12. A extensão $\mathbb{R}/\mathbb{Q}$ é transcendente. Para ver isso, perceba que $\mathbb{Q}_n[x] = \{f(x) \in \mathbb{Q}[x] : \deg(f(x)) \leq n\}$ é um conjunto enumerável, pois tem a mesma cardinalidade que $\mathbb{Q}^{n+1}$, por meio da bijeção óbvia que toma os coeficientes e os transforma e uma $(n+1)$-upla, e esse conjunto é enumerável pois $\mathbb{Q}$ é enumerável, e o produto de enumeráveis é enumerável.

Também, o conjunto $V(f(x)) := \{\theta \in \mathbb{R} : f(\theta) = 0\}$ é finito (portanto enumerável), o que implica que o conjunto $V(\mathbb{Q}_n[x]) := \bigcup_{f(x) \in \mathbb{Q}_n[x]} V(f(x))$ é enumerável (união enumerável de enumeráveis é enumerável). Assim, o conjunto dos números reais que são algébricos sobre $\mathbb{Q}$ é $\bigcup_{n \in \mathbb{N}} V(\mathbb{Q}_n[x])$, que é enumerável pelo mesma razão de antes. Como $\mathbb{R}$ é não enumerável, segue que $\mathbb{R}$ contém elementos trascendentes.

Perceba que esse raciocínio funciona analogamente no caso geral: se L/K é uma extensão de corpos onde K é enumerável e L é não enumerável, então L contém elementos transcendentes sobre K.

2.2 O POLINÔMIO MINIMAL

Vimos na seção anterior que elementos algébricos sobre um corpo base K são aqueles que satisfazem uma relação polinomial com os elementos desse corpo.

Nessa seção veremos que, dentre todas essas relações polinomiais que um elemento algébrico tem sobre K, existe uma que pode ser considerada a relação polinomial "primordial" desse elemento, onde todas as outras relações polinomiais provém dessa. Essa relação "primordial", como veremos, será dada pelo chamado polinômio minimal. Sua construção é dada pelo teorema a seguir.

Teorema 2.13. Seja L/K uma extensão e $\theta \in L$ um elemento algébrico sobre K. Então, existe um polinômio mônico e irredutível $m(x) \in K[x]$, unicamente determinado, onde $m(\theta) = 0$.

Demonstração. Considere o conjunto $\mathfrak{m} = \{f(x) \in K[x] : f(\theta) = 0\}$. Perceba que tal conjunto é um ideal primo não trivial de $K[x]$.

De fato, para qualquer $g(x) \in K[x]$ e $f(x), h(x) \in \mathfrak{m}$, devemos ter que $g(\theta)f(\theta) = g(\theta) \cdot 0 = 0$, logo $g(x)f(x) \in \mathfrak{m}$, e $f(\theta) - h(\theta) = 0 + 0 = 0 \implies f(x) - h(x) \in \mathfrak{m}$. Também, $\mathfrak{m}$ é não trivial, já que θ é um elemento algébrico, logo existe um polinômio não nulo tal que θ é raiz. E, por fim, $\mathfrak{m}$ é primo, pois se $f_1(x)f_2(x) \in \mathfrak{m}$, então

$$f_1(\theta)f_2(\theta) = 0 \implies f_1(\theta) = 0 \text{ ou } f_2(\theta) = 0,$$

portanto $f_1(x) \in \mathfrak{m}$ ou $f_2(x) \in \mathfrak{m}$.

Como $K[x]$ é um domínio principal, $\mathfrak{m}$ também será um ideal maximal, portanto, gerado por um elemento irredutível $m(x) \in K[x]$.

Podemos, sem perda de generalidade, considerar tal polinômio como mônico, basta multiplicá-lo pelo inverso do coeficiente do primeiro termo caso não seja, e ele continuaria gerando o mesmo ideal.

Por fim, tal polinômio é único, já que dois geradores do mesmo ideal sempre se dividem entre si, e como são ambos mônicos, devem ser iguais. □

Em um anel A, denotamos o ideal principal gerado por um elemento $a \in A$ por (a).

Corolário 2.14. Na mesma notação do Teorema 2.13, temos que

$$\frac{K[x]}{(m(x))} \cong K[\theta] = K(\theta),$$

onde o isomorfismo entre $K[x]/(m(x))$ e $K[\theta]$ possui os elementos de K como pontos fixos.

Demonstração. Basta considerar o morfismo de anéis $K[x] \to K[\theta]$ dado por $f(x) \mapsto f(\theta)$. O núcleo de tal homomorfismo é precisamente $\mathfrak{m} = (m(x))$, por definição. Logo, a congruência segue pelo Teorema do Núcleo e da Imagem. Perceba que o isomorfismo induzido age como a "identidade" em K (identificando cada elemento de K com sua classe de equivalência em $K[x]/(m(x))$).

Além disso, como $(m(x))$ é maximal, $K[x]/(m(x))$ é um corpo, portanto $K[\theta]$ também é, além disso, $\theta \in K[\theta]$. Assim, por definição de $K(\theta) \subseteq K[\theta]$. Em contrapartida, é evidente, também pelas definições, que $K[\theta] \subseteq K(\theta)$. Logo, vale a igualdade. □

Definição 2.15. Nas mesmas hipóteses do Teorema 2.13, o polinômio $m(x)$ é dito ser o polinômio minimal de θ.

Observação 2.16. Ainda nas mesmas hipóteses do teorema, perceba que se existe um polinômio $f(x) \in K[x]$ onde $f(\theta) = 0$, então $m(x)$

necessariamente é um fator irredutível de f, já que $f(x) \in \mathfrak{m} = (m(x))$, o que implica que $m(x) \mid f(x)$. Ou seja, o polinômio minimal é o polinômio de menor grau que tem θ como raiz, e todos os outros polinômios com tal propriedade são múltiplos de $m(x)$.

Exemplo 2.17. Seja $K(\sqrt{\alpha})/K$ uma extensão quadrática qualquer. Perceba que o polinômio minimal de $\sqrt{\alpha}$ deve ser $x^2 - \alpha$, visto que nenhuma de suas raízes está em K por hipótese, e esse polinômio tem um grau suficientemente pequeno para que a sua falta de raízes em K implique irredutibilidade em K.

Isso ocorre com qualquer polinômio de grau até 3, pois qualquer fatoração de polinômios de grau 2 ou 3 deve conter um fator linear (de grau 1), portanto, deve conter uma raiz, isso será amplamente utilizado no texto.

A interpretação que pode-se ter nesse caso é que a relação $(\sqrt{\alpha})^2 - \alpha = 0$ completamente define esse elemento sob o ponto de vista de K: a propriedade fundamental de $\sqrt{\alpha}$ é que, quando elevamos esse número ao quadrado, ele se iguala a α.

Perceba que não é apenas $\sqrt{\alpha}$ que satisfaz tal relação, pois $-\sqrt{\alpha}$ também é raiz de $x^2 - \alpha$, como já comentado. Na prática, isso significa que $\sqrt{\alpha}$ e $-\sqrt{\alpha}$ são algebricamente indistinguíveis sob o ponto de vista de K, ou, em outras palavras, $\sqrt{\alpha}$ satisfaz a relação polinomial $f(\sqrt{n}) = 0$ se, e somente se, $f(-\sqrt{\alpha}) = 0$, basta notar que, em ambos os casos, $f(x) \in (x^2 - \alpha)$, logo ele deve ter ambas.

Exemplo 2.18. Seja $m \in \mathbb{Z}$ um número cuja fatoração prima tem, ao menos, um primo de multiplicidade 1, e $n \in \mathbb{N}$. Então, o polinômio minimal de $\sqrt[n]{m}$ (este símbolo está representando alguma das n raízes complexas n-ésimas de m) sobre $\mathbb{Q}$ é $x^n - m$.

De fato, $x^n - m$ é irredutível pelo critério de Eisenstein, utilizando o primo de multiplicidade 1 de m e, claramente, tem $\sqrt[n]{m}$ como

raiz.

Exemplo 2.19. Como visto pelo exemplo anterior, os números $\pm\sqrt[4]{2}$ tem polinômio minimal igual a $x^4 - 2$ sobre $\mathbb{Q}$. Entretanto, eles tem polinômio minimal igual a $x^2 - \sqrt{2}$ sobre $\mathbb{Q}(\sqrt{2})$.

Com efeito, primeiro perceba que todo elemento $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ tem polinômio minimal sobre $\mathbb{Q}$ de, no máximo, grau 2, já que é raiz de $(x-a)^2 - 2b^2$. Todavia, os números $\pm\sqrt[4]{2}$ tem polinômio minimal de grau 4 sobre $\mathbb{Q}$, logo $\pm\sqrt[4]{2} \notin \mathbb{Q}(\sqrt{2})$, e segue que o polinômio $x^2 - \sqrt{2}$ é irredutível em $\mathbb{Q}(\sqrt{2})[x]$, pois $\pm\sqrt[4]{2}$ são precisamente suas raízes. Ou seja, o polinômio minimal depende do corpo base.

Exemplo 2.20. Seja p um primo e $\zeta = e^{2\pi i/p}$ a raiz p-ésima principal da unidade. Afirmamos que seu polinômio minimal sobre $\mathbb{Q}$ é $f(x) = x^{p-1} + \cdots + x + 1$.

O elemento ζ é, de fato, raiz de tal polinômio pois é raiz de $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$, porém não é raiz de $x - 1$. Basta então mostrar que $x^{p-1} + \cdots + x + 1$ é irredutível.

Considere, então, o automorfismo de $\mathbb{Q}[x]$ dado por $p(x) \mapsto p(x+1)$ (com inverso dado por $p(x) \mapsto p(x-1)$). Dessa forma, temos que a imagem de $f(x)$ pelo autormorfismo é

$$\begin{aligned}(x+1)^{p-1} + \cdots + (x+1) + 1 &= \frac{(x+1)^p - 1}{(x+1) - 1} \\ &= \frac{1}{x}\left(\sum_{i=0}^{p} \binom{p}{i} x^i - 1\right) \\ &= \frac{1}{x}\sum_{i=1}^{p} \binom{p}{i} x^i \\ &= \sum_{i=1}^{p} \binom{p}{i} x^{i-1},\end{aligned}$$

que é um polinômio irredutível pelo critério de Eisenstein, utilizando o primo p, logo $f(x)$ também é.

O polinômio $x^p + \cdots + x + 1$ do exemplo anterior, por ser o polinômio minimal de uma raiz da unidade sobre $\mathbb{Q}$, é dito ser um polinômio ciclotômico. Tais polinômios serão estudados mais profundamente no Capítulo 4.

Exemplo 2.21. Vamos descobrir o polinômio minimal de $\alpha = 1 + 2\sqrt[3]{2} + \sqrt[3]{4}$ sobre $\mathbb{Q}$. Para isso, perceba que esse elemento é uma $\mathbb{Q}$-combinação linear dos elementos de $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$, que é também um conjunto gerador de $\mathbb{Q}(\sqrt[3]{2})$. Vejamos, então, como que a multiplicação por α transforma esse conjunto. Temos que

$$\begin{aligned} \alpha &= 1 + 2\sqrt[3]{2} + \sqrt[3]{4}, \\ \alpha\sqrt[3]{2} &= 2 + \sqrt[3]{2} + 2\sqrt[3]{4}, \\ \alpha\sqrt[3]{4} &= 4 + 2\sqrt[3]{2} + \sqrt[3]{4}. \end{aligned}$$

Escrevendo essas igualdades matricialmente, temos que

$$\begin{bmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{bmatrix} \begin{bmatrix} 1 \\ \sqrt[3]{2} \\ \sqrt[3]{4} \end{bmatrix} = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 1 & 2 \\ 4 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ \sqrt[3]{2} \\ \sqrt[3]{4} \end{bmatrix}.$$

Reorganizando

$$\begin{bmatrix} \alpha - 1 & -2 & -1 \\ -2 & \alpha - 1 & -2 \\ -4 & -2 & \alpha - 1 \end{bmatrix} \begin{bmatrix} 1 \\ \sqrt[3]{2} \\ \sqrt[3]{4} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

Portanto, como o sistema linear homogêneo definido por essa matriz

tem solução não trivial, obtemos que

$$\begin{vmatrix} \alpha-1 & -2 & -1 \\ -2 & \alpha-1 & -2 \\ -4 & -2 & \alpha-1 \end{vmatrix} = 0$$

$$\iff (\alpha-1)^3 - 16 - 4 - 4(\alpha-1) - 4(\alpha-1) - 4(\alpha-1) = 0$$

$$\iff \alpha^3 - 3\alpha^2 + 3\alpha - 1 - 20 - 12\alpha + 12 = 0$$

$$\iff \alpha^3 - 3\alpha^2 - 9\alpha - 9 = 0.$$

Assim, α é raiz do polinômio $f(x) = x^3 - 3x^2 - 9x - 9$. É fácil checar também que os números $1 + 2\zeta\sqrt[3]{2} + \zeta^2\sqrt[3]{4}$ e $1 + 2\zeta^2\sqrt[3]{2} + \zeta\sqrt[3]{4}$, onde $\zeta = e^{2\pi i/3}$, são as outras raízes de $f(x)$ (extraindo as outras raízes cúbicas complexas de 2).

Esse números não são reais. De fato, perceba que $\zeta = (1 + \sqrt{3}i)/2$ e $\zeta^2 = (1 - \sqrt{3}i)/2$. Assim, calculando as partes imaginárias de $1 + 2\zeta\sqrt[3]{2} + \zeta^2\sqrt[3]{4}$ e $1 + 2\zeta^2\sqrt[3]{2} + \zeta\sqrt[3]{4}$, obtemos, respectivamente, $\sqrt{3}\sqrt[3]{2} - \sqrt{3}\sqrt[3]{4}/2$ e $-\sqrt{3}\sqrt[3]{2} + \sqrt{3}\sqrt[3]{4}/2$. Esses número não são igual a 0, visto que $\sqrt[3]{2} \neq \sqrt[3]{4}/2$, pois quando elevados ao cubo não resultam em números iguais.

Exemplo 2.22. Seja $\alpha = \sqrt{3} + \sqrt{5}$, vamos encontrar seu polinômio minimal sobre $\mathbb{Q}$. Temos que

$$\begin{aligned} \alpha^2 = 3 + 2\sqrt{15} + 5 &\implies \frac{1}{2}\alpha^2 - 4 = \sqrt{15} \\ &\implies \left(\frac{1}{2}\alpha^2 - 4\right)^2 = 15 \\ &\implies \frac{1}{4}\alpha^4 - 4\alpha^2 + 16 = 15 \\ &\implies \frac{1}{4}\alpha^4 - 4\alpha^2 + 1 = 0 \\ &\implies \alpha^4 - 16\alpha^2 + 4 = 0. \end{aligned}$$

Ou seja, o polinômio minimal de $\sqrt{3}+\sqrt{5}$ é algum fator primo de $f(x) = x^4 - 16x^2 + 4$, que tem $\pm\sqrt{3} \pm \sqrt{5}$ como raízes, como pode ser facilmente verificado, fazendo os passos contrários da cadeia de equações acima. Afirmamos que $f(x)$ é irredutível, sendo assim o próprio polinômio minimal sobre $\mathbb{Q}$. De fato, se $f(x)$ fosse redutível, ele deveria ter um fator de grau 1 ou 2 em $\mathbb{Q}[x]$. Não é possível ter um fator de grau 1, já que todas as suas raízes são irracionais, e os únicos divisores mônicos de grau 2 são os 6 polinômios

$$\begin{aligned}
(x-\sqrt{3}-\sqrt{5})(x-\sqrt{3}+\sqrt{5}) &= x^2 - 2\sqrt{3}x - 2,\\
(x-\sqrt{3}-\sqrt{5})(x+\sqrt{3}-\sqrt{5}) &= x^2 - 2\sqrt{5}x + 2,\\
(x-\sqrt{3}-\sqrt{5})(x+\sqrt{3}+\sqrt{5}) &= x^2 - 2\sqrt{15} - 8,\\
(x-\sqrt{3}+\sqrt{5})(x+\sqrt{3}-\sqrt{5}) &= x^2 + 2\sqrt{15} - 8,\\
(x-\sqrt{3}+\sqrt{5})(x+\sqrt{3}+\sqrt{5}) &= x^2 + 2\sqrt{5} + 2,\\
(x+\sqrt{3}-\sqrt{5})(x+\sqrt{3}+\sqrt{5}) &= x^2 + 2\sqrt{3}x - 2.
\end{aligned}$$

Porém, nenhum deles tem coficientes em $\mathbb{Q}$. Segue, então, que $x^4 - 16x + 4$ é irredutível e é o polinômio minimal de $\sqrt{3}+\sqrt{5}$ sobre $\mathbb{Q}$

Exemplo 2.23. Vamos descobrir o polinômio minimal de $\sqrt{1+\sqrt{2}}$ sobre $\mathbb{Q}$. Note que

$$\begin{aligned}
\sqrt{1+\sqrt{2}} = \alpha &\implies 1+\sqrt{2} = \alpha^2\\
&\implies \sqrt{2} = \alpha^2 - 1\\
&\implies 2 = (\alpha^2-1)^2\\
&\implies \alpha^4 - 2\alpha^2 - 1 = 0.
\end{aligned}$$

Ou seja, $\sqrt{1+\sqrt{2}}$ é raiz do polinômio $f(x) = x^4 - 2x^2 - 1$. Podemos facilmente achar as raízes desse polinômio, que são $\pm\sqrt{1 \pm \sqrt{2}}$, e encontrar que $f(x)$ se fatora sobre $\mathbb{Q}(\sqrt{1+\sqrt{2}})[x]$ da seguinte forma $f(x) = (x-\sqrt{1+\sqrt{2}})(x+\sqrt{1-\sqrt{2}})(x^2-1+\sqrt{2})$, visto que as raízes $\pm\sqrt{1-\sqrt{2}}$ são complexas.

Como nenhuma combinação de dois desses fatores resulta em um polinômio com coeficientes em $\mathbb{Q}$, $f(x)$ será irredutível em $\mathbb{Q}[x]$. Assim, deve ser o polinômio minimal de $\sqrt{1+\sqrt{2}}$.

2.3 EXTENSÕES SIMPLES E FINITAS

Definição 2.24. Seja L/K uma extensão de corpos. Então, dizemos que

- L/K é simples se existe $\theta \in L$ tal que $L = K(\theta)$
- L/K é uma extensão finita se L é um K-espaço vetorial de dimensão finita, onde a dimensão é denotada por $[L : K]$, também chamado de grau da extensão.
- L/K é uma extensão infinita se L é um K espaço de dimensão infinita.

Exemplo 2.25. Toda extensão quadrática $K(\sqrt{\alpha})/K$, como visto no Exemplo 2.5 é uma extensão simples, de grau 2, com base, como K-espaço vetorial, dada por $\{1, \sqrt{\alpha}\}$. A recíproca, se $\text{char}(K) \neq 2$, onde $\text{char}(K)$ denota a característica de K, também é verdadeira.

De fato, Seja L/K uma extensão de corpos onde $\text{char}(K) \neq 2$ com $[L : K] = 2$, e seja $\theta \in L \setminus K$ um elemento qualquer, então claramente $K(\theta) = L$, visto que deve ser um K-subespaço de L com dimensão maior que 1, portanto diferente de K, logo a única maneira disso ocorrer é se $L = K(\theta)$, assim $\{1, \theta, \theta^2\}$ forma um conjunto linearmente dependente sobre $K(\theta)$, pois tem 3 elementos, e, portanto, há elementos $a, b, c \in K$ onde $a\theta^2 + b\theta + c = 0$.

Utilizando a fórmula para a equação de segundo grau (que é válida em qualquer corpo de característica diferente de 2, pois $2a \neq 0$ para qualquer $a \neq 0$), devemos ter que $\theta = \frac{-b+\sqrt{\Delta}}{2a}$, onde $\Delta = b^2 - 4ac$

(aqui $\sqrt{\Delta}$ representa a raiz quadrada apropriada para que a igualdade se verifique).

Ou seja, como $a, b, c \in K$, fazer a adjunção de $\theta = \frac{-b+\sqrt{\Delta}}{2a}$ equivale a fazer a adjunção de $\sqrt{\Delta}$, daí $L = K(\sqrt{\Delta})$.

Exemplo 2.26. Como visto no Exemplo 2.7, a extensão $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}$ tem grau 4, com base, como $\mathbb{Q}$-espaço dada por $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$. Além disso, afirmamos que a extensão é simples, com $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$.

A inclusão $\mathbb{Q}(\sqrt{3}, \sqrt{5}) \supseteq \mathbb{Q}(\sqrt{3} + \sqrt{5})$ é óbvia, visto que $\sqrt{3} + \sqrt{5} \in \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Já para a recíproca, perceba que o conjunto $\mathcal{B} = \{1, \sqrt{3} + \sqrt{5}, (\sqrt{3} + \sqrt{5})^2, (\sqrt{3} + \sqrt{5})^3\}$ é um conjunto linearmente independente de $\mathbb{Q}(\sqrt{3} + \sqrt{5})$ como $\mathbb{Q}$-espaço.

De fato, qualquer combinação linear, com coeficientes não todos nulos, dos elementos de $\mathcal{B}$, digamos

$$a(\sqrt{3} + \sqrt{5})^3 + b(\sqrt{3} + \sqrt{5})^2 + c(\sqrt{3} + \sqrt{5}) + d,$$

com $a, b, c, d \in \mathbb{Q}$, e $(a, b, c, d) \neq (0, 0, 0, 0)$, seria igual a $f(\sqrt{3} + \sqrt{5})$, onde $f(x) = ax^3 + bx^2 + cx + d$ é um polinômio não nulo de grau no máximo 3. Todavia, seu polinômio minimal tem grau 4, pelo Exemplo 2.22, portanto $\sqrt{3} + \sqrt{5}$ não pode ser raiz de $f(x)$, ou seja, $f(\sqrt{3} + \sqrt{5}) \neq 0$. Segue então que $\mathcal{B}$ é linearmente independente.

Ou seja, $\mathbb{Q}(\sqrt{3} + \sqrt{5})$ é um $\mathbb{Q}$-subespaço vetorial de $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ de dimensão, no mínimo, 4. Como $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ é um $\mathbb{Q}$-espaço vetorial de dimensão 4, isso só pode ser o caso se $\mathbb{Q}(\sqrt{3} + \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

Veremos agora as principais propriedades das extensões finitas, que serão as mais estudadas nesse trabalho.

O seguinte resultado é uma generalização do Corolário 2.14, que nos dá uma poderosa ferramenta de "criação" de raízes para polinômios, e geração de extensões simples.

Teorema 2.27. Seja K um corpo, e $f(x) \in K[x]$ um polinômio irredutível de grau n. Então, se identificarmos K, pela projeção canônica, como um subcorpo de $L = K[x]/(f(x))$, então L/K é uma extensão simples de corpos, que faz a adjunção de uma raiz de $f(x)$. Ou seja, $L = K(\alpha)$ para algum $\alpha \in L$ onde $f(\alpha) = 0$. Além disso, $[L : K] = n$.

Demonstração. A extensão L/K está bem definida, visto que $f(x)$ é irredutível, portanto, $(f(x))$ é maximal, pois $K[x]$ é um domínio principal, que faz com que $K[x]/(f(x))$ seja um corpo. Para mostrar que a extensão é simples, gerada por uma raiz de $f(x)$, basta considerar $\alpha = \overline{x}$, onde a barra denota a classe de equivalência, em $K[x]/(f(x))$, do polinômio.

De fato, para todo elemento $\theta \in L$, temos pela definição de L que existe um polinômio $g(x) \in K[x]$ onde $\theta = \overline{g(x)} = g(\overline{x}) = g(\alpha) \in K(\alpha)$, e, claramente, $f(\alpha) = f(\overline{x}) = \overline{f(x)} = \overline{0}$.

Por fim, perceba que $\mathcal{B} = \{1, \alpha, \cdots, \alpha^{n-1}\}$ é uma base de L como K-espaço. De fato, dizer que existe uma combinação K-linear não trivial dos elementos de $\mathcal{B}$ que resulta em 0 equivale a dizer que existe um polinômio $r(x) \in K[x]$ não nulo com grau menor que n tal que $r(\alpha) = 0$. Por sua vez, isso implica que $r(x) \in (f(x))$, portanto $f(x) \mid r(x)$. Mas isso é falso, já que o grau de $r(x)$ é menor que o grau de $f(x)$, portanto não pode existir tal combinação.

Podemos concluir que $\mathcal{B}$ é linearmente independente. O fato de que $\mathcal{B}$ gera L segue diretamente da definição de L. Assim, $\mathcal{B}$ é uma base com n elementos, e $[L : K] = n$. □

Corolário 2.28. Sejam L/K uma extensão de corpos, $\theta \in L$ um elemento algébrico sobre K, $m(x)$ o polinômio minimal de *theta*, e $n = \deg(m(x))$. Então, $K(\theta)/K$ é finita, com $[K(\theta) : K] = n$.

Demonstração. Pelo Corolário 2.14, há um isomorfismo de K-espaços

vetoriais $K(\theta) \cong K[x]/(m(x))$, e o Teorema 2.27 nos diz que

$$\left[\frac{K[x]}{(m(x))} : K\right] = n,$$

logo também temos que $[K(\theta) : K] = n$. □

Segue abaixo uma das principais propriedades dessa noção de grau de uma extensão, que é uma generalização do processo usado para descobrir uma base das extensões nos Exemplos 2.7 e 2.8.

Teorema 2.29. Sejam $M \supseteq L \supseteq K$ corpos. Então,

$$M/K \text{ é finita} \iff M/L \text{ e } L/K \text{ são finitas.}$$

Nessas condições, também temos que

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

Demonstração. ($\Longrightarrow$). Como M é um K-espaço de dimensão finita, então L é um K-subespaço de M, logo também é de dimensão finita. Além disso, a base de M como K-espaço é, claramente, um conjunto gerador finito de M quando visto como L-espaço vetorial, logo também deve ser um espaço de dimensão finita.

($\Longleftarrow$). Seja $\{k_1, \ldots, k_n\}$ uma base de L como K-espaço e $\{l_1, \ldots, l_m\}$ uma base de M como L-espaço, vamos mostrar que $\mathfrak{B} = \{l_i k_j : 1 \leq i \leq n \text{ e } 1 \leq j \leq m\}$ é uma base de M como K-espaço. $\mathfrak{B}$ gera M como K-espaço, já que

$$M = \sum_{i=1}^{n} l_i L = \sum_{i=1}^{n} l_i \left(\sum_{j=1}^{m} k_j K\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} l_i k_j K.$$

Para ver que $\mathfrak{B}$ é linearmente independente sobre K, note que

$$\begin{aligned}\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}l_ik_j = 0 &\implies \sum_{i=1}^{n}\left(\sum_{j=1}^{m} a_{ij}k_j\right)l_i = 0\\ &\implies \sum_{j=1}^{m} a_{ij}k_j = 0 \text{ para qualquer } i\\ &\implies a_{ij} = 0 \text{ para qualquer } i, j.\end{aligned}$$

Portanto, $\mathfrak{B}$ é uma base de M como K-espaço de cardinalidade $nm = [M : L] \cdot [L : K]$, e segue o resultado. □

Teorema 2.30. Toda extensão finita é algébrica.

Demonstração. Seja L/K uma extensão finita com $[L : K] = n$. Então, para qualquer $\theta \in L$, o conjunto $\{1, \theta, \ldots, \theta^n\}$ tem $n + 1$ elementos, então, deve ser linearmente dependente no K-espaço vetorial L. Ou seja, existem $a_0, \ldots, a_n \in K$ não todos nulos tal que $a_0 + a_1\theta + \cdots + a_n\theta^n = 0$. Uma forma equivalente de dizer isso seria que θ é raiz do polinômio $f(x) = a_0 + a_1x + \cdots + a_nx^n$, assim, θ é algébrico sobre K. □

A recíproca desse teorema não é verdadeira, como veremos mais tarde no Exemplo 2.34.

Corolário 2.31. Seja L/K uma extensão finita com $n = [L : K]$. Então, todo elemento de L tem um polinômio minimal sobre K de grau no máximo n.

Demonstração. Pelo teorema anterior, todo elemento de L é raiz de um polinômio de grau n, logo seu polinômio minimal tem grau certamente menor ou igual a n, pois divide tal polinômio, pela Observação 2.16. □

Teorema 2.32. Uma extensão L/K é finita se, e somente se, $L = K(\theta_1, \ldots, \theta_n)$ para algum conjunto de elementos $\theta_1, \ldots, \theta_k \in L$ algébricos sobre K.

Demonstração. ($\Longrightarrow$) Vamos fazer por indução em $[L : K]$. Caso $[L : K] = 1$, então $L = K$, e L pode ser tomado como $K(1)$, por exemplo.

Agora suponha que $[L : K] = n$ para algum $n > 1$. Nesse caso, L contém propriamente K, portanto existe $\theta_1 \in L \setminus K$. Dessa forma, $[L : K(\theta_1)] = [L : K]/[K(\theta_1) : K] < [L : K]$, visto que $[K(\theta_1) : K] \geq 2$, por ser uma extensão própria.

Assim, aplicando a hipótese de indução em $L/K(\theta_1)$, devem existir $\theta_2, \cdots, \theta_k$ algébricos sobre $K(\theta_1)$, onde $L = K(\theta_1, \cdots, \theta_k)$, e como L/K é algébrica (pois é finita por hipótese), devemos ter que $\theta_1, \cdots, \theta_k$ são algébricos sobre K.

($\Longleftarrow$) Basta considerar a cadeia de extensões simples

$$K(\theta_1, \cdots, \theta_k) \supseteq \cdots \supseteq K(\theta_1, \theta_2) \supseteq K(\theta_1) \supseteq K$$

como cada um dos θ_i é algébrico sobre K, ele também será algébrico sobre $K(\theta_1, \cdots, \theta_{i-1})$ para $i \geq 2$. Assim são todas extensões finitas pelo Corolário 2.28, portanto, a extensão $K(\theta_1, \cdots, \theta_k)/K$ é finita, pelo Teorema 2.29. □

Corolário 2.33. Seja L/K uma extensão, e $a, b \in L$ elementos algébricos sobre K, então $a \pm b$, ab e a/b (desde que $b \neq 0$) são também algébricos sobre K. Ou seja, os elementos de L algébricos sobre K formam um corpo.

Demonstração. Se $a, b \in K$ são algébricos sobre K, então $K(a, b)$ é uma extensão finita (Teorema 2.32), portanto, algébrica (Teorema 2.30), de K. Além disso, como $a \pm b, ab, a/b \in K(a, b)$, esses elementos

são algébricos. Ou seja, o subconjunto dos elementos algébricos de L é fechado sob as operações de L, logo é, também, um subcorpo. □

Exemplo 2.34. A recíproca do Teorema 2.30 não é verdadeira, isto é, existe uma extensão algébrica infinita de corpos.

De fato, considere a extensão $K/\mathbb{Q}$ onde K é o corpo dos números complexos algébricos sobre $\mathbb{Q}$ (que é de fato um corpo pelo Corolário 2.33).

Como visto no Exemplo 2.18, os elementos da forma $\sqrt[n]{m}$, onde m é m inteiro com ao menos um primo de multiplicidade 1 em sua fatoração, são algébricos sobre $\mathbb{Q}$. Portanto estão em K. Além disso, $\sqrt[n]{m}$ tem polinômio minimal sobre $\mathbb{Q}$ igual $x^n - m$.

Ou seja, existem elementos com polinômio minimal sobre $\mathbb{Q}$ de grau arbitrariamente grande, visto que n pode ser tomado arbitrariamente nessa construção. Portanto, $K/\mathbb{Q}$ não pode ser finita pelo Corolário 2.31.

Teorema 2.35. Sejam $M \supseteq L \supseteq K$ corpos, então

$$M/K \text{ é algébrica } \iff M/L \text{ e } L/K \text{ são algébricas.}$$

Demonstração. ($\Longrightarrow$) Como todos os elementos de M são algébricos sobre K, o mesmo é claramente válido para os elementos de L, ademais, todos os elementos de M também serão algébricos sobre L, visto que $K[x] \subseteq L[x]$.

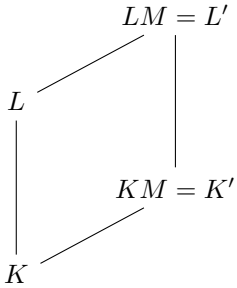
($\Longleftarrow$) Seja $\theta \in M$ um elemento arbitrário. Para mostrar que θ é algébrico sobre K, mostraremos que ele está em uma extensão finita de K. O resultado segue, então, pelo fato de que toda extensão finita é algébrica (Teorema 2.30).

Seja $m(x) = x^n + b_1 x^{n-1} + \cdots + b_n$ o polinômio minimal de θ sobre L. Como $b_1, \ldots, b_n \in L$, eles são todos algébricos sobre K, pois L/K é algébrica por hipótese. Assim, a extensão $K(b_1, \ldots, b_n)$ é

finita, pelo Teorema 2.32. Isso implica, por sua vez, que θ é algébrico sobre $K(b_1, \ldots, b_n)$.

Como a extensão $K(b_1, \ldots, b_n, \theta)/K(b_1, \ldots, b_n)$ é finita, pelo Corolário 2.28, podemos concluir que $K(b_1, \ldots, b_n, \theta)/K$ também é finita, pelo teorema 2.29. Isso mostra que θ está contido em uma extensão finita de K, como queríamos. □

Definição 2.36. Sejam L/K e L'/K' extensões de corpos, e Ω um corpo que contém todos eles. Então, a extensão L'/K' é dita ser um transporte paralelo de L/K se existe um corpo $M \subseteq \Omega$ onde $L' = LM$ e $K' = KM$. ou, equivalentemente, se $K \subseteq K'$ e $L' = LK'$.



Transportes paralelos são muitos úteis quando estudamos corpos de estrutura mais complicadas, a partir de corpos mais simples. Isso ocorre pois, geralmente, preservam propriedades da extensão.

O grau de extensões finitas, por exemplo, é preservado, simplificado, com transportes paralelos, como o seguinte teorema mostra.

Teorema 2.37. Seja L/K uma extensão finita e L'/K' um transporte paralelo de L/K. Então, $[L' : K'] \leq [L : K]$.

Demonstração. Considere, primeiramente, o caso onde a extensão é simples, ou seja, $L = K(\theta)$ para algum $\theta \in L$. Nesse caso, sabemos que o grau de L/K coincide com o grau do polinômio minimal de θ sobre

K, como visto no Teorema 2.28. Digamos, então, que $m(x) \in K[x]$ é tal polinômio minimal, com $\deg(m(x)) = [L : K] = n$.

Perceba que L'/K' também é uma extensão simples. De fato, por hipótese temos que $L' = LM$ para algum corpo M. Além disso, como já sabemos que $L = K(\theta)$, também é verdade que $L' = KM(\theta) = K'(\theta)$.

Como $m(x) \in K[x] \subseteq K'[x]$, e θ é raiz de $m(x)$, então o polinômio minimal de θ sobre K', digamos $f(x) \in K'[x]$, certamente divide $m(x)$. Ou seja, $[L' : K'] = \deg(f(x)) \leq \deg(m(x)) = [L : K]$, como queríamos.

No caso geral, L pode ser decomposto em uma cadeia de extensões simples, pelo Teorema 2.32. Assim temos a cadeia de extensões simples

$$L = K_n \supseteq \cdots \supseteq K_1 \supseteq K_0 = K.$$

De forma análoga ao que foi feito no caso simples, essa cadeia corresponde à seguinte cadeia, também de extensões simples

$$L' = MK_n \supseteq \cdots \supseteq MK_1 \supseteq MK_0 = K'.$$

Então, como o caso simples já foi provado, temos que

$$\begin{aligned}
[L : K] &= [K_n : K_{n-1}] \cdots [K_1 : K_0] \\
&\geq [MK_n : MK_{n-1}] \cdots [MK_1 : MK_0] \\
&= [ML : MK] \\
&= [L' : K'].
\end{aligned}$$

□

Teorema 2.38. Sejam L_1/K e L_2/K extensões de corpos, onde esses corpos estão todos contidos em um corpo maior Ω. Então,

$$[L_1L_2 : K] = [L_1 : K][L_2 : K] \implies L_1 \cap L_2 = K.$$

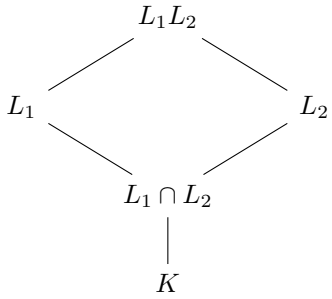
Demonstração. Pelo Teorema **??**, sabemos que $[L_1L_2 : K] = [L_1L_2 : L_1][L_1 : K]$. Assim, pela hipótese, $[L_1 : K][L_2 : K] = [L_1L_2 : L_1][L_1 : K]$. Cancelando os fatores de $[L_1 : K]$ em ambos os lados, temos que $[L_2 : K] = [L_1L_2 : L_1]$

Além disso, como L_1L_2/L_1 é um transporte paralelo de $L_2/L_1 \cap L_2$, temos que

$$[L_1L_2 : L_1] \leq [L_2 : L_1 \cap L_2] \leq [L_2 : K] = [L_1L_2 : L_1].$$

Perceba que o início e o fim da cadeia de desigualdades acima são iguais, portato são todas igualdades. Assim,

$$[L_1 \cap L_2 : K] = [L_2 : K]/[L_2 : L_1 \cap L_2] = 1 \implies L_1 \cap L_2 = K.$$



□

2.4 CORPOS DE RAÍZES, CORPOS ALGEBRICAMENTE FECHADOS E FECHOS ALGÉBRICOS

Como vimos, o Teorema 2.27, é sempre possível criar extensões que adicionam uma raiz de um polinômio irredutível (e, portanto, qualquer polinômio, basta adicionar uma raiz para algum fator irredutível seu). Esse teorema, naturalmente, pode ser usado repetidas vezes para adicionar as raízes de algum polinômio onde "faltam raízes", digamos $f(x)$, uma a uma, por meio de extensões simples, obtendo assim um

corpo que tem ‘´todas as raízes” de $f(x)$ (e é precisamente gerado por essas raízes).

Essa noção de ter “todas as raízes” é o que será estudado nessa seção, porém, é trocada pela condição mais clara de que $f(x)$ se decompõe em fatores lineares (que são fatores de grau 1), visto que falar nas raízes de um polinômio que, a priori, não tem raízes não faz muito sentido. Esse abuso de linguagem, entretanto, será feito de vez em quando no texto, e deve ser entendido pela noção de decomposição em fatores lineares. Iniciamos com a noção de corpo de raízes.

Definição 2.39. Sejam K um corpo, $f(x) \in K[x]$, $L \supseteq K$ uma extensão onde $f(x)$ se fatora em lineares, e $\theta_1, \ldots, \theta_n \in L$ as raízes de cada um desses fatores lineares. Então, $K(\theta_1, \ldots, \theta_n)$ é dito ser um corpo de raízes de $f(x)$ sobre K. Ou seja, é a extensão de K gerada, precisamente, pelas raízes de $f(x)$.

Exemplo 2.40. Temos que $\mathbb{C}$ não é um corpo de raízes de $x^2 - 2$ sobre $\mathbb{Q}$, pois $\mathbb{C}$ não é gerado por $\pm\sqrt{2}$. O corpo de raízes correto seria, simplesmente, $\mathbb{Q}(\sqrt{2})$, visto que é o menor corpo onde $x^2 - 2$ se fatora em lineares como $(x - \sqrt{2})(x + \sqrt{2})$.

Exemplo 2.41. Perceba que, como o polinômio minimal, o corpo de raízes de um polinômio depende do corpo base. De fato, o corpo de raízes de $x^2 - 2$ sobre $\mathbb{Q}$ é $\mathbb{Q}(\sqrt{2})$, enquanto o corpo de raízes desse polinômio sobre $\mathbb{R}$ é o próprio $\mathbb{R}$.

Exemplo 2.42. Como visto no Exemplo 2.23, a extensão de corpos $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}$ faz a adjunção de uma raiz do polinômio $f(x) = x^4 - 2x^2 - 1$, porém não é seu corpo de raízes sobre $\mathbb{Q}$. De fato, $f(x)$ tem como raízes os números $\pm\sqrt{1 \pm \sqrt{2}}$, porém $\pm\sqrt{1-\sqrt{2}} \notin \mathbb{Q}(\sqrt{1+\sqrt{2}})$, visto são valores complexos.

Dessa forma, o corpo de raízes de $f(x)$ sobre $\mathbb{Q}$ é

$$\mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}}).$$

Exemplo 2.43. Seja $x^n - a \in \mathbb{Q}[x]$ um polinômio com $n \in \mathbb{N}$. Tal polinômio tem n raízes complexas distintas, sendo elas $\zeta_n^i \sqrt[n]{a}$, onde $\zeta_n = e^{2\pi i/n}$, a raiz principal da unidade, e $i \in \{0, 1, \cdots, n-1\}$. Dessa forma, o corpo de raízes de $x^n - a$ sobre $\mathbb{Q}$ é $\mathbb{Q}(\sqrt[n]{a}, \zeta_n \sqrt[n]{a}, \cdots, \zeta_n^{n-1} \sqrt[n]{a})$, que pode ser reescrito como $\mathbb{Q}(\zeta_n, \sqrt[n]{a})$.

Um resultado de grande importância é que todo polinômio admite um corpo de raízes, que pode ser indutivamente construído com o Teorema 2.27.

Teorema 2.44. Seja K um corpo e $f(x) \in K[x]$ um polinômio de grau $n \geq 1$, então existe uma extensão de L/K finita com grau até $n!$, onde $f(x)$ se fatora como um produto de fatores lineares, e L é gerado precisamente pelas raízes desses fatores.

Demonstração. Suponha, sem perda de generalidade, que $f(x)$ é mônico. Mostraremos o teorema por indução no grau de $f(x)$. Caso $f(x)$ seja linear, não há nada a fazer, pois sua raiz já estará em K, logo o mesmo será seu corpo de raízes.

Agora, suponha que o grau de $f(x)$ seja n. Se $f(x)$ é irredutível, $L = K[x]/(f(x))$ é uma extensão de grau $n > 1$ de K que adiciona uma raiz de $f(x)$ (Teorema 2.27), que denotaremos por θ_1. Assim, utilizando o algoritmo da divisão, temos que $f(x) = (x - \theta_1)g(x)$ para algum $g(x) \in L[x]$ de grau $n - 1$. Também, pela hipótese de indução, existe uma extensão de $M \supseteq L$, de grau até $(n-1)!$, onde $g(x)$ se decompõe em fatores lineares em $M[x]$. Ou seja, existem $\theta_2, \ldots, \theta_n \in M$ tal que $f(x) = (x - \theta_1) \cdots (x - \theta_n)$.

Além disso, também é verdade que

$$[M : K] = [M : L] \cdot [L : K] \leq n(n-1)! = n!,$$

pelo Teorema 2.29. Agora, se $f(x)$ é redutível, então existem irredutíveis $g_1(x), \ldots, g_m(x) \in K[x]$, onde $\deg(g_i(x)) = n_i < n$, tal que $f(x) = g_1(x) \cdots g_k(x)$„ pela fatoração única em $K[x]$, assim, pela hipótese de indução, existem extensões

$$L = K_{g_m} \supseteq K_{g_{m-1}} \supseteq \cdots \supseteq K_{g_1} \supseteq K,$$

onde $g_i(x)$ se decompõe em fatores lineares em K_{g_i}, e $[K_{g_i} : K_{g_{i-1}}] \leq n_i!$, ou seja, $f(x)$ também se decompõe em lineares em L, e

$$\begin{aligned}
[L : K] &= [K_{g_m} : K_{g_{m-1}}] \cdot [K_{g_{m-1}} : K_{g_{m-2}}] \cdots [K_{g_1} : K] \\
&\leq n_m! \cdot n_{m-1}! \cdots n_1! \\
&< (n_m + n_{m-1} + \cdots + n_1)! \\
&= n!,
\end{aligned}$$

o que termina o passo indutivo. □

Uma noção mais forte ainda do que a de corpos de raízes é a noção de corpos algebricamente fechados, onde todos os seus polinômios tem "todas as suas raízes". A definição a seguir torna essa noção mais precisa.

Definição 2.45. Um corpo K é dito ser algebricamente fechado se todo polinômio não constante em K se fatora em um produto de polinômios lineares em $K[x]$. Ou seja, todo polinômio de grau $n \geq 1$ tem exatamente n raízes em K, contando suas multiplicidades.

Exemplo 2.46. Pelo Teorema Fundamental da Álgebra, $\mathbb{C}$ é um corpo algebricamente fechado. Caso o leitor já tenha feito um curso introdutório de análise complexa, já deve ter visto uma demonstração desse fato com ferramentas analíticas, utilizando o Teorema de Liouville. Mais adiante no texto faremos uma demonstração algébrica

desse fato, porém como os complexos não são um conjunto de natureza unicamente algébrica, ainda necessitaremos de alguns resultados analíticos para mostrar tal fato.

A seguir, temos algumas equivalências básicas da condição de ser algebricamente fechado.

Teorema 2.47. Seja K um corpo. Então, as seguintes condições são equivalentes:

(i) K é algebricamente fechado.

(ii) Todo polinômio não constante em $K[x]$ possui uma raiz em K.

(iii) A única extensão algébrica de K é o próprio K.

(iv) Os polinômios irredutíveis de $K[x]$ são os de grau 1.

Demonstração. (i) $\implies$ (ii). Imediato.

(ii) $\implies$ (iii). Seja L/K uma extensão algébrica e $\theta \in L \setminus K$ um elemento qualquer. Como θ é algébrico sobre K, ele tem um polinômio minimal sobre K, digamos $f(x)$. Pela definição de polinômio minimal, $f(x)$ é irredutível. Assim, pela nossa hipótese, $f(x)$ deve ter grau igual a 1.

Ademais, pelo Corolário 2.14, devemos, então, ter que $[K(\theta) : K] = 1$, o que implica que $\theta \in K$. Como θ foi tomado arbitrariamente, todo elemento de L deve ser, também, um elemento de K, isto é, $L = K$.

(iii) $\implies$ (iv). Suponha, por absurdo, que $f(x) \in K[x]$ é um polinômio irredutível de grau maior que 1. Então, existe uma extensão L de K, de grau precisamente $\deg(f(x))$, que adiciona uma raiz de $f(x)$, pelo Teorema 2.27. Porém, como K não admite extensões algébricas próprias, temos necessariamente que $L = K$, que, por sua vez, implica que $\deg(f(x)) = [L : K] = 1$, mas isso é um absurdo.

(iv) $\implies$ (i) Segue pela fatoração em irredutíveis em $K[x]$, que é um domínio de fatoração única (DFU). □

Definição 2.48. Seja Ω/K uma extensão algébrica de corpos. Se Ω é algebricamente fechado, então dizemos que Ω é um fecho algébrico de K.

O fecho algébrico é entendido como a "maior" das extensões algébricas de um corpo, fato que será melhor entendido quando estudarmos morfismos entre extensões no próximo capítulo.

O teorema a seguir nos dá uma condição mais simples para verificar o fato de que um corpo é algebricamente fechado.

Lema 2.49. Seja Ω/K uma extensão algébrica de corpos. Se todo polinômio em $K[x]$ se decompõe em fatores lineares em $\Omega[x]$, então Ω é algebricamente fechado, portanto, também, um fecho algébrico de K.

Demonstração. Seja $f(x) \in \Omega[x]$ um polinômio irredutível mônico. Devemos mostrar que $f(x)$ tem grau 1, isso mostra que Ω é algebricamente fechado pelo item (iv) do Teorema 2.47.

Seja L o corpo de raízes de $f(x)$ sobre Ω, e $\theta_1, \ldots, \theta_n \in L$ as raízes (não necessariamente distintas) de $f(x)$. Perceba que L/K é algébrica, visto que L/Ω e Ω/K também são. Assim, cada θ_i, possui um polinômio minimal sobre K, digamos $m_i(x) \in K[x] \subseteq \Omega[x]$.

Como todo θ_i é raiz de $\prod_{i=1}^{n} m_i(x)$, devemos ter que $f(x) \mid \prod_{i=1}^{n} m_i(x)$ em $L[x]$, portanto, também, em $\Omega[x]$, visto que ambos os polinômios tem coeficientes em Ω. Além disso, $f(x)$ deve dividir algum dos $m_i(x)$, pois é primo em $\Omega[x]$, porém, esse polinômio $m_i(x)$ se decompõe em fatores lineares em $\Omega[x]$ por hipótese. Portanto $f(x)$ deve dividir algum desses fatores lineares, e isso é apenas possível se $\deg(f(x)) = 1$, como queríamos. □

Ou seja, o teorema anterior nos diz que, para verificar que Ω é algebricamente fechado, não é preciso olhar para todos os polinômios em $\Omega[x]$ para verificar se eles tem todas as suas raízes. Basta olhar apenas para os polinômios com coeficientes em K.

Lema 2.50. Seja Ω/K uma extensão de corpos qualquer, onde Ω é um corpo algebricamente fechado. Nessas condições, o conjunto

$$\Omega' = \{\theta \in \Omega : \theta \text{ é algébrico sobre } K\ \}$$

é um fecho algébrico de K.

Demonstração. Note que Ω' é um corpo pelo Corolário 2.33. Assim, pelo lema anterior, basta provar que todo polinômio em $K[x]$ também se decompõe em fatores lineares em $\Omega'[x]$, já que Ω'/K é uma extensão algébrica, por construção.

Isso de fato ocorre, pois para todo $f(x) \in K[x]$ (mônico, sem perda de generalidade), existem, por hipótese, $\theta_1, \ldots, \theta_n \in \Omega$ onde $f(x) = (x - \theta_1) \cdots (x - \theta_n)$. Como cada θ_i é claramente algébrico sobre K (é raiz de $f(x)$), cada $x - \theta_i$ está em $\Omega'[x]$. Ou seja, $f(x)$ se decompõe em fatores lineares em $\Omega'[x]$, como queríamos. □

Agora podemos demonstrar o principal teorema da seção.

Teorema 2.51. Todo corpo K admite um fecho algébrico K^{alg}.

Demonstração. Mostraremos a existência do corpo Ω descrito no lema anterior. Para isso, crie, para cada polinômio mônico irredutível em $f(x) \in K[x]$, variáveis independentes $T_f = \{t_{f,1}, \ldots, t_{f,d}\}$ onde $d = \deg(f(x))$, e seja $T = \bigcup_{f \in K[x]} T_f$ (suponha $T_f = \emptyset$ se f não é mônico ou irredutível).

Considere, então, o anel polinomial sobre essas infinitas variáveis $A = K[T]$ (que consiste em expressões que usam um número finito

delas), e seja $\mathfrak{a}$ o ideal de A gerado pelos coeficientes dos polinômios de $A[x]$ da forma

$$f(x) - (x - t_{f,1}) \cdots (x - t_{f,d}),$$

com $f(x) \in K[x]$ mônico e irredutível. Assim, em $(A/\mathfrak{a})[x]$ temos que

$$\overline{f}(x) - (x - \overline{t_{f,1}}) \cdots (x - \overline{t_{f,d}}) = \overline{0} \implies \overline{f}(x) = (x - \overline{t_{f,1}}) \cdots (x - \overline{t_{f,d}})$$

(onde $\overline{f}(x)$ é formado substitutindo cada coeficiente de $f(x)$ a sua respectiva classe de equivalência em $A/\mathfrak{a}$) e já que os coeficientes de $f(x) - (x - t_{f,1}) \cdots (x - t_{f,d})$ pertencem a $\mathfrak{a}$, logo suas classes se anulam em $A/\mathfrak{a}$.

Ou seja, todo irredutível mônico em $K[x]$ (e, portanto, todo polinômio, por fatoração em irredutíveis em $K[x]$) se decompõe em fatores lineares em $(A/\mathfrak{a})[x]$. O único problema é que $A/\mathfrak{a}$ não é necessariamente um corpo, porém existe um quociente dele que é.

De fato, para ver isso, note que $\mathfrak{a}$ é um ideal próprio, já que, se $\mathfrak{a}$ não fosse próprio, existiriam $a_1, \ldots, a_n \in \mathfrak{a}$ e $k_1, \ldots, k_n \in K$ onde

$$1 = k_1 a_1 + \cdots + k_n a_n. \tag{1}$$

Po definição, cada a_i é algum coeficiente de um polinômio de $A[x]$ da forma

$$f_i(x) - (x - t_{f_i,1}) \cdots (x - t_{f_i,d_i}),$$

com $f_j(x)$ mônico irredutível, e $d_j = \deg(f_j(x))$ para $j \in \{1, \ldots, i\}$. Seja, então, L o corpo de raízes de $f_1(x) \cdots f_n(x)$ sobre K e $\theta_{i,1}, \ldots, \theta_{i,d_i}$ as raízes (não necessariamente distintas) de $f_i(x)$ em L. Assim, temos um morfismo $\phi : A[x] \to L[x]$, onde $\phi(t_{f_i,j}) = \theta_{i,j}$, para os polinômios $f_i(x)$, e $\phi(t_{f,j}) = 0$ caso contrário, que preserva $K[x]$ ponto a ponto. Assim, para qualquer i, teremos que

$$\begin{aligned}\phi(f_i(x) - (x - t_{f_i,1}) \cdots (x - t_{f_i,d_i})) &= f_i(x) - (x - \theta_{i,1}) \cdots (x - \theta_{i,d_i}) \\ &= 0.\end{aligned}$$

Isso implica que a imagem de todos os coeficientes do polinômio acima se anula.

Em particular, temos que $\phi(a_i) = 0$ para todo i. Aplicando ϕ na equação (1), obtemos, então, que $1 = 0$ (igualdade em $L[x]$), que é um absurdo, pois $L[x]$ não é um anel trivial.

Portanto $\mathfrak{a}$ é um ideal próprio. Assim, existe um ideal maximal $\mathfrak{m}$ que o contém. Pelo Teorema da Correspondência, o ideal maximal $\mathfrak{m}$ de A corresponde a um ideal $\overline{\mathfrak{m}}$, também maximal, de $A/\mathfrak{a}$. Logo, $(A/\mathfrak{a})/\overline{\mathfrak{m}}$ é um corpo, e como todo polinômio em $K[x]$ se fatora em lineares em $(A/\mathfrak{a})[x]$, o mesmo vale para os polinômios com coeficientes em $(A/\mathfrak{a})/\overline{\mathfrak{m}}$, esse é o nosso corpo Ω procurado. Agora, basta aplicar o corolário anterior, identificando K com o subcorpo das classes de equivalência de seus elementos em $(A/\mathfrak{a})/\overline{\mathfrak{m}}$. □

Mais tarde, no Corolário 2.74, provaremos que quaisquer dois fechos algébricos de um dado corpo são isomorfos, quando desenvolvermos as ferramentas necessárias sobre morfismos entre extensões.

Definição 2.52. Seja K um corpo, K^{alg} um fecho algébrico, $\theta \in K^{\text{alg}}$ um elemento qualquer, e $m(x) \in K[x]$ seu polinômio minimal sobre K. Dizemos que as outras raízes de $m(x)$ em K^{alg} são os conjugados de θ sobre K.

Para tornar a escrita mais simples, também se fala que eles são os K-conjugados de θ. Em geral, se L é uma extensão de K onde $m(x)$ se fatora em lineares, a mesma definição se aplica.

Os conjugados podem ser entendidos como os elementos de K^{alg} que são indistinguíveis algebricamente sobre K, satisfazendo exatamente as mesmas relações polinomiais com os elementos de K.

Exemplo 2.53. Seja p um número primo e $\zeta_p = e^{2i\pi/p}$. O Exemplo **??** nos diz que o polinômio minimal de ζ_p sobre $\mathbb{Q}$ é $x^{p-1} + \cdots + x + 1$.

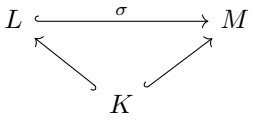
Além disso, esse polinômio tem como raízes as raízes p-ésimas da unidade, com exceção do número 1. Ou seja, os conjugados de ζ_p são os números ζ_p^i, com $i \in \{2, \cdots, p-1\}$, que são as $p-2$ raízes p-ésimas da unidade restantes.

Exemplo 2.54. Seja $K(\sqrt{\alpha})/K$ uma extensão quadrática. Então o K-conjugado do elemento $a + b\sqrt{\alpha} \in K(\sqrt{\alpha})$ é $a - b\sqrt{\alpha}$ se $b \neq 0$ (se tivéssemos $b = 0$, o elemento estaria no corpo K, portanto não teria K-conjugados). De fato, o polinômio minimal de $a + b\sqrt{\alpha}$ sobre K é dado por $(x-a)^2 - b^2\alpha$, e tem $a - b\sqrt{\alpha}$ como raiz.

2.5 IMERSÕES, AUTOMORFISMOS, E O LEMA FUNDAMENTAL

Nessa seção iniciaremos o estudo dos morfismos entre as extensões.

Definição 2.55. Sejam L/K e M/K duas extensões de corpos. Um morfismo $\sigma : L \to M$ é dito ser uma K-imersão se ela fixa K ponto a ponto, ou seja, se o seguinte diagrama comuta.



(nesse diagrama comutativo, como em todos no trabalho, as injeções sem nome serão sempre inclusões). Caso $M = L$, então σ é dito ser um K-automorfismo, e o grupo (sob a operação de composição) de todos os K-automorfismos de uma extensão L/K é denotado por $\mathrm{Aut}(L/K)$.

A necessidade de fixar o corpo K ponto a ponto tem a intenção de relacionar as estruturas L e M como extensões desse corpo, dessa forma K deve ser o "mesmo" em ambos, segundo o morfismo.

Observação 2.56. Lembre que todo morfismo entre corpos é necessariamente injetor, o que justifica utilizar o nome "imersão", tradicionalmente usado para aplicações injetoras.

Também, como todo morfismo de corpos necessariamente fixa a identidade multiplicativa, eles também fixarão o corpo gerado pela unidade, em particular, em um corpo de característica 0, todo morfismo fixa $\mathbb{Q}$ (que é isomorfo a um subcorpo de todo corpo de característica 0) ponto a ponto.

Exemplo 2.57. Vamos calcular o grupo de automorfismos de uma extensão quadrática $\mathrm{Aut}(K(\sqrt{\alpha})/K)$. Seja σ um K-automorfismo de $K(\sqrt{\alpha})$, e $a + b\sqrt{\alpha}$ um elemento qualquer. Então, como σ preserva os elementos de K, temos que $\sigma(a + b\sqrt{\alpha}) = a + b\sigma(\sqrt{\alpha})$, ou seja, o morfismo é completamente determinado pelo valor de $\sigma(\sqrt{\alpha})$. Esse valor, no entanto, não é arbitrário, pois

$$(\sqrt{\alpha})^2 - \alpha = 0 \implies \sigma\left((\sqrt{\alpha})^2 - \alpha\right) = 0 \implies \sigma(\sqrt{\alpha})^2 - \alpha = 0$$

e as únicas soluções para $\sigma(\sqrt{\alpha})$, na última, equação são $\pm\sqrt{\alpha}$ caso $\mathrm{char}(K) \neq 2$, ou apenas $\sqrt{\alpha}$ no caso onde $\mathrm{char}(K) = 2$, pois todo elemento é seu próprio oposto em corpos de característica 2.

No caso onde $\sigma(\sqrt{\alpha}) = \sqrt{\alpha}$, então $\sigma = \mathrm{id}$, e caso $\sigma(\sqrt{\alpha}) = -\sqrt{\alpha}$, temos que σ é a "conjugação", dada por $\sigma(a+b\sqrt{\alpha}) = a-b\sqrt{\alpha}$. É fácil verificar que tal aplicação é, de fato, um automorfismo de $K(\sqrt{\alpha})$.

Ou seja, se $\mathrm{char}(K) \neq 2$, então $\mathrm{Aut}(K(\sqrt{\alpha})/K) = \{\mathrm{id}, \tau\} \cong \mathbb{Z}/2\mathbb{Z}$, onde τ é a conjugação, e se $\mathrm{char}(K) = 2$, $\mathrm{Aut}(K(\sqrt{\alpha})/K) = \langle \mathrm{id} \rangle$.

Exemplo 2.58. A única $\mathbb{Q}$-imersão de $\mathbb{Q}(\sqrt[3]{2})$ em si mesmo é a identidade. De fato, temos que, para qualquer $\mathbb{Q}$-imersão $\sigma : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$,

$$(\sqrt[3]{2})^3 = 2 \implies \sigma((\sqrt[3]{2})^3) = \sigma(2) \implies \sigma(\sqrt[3]{2})^3 = 2.$$

Pela última equação, os únicos valores possíveis para $\sigma(\sqrt[3]{2})$ são $\sqrt{3}, \zeta\sqrt{3}$ e $\zeta^2\sqrt{3}$, onde $\zeta = e^{2\pi i/3}$. No entanto, o único entre esses números que está em $\mathbb{Q}(\sqrt[2]{2})$ é $\sqrt[3]{2}$, já que os outros não são números reais. Ou seja, $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{id}\}$.

Morfismos entre extensões tem uma propriedade que será muito utilizada, conhecida como o Princípio de Conservação de Raízes.

Proposição 2.59. Seja $\sigma : K \to L$ uma imersão de corpos e $f(x) \in K[x]$. Então, σ induz um morfismo $\sigma : K[x] \to L[x]$ (que também chamaremos de σ, por simplicidade), onde

$$\sigma(a_n x^n + \cdots + a_0) = \sigma(a_n)x^n + \cdots + \sigma(a_0).$$

Também, por fins de simplicidade, escreveremos $f^\sigma(x)$, ao invés de $\sigma(f(x))$. Esse morfismo preserva raízes, isto é, se $\theta \in K$ é raiz de $f(x) \in K[x]$, então $\sigma(\theta)$ será raiz de $f^\sigma(x) \in L[x]$.

Demonstração. Vamos primeiro mostrar que $\sigma : K[x] \to L[x]$ é um morfismo. Para isso, veja que, para quaisquer dois polinômios em $K[x]$, digamos $f(x) = \sum_{i=0}^{n} a_i x^i$ e $g(x) = \sum_{i=0}^{n} b_i x^i$ (perceba que o limite superior é o mesmo em ambas as somas, isso pode ser feito sem perda de generalidade, basta permitir que os coeficientes dos termos do polinômio de menor grau que "faltam" sejam nulos), temos que

$$\begin{aligned}(f+g)^\sigma(x) &= \sum_{i=0}^{n} \sigma(a_i + b_i)x^i \\ &= \sum_{i=0}^{n} (\sigma(a_i) + \sigma(b_i))x^i \\ &= \sum_{i=0}^{n} \sigma(a_i)x^i + \sum_{i=0}^{n} \sigma(b_i)x^i \\ &= f^\sigma(x) + g^\sigma(x).\end{aligned}$$

Além disso, temos que

$$\begin{aligned}(fg)^\sigma(x) &= \sum_{i=0}^{n^2} \sigma\left(\sum_{j=0}^{i} a_j b_{n-j}\right) x^i \\ &= \sum_{i=0}^{n^2} \left(\sum_{j=0}^{i} \sigma(a_j)\sigma(b_{n-j})\right) x^i \\ &= f^\sigma(x) g^\sigma(x).\end{aligned}$$

Portanto, σ é um morfismo de anéis.

Para ver que σ preserva raízes, basta ver que

$$f(\theta) = 0 \implies \sigma(f(\theta)) = 0 \implies f^\sigma(\sigma(\theta)) = 0,$$

o que prova a proposição. □

O próximo resultado é um caso especial desse teorema, que será amplamente utilizado no texto.

Corolário 2.60 (Princípio de Conservação de Raízes)**.** Seja L/K uma extensão de corpos, $\sigma : L \to L$ um K-automorfismo, e $\theta \in L$ um elemento algébrico sobre K. Então, $\sigma(\theta)$ é um conjugado de θ sobre K

Demonstração. Seja $m(x) \in K[x]$ o polinômio minimal de θ, basta então notar que $m^\sigma(x) = m(x)$, já que seus coeficientes estão em K, e aplicar a proposição anterior. □

Exemplo 2.61. Seja M um corpo qualquer, e considere a extensão $L/K = M(x_1, \ldots, x_n)/M(e_1, \ldots, e_n)$, onde os e_i's são os polinômios simétricos elementares em n variáveis (definição e propriedades consta no apêndice B). Essa extensão é dita ser uma extensão genérica n-ésima, e será de grande importância no Capítulo 6, que fala sobre a solubilidade de equações polinomiais por radicais.

Primeiro perceba que todos os x_i são raízes de $x^n - e_1 x^{n-1} + \cdots + (-1)^n e_n$, visto que esse polinômio se fatora como $(x - x_1) \cdots (x - x_n)$ em L. Assim, pelo Princípio de Consevação de Raízes, qualquer K-automorfismo de L deve permutar os x_i entre si, ou seja, $\mathrm{Aut}(L/K)$ é isomorfo a algum subgrupo de S_n, que age sobre os coeficientes das variáveis. Vamos mostrar que, na verdade, $\mathrm{Aut}(L/K)$ é precisamente isomorfo a S_n.

De fato, perceba que, para qualquer $\sigma \in S_n$, temos que a aplicação dada por $f(x_1, \ldots, x_n) \mapsto f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ fixa K, pois K é um corpo de expressões simétricas, e é um automorfismo de L. Isso se dá porque σ é morfismo de L em si mesmo, pois, para quaisquer $f, g \in K(x_1, \ldots, x_n)$, temos, por definição

$$(f+g)(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) + g(x_{\sigma(1)}, \ldots, x_{\sigma(n)}),$$
$$(fg)(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) g(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Além disso, como L/K é uma extensão finita (gerada pelos elementos x_i que algébricos sobre K), esse morfismo deve obrigatoriamente ser sobrejetor, pois é uma K-transformação injetora entre K-espaços vetoriais de mesma dimensão. Ou seja, $\mathrm{Aut}(L/K) \cong S_n$

Lema 2.62. Seja $\sigma : K \to K'$ um isomorfismo de corpos e $m(x) \in K[x]$ um polinômio irredutível, então

$$\frac{K[x]}{(m(x))} \cong \frac{K'[x]}{(m^\sigma(x))},$$

com isomorfismo dado por $\overline{f(x)} \mapsto \overline{f^\sigma(x)}$

Demonstração. Considere a aplicação $\phi : K[x] \to K'[x]/(m^\sigma(x))$ onde $\phi(f(x)) = \overline{f^\sigma(x)}$, essa aplicação é um morfismo, visto que é dada pela composição de dois morfismos, e $\phi(1) = \overline{1} \neq \overline{0}$, logo, por ser um morfismo não nulo, $\mathrm{Ker}(\phi) \subsetneq K[x]$, e, claramente, temos que

$(m(x)) \subseteq \mathrm{Ker}(\phi)$, visto que $\phi(m(x)) = \overline{0}$, e como $(m(x))$ é maximal, já $m(x)$ é irredutível em um domínio principal, temos que a igualdade $(m(x)) = \mathrm{Ker}(\phi)$ deve ocorrer. Assim, o resultado segue pelo Teorema do Isomorfismo. □

O lema a seguir será a nossa principal ferramenta para o cálculo explicito dos automorfismos de um corpo. Ele generaliza algumas das linhas argumentativas vistas nos exemplos até então e torna o cálculo de grupos de automorfismos mais fácil.

Lema 2.63 (Lema Fundamental da Teoria de Galois)**.** Sejam

- $K(\theta)/K$ uma extensão algébrica simples,
- L'/K' uma extensão qualquer,
- $\sigma : K \to K'$ um isomorfismo,
- $m(x) \in K[x]$ o polinômio minimal de θ sobre K.

Existe uma correspondência biunívoca entre os morfismos $\tilde{\sigma} : K(\theta) \to L'$ que estendem σ (ou seja, fazem o diagrama abaixo comutar) e raízes de $m^\sigma(x)$ em L', dada por $\tilde{\sigma} \mapsto \tilde{\sigma}(\theta)$.

$$\begin{array}{ccc} K(\theta) & \xhookrightarrow{\tilde{\sigma}} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow[\approx]{\sigma} & K' \end{array}$$

Demonstração. Pela Proposição 2.59, $\sigma(\theta)$ é, de fato, uma raiz de $m^\sigma(x) \in L'[x]$, logo a correspondência dada está bem definida. Vamos então provar que ela é biunívoca.

Para ver que ela é injetora, perceba que $K(\theta)$ é uma extensão algébrica simples, assim $K(\theta) = K[\theta]$, portanto, $\tilde{\sigma}$ é completamente determinada pelo valor de $\tilde{\sigma}(\theta)$. De fato, $\tilde{\sigma}(f(\theta)) = f^\sigma(\tilde{\sigma}(\theta))$ para

qualquer $f(\theta) \in K(\theta)$. Ou seja, se $\sigma_1(\theta) = \sigma_2(\theta)$, devemos necessariamente ter que $\theta_1 = \theta_2$, o que mostra a injetividade.

Para a sobrejetividade, considere $\theta' \in L'$ como sendo um raiz qualquer de $m^\sigma(x)$, devemos mostrar que existe uma extensão $\tilde{\sigma}$ de σ onde $\tilde{\sigma}(\theta) = \theta'$. Para isso, considere a seguinte composição de morfismos

$$K(\theta) \xrightarrow[\approx]{\text{(i)}} \frac{K[x]}{(m(x))} \xrightarrow[\approx]{\text{(ii)}} \frac{K'[x]}{(m^\sigma(x))} \xrightarrow[\approx]{\text{(iii)}} K'(\theta') \xhookrightarrow{\text{(iv)}} L'.$$

As aplicações (i) e (iii) são dadas por $f(\theta) \mapsto \overline{f(x)}$ e $\overline{f(x)} \mapsto f(\theta')$. Elas estão bem definidos e são isomorfismos pelo Lema 2.14. A aplicação (ii) é definida por $\overline{f(x)} \mapsto \overline{f^\sigma(x)}$ como no Teorema 2.62, logo também é um morfismos. A aplicação (iv) é simplesmente a a inclusão. Logo, a composição de todas essas aplicações é, também, um morfismo. Por fim, a composição delas é uma extensão de σ, já que, para qualquer $a \in K$, temos que

$$a \mapsto \overline{a} \mapsto \overline{\sigma(a)} \mapsto \sigma(a) \mapsto \sigma(a).$$

Além disso, essa composição também leva θ até θ', como queríamos, pois

$$\theta \mapsto \overline{x} \mapsto \overline{x} \mapsto \theta' \mapsto \theta',$$

se aplicarmos (i), (ii), (iii) e (iv) sucessivamente. □

Lema 2.64. Seja $L \supseteq K$ uma extensão finita, $L' \supseteq K'$ uma extensão qualquer, e $\sigma : K \to K'$ um isomorfismo. Então, existem no máximo $[L : K]$ imersões $\tilde{\sigma} : L \to L'$ que fazem o seguinte diagrama comutar

$$\begin{array}{ccc} L & \xhookrightarrow{\tilde{\sigma}} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow[\approx]{\sigma} & K' \end{array}$$

ou seja, que estendem σ.

Demonstração. Vamos fazer por indução em $n = [L : K]$. Caso $[L : K] = 1$, o resultado é óbvio, a única imersão possível e o próprio σ. Suponha, agora, que $[L : K] \geq 2$. Nesse caso, seja $\theta \in L \setminus K$ e $m(x)$ o polinômio minimal de θ, dessa forma, temos que $[K(\theta) : K] > 1$, e, portanto, $[L : K(\theta)] < [L : K]$. Pelo Lema Fundamental, existem no máximo $\deg(m^\sigma(x)) = \deg(m(x)) = [K(\theta) : K]$ imersões $\sigma' : K(\theta) \to L'$ e, pela hipótese de indução, no máximo $[L : K(\theta)]$ imersões $\tilde{\sigma} : L \to L'$ tal que o diagrama

$$\begin{array}{ccc} L & \xhookrightarrow{\tilde{\sigma}} & L' \\ \uparrow & & \uparrow \\ K(\theta) & \xrightarrow[\approx]{\sigma'} & \sigma'(K(\theta)) \\ \uparrow & & \uparrow \\ K & \xrightarrow[\approx]{\sigma} & K' \end{array}$$

Logo, existem no máximo $[L : K(\theta)][K(\theta) : K] = [L : K]$ imersões $\tilde{\sigma}$ satisfazendo as condições impostas. □

Teorema 2.65. Se L/K é uma extensão finita, então

$$|\mathrm{Aut}(L/K)| \leq [L : K].$$

Demonstração. Como todo K-automorfismo é uma K-imersão, segue diretamente pelo Lema 2.64, já que existirão no máximo $[L : K]$ K-automorfismos σ tal que o diagrama

$$\begin{array}{ccc} L & \xrightarrow[\approx]{\sigma} & L \\ \uparrow & & \uparrow \\ K & \xrightarrow[\approx]{\mathrm{id}} & K \end{array}$$

comuta. □

Exemplo 2.66. Qualquer extensão de grau 2 de $\mathbb{R}$ é isomorfa a $\mathbb{C}$. De fato, primeiro perceba que $\mathbb{C}$ não admite extensões quadráticas, visto

que é sempre possível extrair a raiz quadrada da fórmula da equação de segundo grau, assim todos os polinômio de segundo grau em $\mathbb{C}[x]$ têm raízes em $\mathbb{C}$.

Suponha, agora, que K é uma extensão de $\mathbb{R}$ de grau 2. Como visto no Exemplo 2.25, K deve ser uma extensão quadrática de $\mathbb{R}$, ou seja, $K = \mathbb{R}(\sqrt{\Delta})$ para algum $\Delta < 0$ em $\mathbb{R}$. Dessa forma, o polinômio minimal de $\sqrt{\Delta}$ é $x^2 - \Delta \in \mathbb{R}[x]$. Assim, pelo Lema Fundamental, existem duas $\mathbb{R}$-imersões de $\mathbb{R}(\sqrt{\Delta})$ até $\mathbb{C}$, uma para cada raiz de $x^2 - \Delta$, definidas por $\sqrt{\Delta} \mapsto \pm i\sqrt{|\Delta|}$, já que $\pm i\sqrt{|\Delta|}$ são as raízes de $x^2 - \Delta$ em $\mathbb{C}$.

Como essas $\mathbb{R}$-imersões são, também, $\mathbb{R}$-transformações lineares injetoras entre $\mathbb{R}$-espaços vetoriais de dimensão 2, elas também devem ser sobrejetoras, logo são $\mathbb{R}$-automorfismos.

Ou seja, não há nada de especial, particularmente, na construção dos complexos a partir da adjunção de uma raiz de $x^2 + 1$, a mesma construção poderia ter sido feita fazendo a adjunção da raiz de qualquer outro polinômio de segundo grau sem raízes em $\mathbb{R}$. Há de se argumentar, porém, que $x^2 + 1$ é o mais simples de tais polinômios, o que justifica a ampla utilização desse polinômio em particular para a construção de $\mathbb{C}$.

Vamos aplicar o Lema Fundamental em alguns exemplos para ilustrar o processo de como o grupo de automorfismos pode ser encontrado.

Exemplo 2.67. Considere a extensão $\mathbb{Q}(\sqrt{1+\sqrt{2}})$. Já vimos no Exemplo 2.23 que o polinômio minimal de $\sqrt{1+\sqrt{2}}$ é $x^4 - 2x^2 - 1$, cuja as raízes em $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ são $\pm\sqrt{1+\sqrt{2}}$ (as outras duas raízes são $\pm\sqrt{1-\sqrt{2}}$, que não são valores reais). Ou seja, pelo Lema Fundamental, existem apenas dois automorfismos de $\mathbb{Q}(\sqrt{1+\sqrt{2}})$,

que são a identidade, e σ definido por

$$\sigma(f(\sqrt{1+\sqrt{2}})) = f(\sigma(\sqrt{1+\sqrt{2}})) = f(-\sqrt{1+\sqrt{2}})$$

para qualquer $f(\sqrt{1+\sqrt{2}}) \in \mathbb{Q}(\sqrt{1+\sqrt{2}})$. Dessa forma,

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}) = \{\mathrm{id}, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}.$$

Exemplo 2.68. Vamos calcular o grupo de automorfismos da extensão $\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q}$. A ideia é olhar para essa extensão como uma cadeia de extensões simples

$$\mathbb{Q}(\sqrt{3},\sqrt{5}) \supseteq \mathbb{Q}(\sqrt{3}) \supseteq \mathbb{Q}$$

e utilizar o Lema Fundamental para calcular os automorfismos a cada "passo". Primeiramente temos a extensão quadrática $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$, e já sabemos, pelo Exemplo 2.57, que $\mathrm{Aut}(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) = \{\mathrm{id}, \tau\}$, onde τ é a conjugação. Vamos olhar agora para a extensão $\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q}(\sqrt{3})$ para descobrir todas as extensões possíveis desses $\mathbb{Q}$-automorfismos.

Sabemos que o polinômio minimal de $\sqrt{5}$ sobre $\sqrt{3}$ é $m(x) = x^2 - 5$ (visto que $\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$), assim, considere o seguinte diagrama

$$\begin{array}{ccc}
\mathbb{Q}(\sqrt{3},\sqrt{5}) & \xhookrightarrow{\tilde{\sigma}} & \mathbb{Q}(\sqrt{3},\sqrt{5}) \\
\uparrow & & \uparrow \\
\mathbb{Q}(\sqrt{3}) & \xhookrightarrow{\sigma} & \mathbb{Q}(\sqrt{3},\sqrt{5}) \\
\uparrow & & \uparrow \\
\mathbb{Q} & \hookrightarrow & \mathbb{Q}(\sqrt{3},\sqrt{5})
\end{array}$$

Caso $\sigma = \mathrm{id}$, então, pelo Lema Fundamental, temos duas possibilidades para $\tilde{\sigma}$, uma para cada raiz de $m^\sigma(x) = x^2 - 5$, que são $\pm\sqrt{5}$. Ou seja, existe a extensão de id que leva $\sqrt{5}$ para si mesmo, que será a identidade em $\mathbb{Q}(\sqrt{3},\sqrt{5})$, e a que leva $\sqrt{5}$ para $-\sqrt{5}$, que será extensão de id que "conjuga" $\sqrt{5}$. Vamos chamar este $\mathbb{Q}$-automorfismo de ρ.

No caso onde $\sigma = \tau$, novamente temos que $m^\sigma(x) = x^2 - 5$, assim, temos duas opções análogas: a extensão de τ que leva $\sqrt{5}$ em si mesma, que também chamaremos de τ, e a extensão de τ que leva $\sqrt{5}$ em $-\sqrt{5}$, que, coincidentemente, é igual às composições $\rho\tau$ e $\tau\rho$.

Note que, o Lema Fundamental garante apenas que essas aplicações são injetoras, e não necessariamente sobrejetoras. Entretanto, $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ é um $\mathbb{Q}$-espaço vetorial de dimensão finita, e essas aplicações podem ser vistas como transformações $\mathbb{Q}$-lineares. Nesse caso, elas serão bijeções, pois toda transformação injetora entre espaços de mesma dimensão são, também, obrigatoriamente sobrejetoras.

Resumindo, temos 4 $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\sqrt{3}, \sqrt{5})$, sendo eles

$$\begin{aligned}
\mathrm{id} &: \sqrt{3} \mapsto \sqrt{3} \text{ e } \sqrt{5} \mapsto \sqrt{5}, \\
\tau &: \sqrt{3} \mapsto -\sqrt{3} \text{ e } \sqrt{5} \mapsto \sqrt{5}, \\
\rho &: \sqrt{3} \mapsto \sqrt{3} \text{ e } \sqrt{5} \mapsto -\sqrt{5}, \\
\tau\rho &: \sqrt{3} \mapsto -\sqrt{3} \text{ e } \sqrt{5} \mapsto -\sqrt{5}.
\end{aligned}$$

Como, claramente, $\tau^2 = \rho^2 = \mathrm{id}$, devemos ter o seguinte isomorfismo

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}) = \langle \tau, \rho \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Visto que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ é o único grupo de ordem 4 que tem todos os elementos de ordem 2 (excluindo o elemento neutro).

Exemplo 2.69. Considere a extensão $\mathbb{Q}(\zeta)/\mathbb{Q}$, onde $\zeta = e^{2\pi i/p}$, a raiz p-ésima principal da unidade. Pelo Lema Fundamental, há uma correspondência de $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\zeta)$ com raízes de $f(x) = x^{p-1} + \cdots + x + 1$, que é o polinômio minimal de ζ sobre $\mathbb{Q}$, pelo Exemplo 2.20.

Como $f(x) = (x^p - 1)/(x - 1)$, suas raízes são compostas pelas raízes p-ésimas da unidade, com exceção de 1, que são dadas precisamente pelos números ζ^a com $a \in \{1, \cdots, p-1\}$. Assim, temos $p - 1$ $\mathbb{Q}$-automorfismos distintos, definidos por $\sigma_a(\zeta) = \zeta^a$ com $a \in \mathbb{Z}$.

É claro ver que

$$\sigma_a = \sigma_b \iff a \equiv b \pmod{p}.$$

Além disso, como $\sigma_a(\sigma_b(\zeta)) = \zeta^{ab} = \sigma_{ab}$, temos que $\sigma_a\sigma_b = \sigma_{ab}$. Dessa forma, há um isomorfismo de grupos (visto que é um homomorfismo injetor entre grupos finitos) $\mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$ dado por $\sigma_a \mapsto a \pmod{p}$.

Exemplo 2.70. Vamos calcular o grupo de automorfismos da extensão $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}$. Para isso, considere o empilhamento de diagramas

$$\begin{array}{ccc}
\mathbb{Q}(i, \sqrt[4]{2}) & \xrightarrow[\approx]{g} & \mathbb{Q}(i, \sqrt[4]{2}) \\
\uparrow & & \uparrow \\
\mathbb{Q}(\sqrt[4]{2}) & \xrightarrow{\quad f \quad} & \mathbb{Q}(i, \sqrt[4]{2}) \\
\uparrow & & \uparrow \\
\mathbb{Q} & \longrightarrow & \mathbb{Q}(i, \sqrt[4]{2})
\end{array}$$

Pelo Lema Fundamental, há uma opção de f para cada raiz do polinômio $x^4 - 2$, que é o polinômio minimal de $\sqrt[4]{2}$ sobre $\mathbb{Q}$. Ou seja, as quatro opções são definidas por $\sqrt[4]{2} \mapsto \sqrt[4]{2}$, $\sqrt[4]{2} \mapsto i\sqrt[4]{2}$, $\sqrt[4]{2} \mapsto -\sqrt[4]{2}$, $\sqrt[4]{2} \mapsto -i\sqrt[4]{2}$.

Para cada um desses morfismos, o polinômio minimal de i sobre $\mathbb{Q}(\sqrt[4]{2})$, quando aplicado a eles, continue $x^2 + 1$. Logo, há duas opções de g para cada uma das opções de f, definidas por $i \mapsto i$ e $i \mapsto -i$.

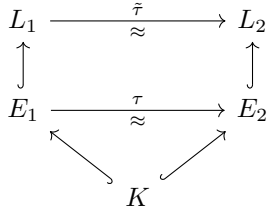
Ou seja, há 8 isomorfismos ao todo, sendo eles

$$\begin{aligned}
\mathrm{id} &: \sqrt[4]{2} \mapsto \sqrt[4]{2}, i \mapsto i,\\
\sigma &: \sqrt[4]{2} \mapsto i\sqrt[4]{2}, i \mapsto i,\\
\sigma^2 &: \sqrt[4]{2} \mapsto -\sqrt[4]{2}, i \mapsto i,\\
\sigma^3 &: \sqrt[4]{2} \mapsto -i\sqrt[4]{2}, i \mapsto i,\\
\tau &: \sqrt[4]{2} \mapsto \sqrt[4]{2}, i \mapsto -i,\\
\sigma\tau &: \sqrt[4]{2} \mapsto i\sqrt[4]{2}, i \mapsto -i,\\
\sigma^2\tau &: \sqrt[4]{2} \mapsto -\sqrt[4]{2}, i \mapsto -i,\\
\sigma^3\tau &: \sqrt[4]{2} \mapsto -i\sqrt[4]{2}, i \mapsto -i.
\end{aligned}$$

Ou seja, $\mathrm{Aut}(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}) = \langle \sigma, \tau \rangle$. É fácil ver que tal grupo é isomorfo a D_8, onde σ é a rotação de 90° e τ é a reflexão sobre a reta vertical que passa ao centro do quadrado, já que as ordens de σ e τ são, respectivamente, 4 e 2, e $\sigma\tau = \tau\sigma^3$.

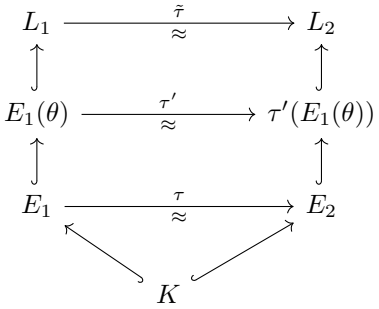
Por fim, vamos mostrar a unicidade, a menos de isomorfismo, dos corpos de raízes e fechos algébricos.

Teorema 2.71. Sejam $L_1 \supseteq E_1 \supseteq K$ e $L_2 \supseteq E_2 \supseteq K$ corpos, de tal forma que L_1 e L_2 sejam dois corpos de raízes de um polinômio $f(x) \in K[x]$, e $\tau : E_1 \to E_2$ um K-isomorfismo. Então, existe um K-isomorfismo $\tilde{\tau} : L_1 \to L_2$ que estende τ, ou equivalentemente, que faz o seguinte diagrama comutar



Demonstração. Vimos no Teorema 2.44 que o grau das extensões $L_1 \supseteq K$ e $L_2 \supseteq K$ são ambas finitas, e, portanto, $L_i \supseteq E_i$ (i = 1,2) também são, vamos fazer então indução sobre $[L_1 : E_1]$. Caso $[L_1 : E_1] = 1$, temos que $L_1 = E_1$ e basta tomar $\tilde{\tau} = \tau$.

Para o passo indutivo, suponha que $[L_1 : E_1] > 1$, e seja $\theta \in L_1 \setminus E_1$ uma raiz de $f(x)$. Então, pelo Lema Fundamental, existe uma extensão de τ, digamos $\tau' : E_1(\theta) \to L_2$, para cada raiz de $f^{\tau}(x) = f(x)$ em L_2. Como L_2 e um corpo de raízes de $f(x)$, tal extensão certamente existe. Além disso, já que $[L_1 : E_1(\theta)] < [L_1 : E_1]$, temos, pela hipótese de indução, que existe uma extensão $\tilde{\tau}$ estendendo τ' de forma que o diagrama comute



Logo $\tilde{\tau}$ é uma extensão de τ, o que completa o teorema. □

Corolário 2.72. Seja K um corpo e $f(x) \in K[x]$, então quaisquer dois corpos de raízes de $f(x)$ sobre K são isomorfos.

Demonstração. Basta tomar $E_1 = E_2 = K$, e $\tau = \mathrm{id}$ no teorema anterior. □

O seguinte teorema nos diz que qualquer extensão algébrica pode ser "encaixada" em um corpo algebricamente fechado.

Teorema 2.73. Seja $L \supseteq K$ uma extensão algébrica, Ω é um corpo algebricamente fechado, e $\sigma : K \to \Omega$ uma imersão, então existe uma

extensão $\tilde{\sigma} : L \to \Omega$ de σ. Ou seja, para qualquer σ, existe $\tilde{\sigma}$ tal que o diagrama a seguir comuta

$$\begin{array}{ccc} L & \xrightarrow{\tilde{\sigma}} & \Omega \\ \uparrow & \nearrow_{\sigma} & \\ K & & \end{array}$$

Demonstração. Seja S o conjunto de pares (E, τ) onde $E \supseteq K$ é uma extensão algébrica e τ é uma extensão de σ. Considere a seguinte relação de ordem parcial sobre S, onde

$$(E_1, \tau_1) \succeq (E_2, \tau_2) \iff E_1 \supseteq E_2 \text{ e } \tau_1 \text{ é uma extensão de } \tau_2.$$

Utilizaremos o Lema de Zorn para provar que S tem um elemento maximal. Note que S não é vazio, pois obviamente $(K, \sigma) \in S$. Também, para qualquer subconjunto totalmente ordenado de S $C = \{(E_i, \tau_i) : i \in I\}$ (onde I é algum conjunto de índices) temos que a extensão $E' = \bigcup_{i \in I} E_i$ junto com a imersão $\tau' : E' \to \Omega$ definida por $\tau'(x) = \tau_i(x)$ se $x \in E_i$ formam claramente uma cota superior de C. Como C é arbitrária, S tem um elemento maximal em relação a $\succeq$.

Seja $(M, \tilde{\sigma})$ esse elemento maximal, vamos provar que $M = L$. De fato, se tivéssemos $L \supsetneq M$, existiria $\theta \in L \setminus M$ algébrico sobre K, de forma que $M(\theta) \supsetneq M$. Assim, pelo Lema Fundamental, teríamos que existe uma extensão de $\tilde{\sigma}$ que leva $M(\theta)$ até Ω (já que Ω é algebricamente fechado logo possui todas as raízes da imagem do polinômio minimal de θ), o que é um absurdo, pois contradiz a maximalidade de $(M, \tilde{\sigma})$. Portanto segue o resultado. □

Corolário 2.74. Seja K um corpo, então quaisquer dois fechos algebricos K_1^{alg} e K_2^{alg} de K são isomorfos.

Demonstração. Pelo teorema anterior, existe uma K-imersão

$$\sigma : K_1^{\text{alg}} \to K_2^{\text{alg}}.$$

Perceba que $\sigma(K_1^{\text{alg}})$ é algebricamente fechado, pois é isomorfo a K_1^{alg}). Além disso, a extensão $K_2^{\text{alg}} \supseteq \sigma(K_1^{\text{alg}})$ é algébrica. Segue, então, que $\sigma(K_1^{\text{alg}}) = K_2^{\text{alg}}$ pela condição (iii) do Teorema 2.47. □

Corolário 2.75. Seja K um corpo, $\sigma : K \to K$ um automorfismo e K^{alg} seu fecho algébrico. Então, existe um automorfismo $\tilde{\sigma}$ de K^{alg} que estende σ, ou equivalentemente, que faz o seguinte diagrama comutar

$$\begin{array}{ccc} K^{\text{alg}} & \xrightarrow[\approx]{\tilde{\sigma}} & K^{\text{alg}} \\ \uparrow & & \uparrow \\ K & \xrightarrow[\approx]{\sigma} & K \end{array}$$

Demonstração. Mudando o contra-domínio de σ para K^{alg}, σ pode ser considerada uma imersão de K em K^{alg}, e portanto, pelo Teorema 2.73, pode ser estendida até uma imersão $\tilde{\sigma} : K^{\text{alg}} \hookrightarrow K^{\text{alg}}$, tal imersão deve ser um isomorfismo, já que $\tilde{\sigma}(K^{\text{alg}})$ é algebricamente fechado, e, portanto, deve coincidir com K^{alg} pela condição (iii) do Teorema 2.47, novamente. □

Nesse capítulo estudamos as estruturas das extensões de corpos e algumas noções fundamentais para o desenvolvimento da teoria que vem a seguir. A existência e unicidade do fecho algébrico de um corpo será um resultado de muita importância quando estudarmos sobre extensões separáveis, a seguir, apesar do fato de que, em geral, um fecho algébrico é um corpo extremamente difícil de ser encontrado explicitamente (no caso dos racionais, seu fecho algébrico pode ser identificado como um subcorpo dos complexos, porém o caso não é tão simples em geral).

3 TEORIA DE GALOIS

Nesse capítulo iniciamos o estudo próprio da Teoria de Galois, que é, resumidamente, o estudo das extensões de corpos por meio de seus grupos de automorfismos.

Até agora, desenvolvemos as ferramentas necessárias para o cálculo do grupo de automorfismos de uma extensão, porém, de nada falamos sobre a relação desse grupo de automorfismos com a estrutura da extensão em si. Veremos aqui que, dada algumas condições chamadas de separabilidade e normalidade, é possível fazer o "caminho reverso": a estrutura do grupo de automorfismos de uma extensão nos dá a informação completa sobre a estrutura dela.

3.1 EXTENSÕES E POLINÔMIOS SEPARÁVEIS

Iniciamos com a noção de separabilidade para polinômios.

Definição 3.1. Seja K um corpo, K^{alg} um fecho algébrico de K e $f(x) \in K[x]$ um polinômio qualquer. Então, $f(x)$ é dito ser separável se todas as suas raízes são distintas em K^{alg}. Caso contrário, $f(x)$ é dito ser um polinômio inseparável.

Veremos que a derivada formal dos polinômios é, surpreendentemente, muito útil para verificar se um polinômio é separável ou não.

Por derivada "formal", queremos dizer que estamos aplicando o cálculo da derivada apenas em forma, desprovido de qualquer significado analítico. visto que os corpos que estamos lidando aqui não são, necessariamente, subcorpos de $\mathbb{C}$. Vamos primeiro definir a derivada formal em termos precisos.

Definição 3.2. Seja K um corpo. Definimos a derivada formal como

uma aplicação $\frac{d}{dx} : K[x] \to K[x]$ onde $\frac{d}{dx}(x^n) = nx^{n-1}$ para qualquer $n \in \mathbb{N}$, e todo elemento de K é um ponto fixo de $\frac{d}{dx}$.

É simples mostrar (e, portanto, não vamos nos alongar nesse aspecto) que ela obedece as regras algébricas da derivada, ou seja, $\frac{d}{dx}(f+g) = \frac{d}{dx}(f) + \frac{d}{dx}(g)$, e $\frac{d}{dx}(fg) = \frac{d}{dx}(f)g + \frac{d}{dx}(g)f$. Com essas regras, é possível mostrar, também, por indução, a "regra do tombo" e a regra da cadeia.

Utilizaremos também a notação f' para representar a derivada do polinômio f, em vez de $\frac{d}{dx}(f)$.

Proposição 3.3. Seja K um corpo e $f(x) \in K[x]$ um polinômio qualquer. Nessas condições, se $p(x)$ é um fator primo de multiplicidade α na fatoração prima de $f(x)$ em $K[x]$ com derivada não nula, então $p(x)$ será um fator primo de multiplicidade $\alpha - 1$ de $f'(x)$.

Demonstração. Se $p(x)$ é um fator primo de multiplicidade α de $f(x)$, então temos que $f(x) = p(x)^\alpha g(x)$ para algum $g(x) \in K[x]$, onde $p(x) \nmid g(x)$. Derivando formalmente $f(x)$, temos que $f'(x) = p(x)^{\alpha-1}(\alpha p'(x)g(x) + p(x)g'(x))$.

Perceba que $p(x)$ definitivamente não divide $p'(x)g(x)+p(x)g'(x)$, pois não divide $p'(x)$ (é um polinômio não nulo de grau menor que $p(x)$), e não divide $g(x)$ por hipótese. Logo, não divide o termo à esquerda, $p'(x)g(x)$, mas divide o termo a direita. Assim, $p'(x)g(x) + p(x)g'(x)$ não pode ser um múltiplo de $p(x)$. Ou seja, $p(x)$ é um fator primo de multiplicidade $\alpha - 1$ de $f(x)$. □

Isso nos leva ao principal critério de separabilidade. Ele nos permite, com facilidade, verificar por meio de algum método ou algoritmo, como o algoritmo de Euclides, se um polinômio é separável olhando apenas para o corpo dos coeficientes, sem a necessidade de qualquer informação relacionada ao fecho algébrico do corpo.

Teorema 3.4. Seja K um corpo e $f(x) \in K[x]$, então

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

Demonstração. ($\Longrightarrow$) Seja K^{alg} um fecho algébrico de K. Se $f(x)$ é separável, sua fatoração prima consiste apenas em fatores lineares distintos de multiplicidade 1 em $K^{\text{alg}}[x]$. Como a derivada de polinômios lineares é sempre não nula, $f(x)$ não compartilha nenhum desses fatores com $f'(x)$, pela Proposição 3.3. Segue que $\text{mdc}(f(x), f'(x)) = 1$ em $K^{\text{alg}}[x]$, portanto o mesmo deve ser verdade em $K[x]$.

($\Longleftarrow$) Se $f(x)$ é inseparável, temos que existe uma raiz múltipla de $f(x)$ em $K^{\text{alg}}[x]$, digamos θ, ou seja, $x - \theta$ é um fator primo com multiplicidade maior que 1 de $f(x)$. Pela Proposição 3.3, temos que $x - \theta$ também é um fator primo de $f'(x)$, portanto $f(\theta) = f'(\theta) = 0$.

Nessas condições, teríamos que o polinômio minimal de θ sobre K é um divisor comum de $f(x)$ e $f'(x)$. Ou seja, o polinômio minimal de θ divide $\text{mdc}(f(x), f'(x))$. Então esse divisor comum não pode ser igual a 1 em $K[x]$. De fato, todo polinômio irredutível tem grau, no mínimo, 1 e, portanto, não pode dividir uma constante. □

Corolário 3.5. Seja K um corpo e $f(x) \in K[x]$ um polinômio irredutível. Nessas condições,

$$f(x) \text{ é separável } \iff f'(x) \neq 0.$$

Demonstração. ($\Longrightarrow$) Suponha por absurdo que $f(x)$ é inseparável, e $f'(x) \neq 0$. Assim, pelo teorema anterior, $\text{mdc}(f(x), f'(x))$ não pode ser 1. Por outro lado, $\text{mdc}(f(x), f'(x)) = f(x)$ apenas se $f'(x) = 0$, pois esse é o único caso onde $f(x) \mid f'(x)$, mas isso não pode ocorrer, pela hipótese.

Ou seja, $\text{mdc}(f(x), f'(x))$ não pode ser 1 nem $f(x)$. Isso é um absurdo, pois esses seriam os únicos candidatos possíveis ao máximo divisor comum, como $f(x)$ é irredutível.

($\Longleftarrow$) Perceba que $f(x)$ certamente não divide $f'(x)$, visto que $f'(x) \neq 0$, e $\deg(f(x)) > \deg(f'(x))$. Nessas condições, como $f(x)$ é irredutível, a única possibilidade para divisor comum de $f(x)$ e $f'(x)$ é 1. □

Exemplo 3.6. Pelo corolário 3.5, todo polinômio irredutível em $\mathbb{Q}[x]$ é separável, visto que a derivada de um polinômio irredutível não pode ser 0. De fato, os únicos elementos de $\mathbb{Q}[x]$ que tem derivada nula são os polinômios constantes, que não são irredutíveis.

O mesmo argumento funciona, em geral, para qualquer corpo de característica 0, logo a separabilidade polinômios irredutíveis se torna um aspecto um tanto trivial.

Exemplo 3.7. Seja K um corpo e $f(x) = x^n - a \in K[x]$, com $n \in \mathbb{N}$ e $a \in K$. Se $\text{char}(K) \nmid n$, então $f'(x) = nx^{n-1}$. Além disso, como $x^n - a$ não possui fatores de x, segue que $\text{mdc}(nx^{n-1}, x^n - 1) = 1$. Ou seja, todas as raízes n-ésimas de a são distintas se $\text{char}(K) \nmid n$.

Por outro lado, se $\text{char}(K) \mid n$, então

$$f'(x) = nx^{n-1} = 0x^{n-1} = 0.$$

Assim, $\text{mdc}(x^n - a, 0) = x^n - a \neq 1$. Ou seja a tem raízes n-ésimas repetidas.

Agora que as definições e resultados relativos a polinômios separáveis já estão estabelecidos, vamos a definição e propriedades das extensões separáveis.

Definição 3.8. Seja L/K uma extensão de corpos e $\theta \in L$, então

- Um elemento algébrico $\theta \in L$ é dito ser um elemento separável sobre K se o seu polinômio minimal é separável, caso contrário, o elemento é dito ser inseparável sobre K.

- De forma semelhante, L/K é dita ser separável se todo elemento de L é separável sobre K, e inseparável caso contrário.

Exemplo 3.9. Toda extensão em corpos de característica 0 é separável, visto todo elemento tem polinômio minimal irredutível, portanto separável, pelo Exemplo 3.6.

O seguinte teorema será demonstrado para auxiliar na demonstração de Teorema 3.11. Posteriormente, no Corolário 3.14, sua recíproca também será demonstrada.

Lema 3.10. Sejam $M \supseteq L \supseteq K$ corpos. Então,

$$M/K \text{ é separável } \implies M/L \text{ e } L/K \text{ são separáveis.}$$

Demonstração. Se o polinômio minimal sobre K de todo elemento de M é separável sobre K, o mesmo será obviamente verdade para L. Portanto L/K é separável.

Agora, como todo elemento $\theta \in M$ tem polinômio minimal $m_K(x)$ (sobre K) separável, o polinômio minimal $m_L(x)$ de θ sobre L o divide. Portanto, $m_L(x)$ também é separável, e segue que L/K é uma extensão separável. □

Teorema 3.11. Seja L/K uma extensão finita, Ω um corpo algébricamente fechado, e $\sigma : K \to \Omega$ uma imersão. Então, o número de K-imersões $\tilde{\sigma} : L \to \Omega$ que fazem o diagrama

$$\begin{array}{ccc} L & \xhookrightarrow{\tilde{\sigma}} & \Omega \\ \uparrow & \nearrow_{\sigma} & \\ K & & \end{array}$$

comutar (ou equivalentemente, estende σ) é no máximo $[L : K]$, com igualdade se, e somente se, L/K é separável.

Demonstração. O fato de que existem no máximo $[L : K]$ imersões que estendem σ segue diretamente do Lema 2.64. Vamos, então, mostrar que a igualdade ocorre se, e somente se, L/K é separável.

Vamos mostrar a ida por indução em $[L : K]$. O caso base onde $[L : K] = 1$ é trivial, teremos apenas σ como morfismo.

Agora, se L/K for separável, as extensões $L/K(\theta)$ e $K(\theta)/K$ são separáveis pelo lema anterior. Logo $m(x)$ e $m^\sigma(x)$ seriam separáveis sobre seus respectivos anéis de polinômios. Ou seja, existem exatamente $[K(\theta) : K]$ imersões σ', devido ao Lema Fundamental e pelo fato de que $m^\sigma(x)$ é separável.

Perceba que $[L : K(\theta)] < [L : K]$, visto que $[K(\theta) : K] > 1$. Assim, pela hipótese de indução, para cada uma dessas $[K(\theta) : K]$ K-imersões de $K(\theta)$ até Ω, existem exatamente $[L : K(\theta)]$ K-imersões de L até Ω que a estendem. Portanto, existem precisamente $[L : K(\theta)][K(\theta) : K] = [L : K]$ K-imersões que vão de L até Ω.

Para a recíproca, vamos demonstrar por contra-positiva. Caso L/K for inseparável, escolha $\theta \in L$ de modo que ele seja inseparável sobre K. Assim teremos um número estritamente menor que $[K(\theta) : K]$ de K-imersões $\sigma' : K(\theta) \to \Omega$ pelo Lema Fundamental.

Isso, definitivamente, resultará em menos que $[L : K] = [L : K(\theta)][K(\theta) : K]$ imersões $\tilde{\sigma}$ ao todo, pois o número de K-morfismos que estendem cada escolha de σ' é, no máximo, $[L : K(\theta)]$. □

Corolário 3.12. Seja L/K uma extensão de corpos e $\theta_1, \ldots, \theta_n \in L$ elementos algébricos sobre K. Então,

$$\theta_1, \ldots, \theta_n \text{ são separáveis sobre } K \iff K(\theta_1, \ldots, \theta_n)/K \text{ é separável.}$$

Demonstração. ($\Longrightarrow$).Vamos primeiro provar o caso onde a extensão é simples, para posteriormente mostrar o caso geral.

Seja $\theta \in L$ um elemento separável sobre K, $m(x)$ seu polinômio minimal e K^{alg} um fecho algébrico de K. Pelo Lema Fundamental,

existem tantas K-imersões de $K(\theta)$ em K^{alg} quanto raízes de $m(x)$ em K^{alg}. Além disso, como $m(x)$ é separável, existem exatamente $\deg(m(x)) = [K(\theta) : K]$ dessas K-imersões. Portanto, $K(\theta)/K$ é separável pelo Teorema 3.11.

Para o caso geral, basta notar que, se tivermos $\theta_1, \ldots, \theta_n \in L$ todos separáveis sobre K, cada um dos θ_i será separável sobre $K(\theta_1, \ldots, \theta_{i-1})$.

De fato, o polinômio minimal de θ_i, para cada $i \in \{1, \ldots, n\}$, sobre $K(\theta_1, \ldots, \theta_{i-1})$ divide seu polinômio minimal sobre K, que é separável, logo também será separável.

Assim, podemos adicionar indutivamente cada θ_i, obtendo que $K(\theta_1, \ldots, \theta_n)$ é uma extensão separável de K.

($\Longleftarrow$). Pela definição de separabilidade, todo polinômio de $K(\theta_1, \ldots, \theta_n)$ é separável sobre K. Em particular, o mesmo será verdade para $\theta_1, \ldots, theta_n$. □

Corolário 3.13. Seja L/K uma extensão de corpos e $\alpha, \beta \in L$ elementos separáveis sobre K, então $\alpha \pm \beta$, $\alpha\beta$ e α/β (para $\beta \neq 0$) são separáveis sobre K.

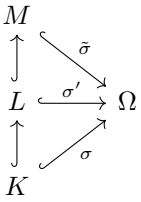
Demonstração. Como α, β são separáveis sobre K, temos, pelo teorema anterior, que $K(\alpha, \beta)/K$ é uma extensão separável. Assim, como $\alpha \pm \beta, \alpha\beta$ e $\alpha/\beta \in K(\alpha, \beta)$ estão em $K(\alpha, \beta)$, esses elementos também são separáveis sobre K. □

Corolário 3.14. Sejam $M \supseteq L \supseteq K$ corpos. Então,

$$M/K \text{ é separável } \iff M/L \text{ e } L/K \text{ são separáveis.}$$

Demonstração. A implicação ($\Longrightarrow$) já foi feita no Lema 3.10. Para a recíproca, suponha que M/L e L/K são separáveis. Vamos demonstrar primeiro o caso em que ambas as extensões são finitas. Para isso, considere um fecho algébrico K^{alg} de K, e $\sigma : K \to K^{\text{alg}}$ a inclusão

de K em K^{alg}. Pelo Teorema 3.11, existem $[L : K]$ imersões σ' e, para cada uma dessas, $[M : L]$ imersões $\tilde{\sigma}$ tal que o diagrama



comuta, resultando em $[M : L][L : K] = [M : K]$ K-imersões totais de M em K^{alg}, e, portanto, M/K é separável.

Vamos provar agora o caso geral. Seja $\theta \in M$ um elemento qualquer, $m(x) = x^n + a_1x^{n-1} + \cdots + a_n \in L[x]$ seu polinômio minimal (separável, por hipótese) sobre L. Por hipótese, $a_1, \ldots, a_n$ são todos separáveis sobre K, logo $K(a_1, \ldots, a_n)/K$ é separável, e como θ é raiz de $m(x)$ que é um polinômio separável em $K(a_1, \ldots, a_n)$, $K(a_1, \ldots, a_n, \theta) \supseteq K(a_1, \ldots, a_n)$ é separável. Pela transitividade do caso finito já mostrada, segue que θ é separável sobre K. □

Teorema 3.15 (Teorema do Elemento Primitivo)**.** Se K é um corpo de cardinalidade infinita e L/K uma extensão finita e separável, então existe $\theta \in L$ tal que $L = K(\theta)$.

Demonstração. Já sabemos que se L/K é finita, existem elementos algébricos $\theta_1, \ldots, \theta_n \in L$ tal que $L = K(\theta_1, \ldots, \theta_n)$, vamos provar por indução em n que é sempre possível escrever L como uma extensão simples. Isso é óbvio para $n = 1$, e para o caso indutivo, mostraremos primeiro que, para quaisquer $\alpha, \beta \in L$, existe $c \in K$ onde $K(\alpha, \beta) = K(\alpha + c\beta)$.

De fato, temos, por hipótese, que $K(\alpha, \beta)/K$ é uma extensão separável. Logo, pelo Teorema 3.11, existem exatamente $m = [K(\alpha, \beta) : K]$ K-imersões, digamos $\sigma_1, \ldots, \sigma_m$, de $K(\alpha, \beta)$ em um fecho algébrico K^{alg} de K.

Cada uma dessas K-imersões induz uma K-imersão de $K(\alpha + c\beta)$ em K^{alg}, para qualquer $c \in K$. Além disso, como $K(\alpha + c\beta)/K$ é separável, seu grau coincide com o número de tais K-imersões distintas.

Assim, para maximizar o grau dessa extensão, basta escolher c de forma que, para quaisquer $i, j \in \{1, \ldots, m\}$ distintos,

$$\sigma_i(\alpha + c\beta) \neq \sigma_j(\alpha + c\beta).$$

Reorganizando a equação, isso equivale a dizer que

$$\sigma_i(\alpha) - \sigma_j(\alpha) \neq c(\sigma_i(\beta) - \sigma_j(\beta)).$$

Se $\sigma_i(\beta) - \sigma_j(\beta) = 0$ para algum par (i, j) onde $i \neq j$, então certamente devemos ter que $\sigma_i(\beta) - \sigma_j(\beta) \neq 0$. De fato, caso contrário σ_i e σ_j seriam morfismos de $K(\alpha, \beta)$ até K^{alg} iguais, o que não pode ocorrer. Ou seja, qualquer valor de c, nesse caso, faria com que a inequação $\sigma_i(\alpha) - \sigma_j(\alpha) \neq c(\sigma_i(\beta) - \sigma_j(\beta))$ fosse verdadeira, visto que o lado direito é nulo, e o esquerdo não.

Agora, caso $\sigma_i(\beta) - \sigma_j(\beta) \neq 0$, podemos dividir ambos os lados por esse elemento e obter que

$$c \notin \left\{ \frac{\sigma_i(\alpha) - \sigma_j(\alpha)}{\sigma_i(\beta) - \sigma_j(\beta)} : 1 \leq i, j \leq m,\ \sigma_i(\beta) \neq \sigma_j(\beta) \right\}$$

Assim, basta tomar c como qualquer elemento não nulo desse conjunto. Isso é sempre possível, pois tal conjunto é finito, enquanto K é infinito. Logo, todas as imersões $\sigma_1, \ldots, \sigma_m$, se restritas a $K(\alpha + c\beta)$, são distintas. Segue, então, que $[K(\alpha + c\beta) : K] \geq m$, pelo Teorema 3.11.

Como $K(\alpha, \beta) \supseteq K(\alpha + c\beta)$, também temos que $m \geq [K(\alpha + c\beta) : K]$. Logo, o grau de ambas as extensões são iguais, assim $K(\alpha, \beta) = K(\alpha + c\beta)$.

Para completar o passo indutivo, suponha que tenhamos uma extensão finita separável $K(\theta_1, \ldots, \theta_n)/K$. Pela hipótese de indução,

$K(\theta_1, \ldots, \theta_n) = K(\theta, \theta_n)$ para algum $\theta \in K(\theta_1, \ldots, \theta_{n-1})$. Daí, existe $c \in K$ tal que $K(\theta, \theta_n) = K(\theta + c\theta_n)$, o que completa a demonstração. □

Observação 3.16. A prova do caso onde K é um corpo finito tem uma abordagem completamente diferente, e será feita mais adiante no Capítulo 4. Seguiremos o texto, porém, assumindo que o teorema é verdade também no caso finito. Isso não afetará a integridade lógica do trabalho, pois nenhum dos resultados nesse capítulo, a partir deste ponto, são utilizados para a demonstração do Teorema do Elemento Primitivo para corpos finitos.

Como resultado final desse capítulo, mostraremos que a separabilidade é preservada em transportes paralelos

Proposição 3.17. Seja L/K' um transporte paralelo de uma extensão L/K. Então, se L/K é separável, L'/M' também é.

Demonstração. Como L'/K' é um transporte paralelo de L/K, então existe um corpo M onde $L' = LM$ e $K' = KM$. Assim, se $\theta \in L' = LM$ é um elemento qualquer, então existem $a_i, a_i' \in L$ e $b_i, b_i' \in M$ onde

$$\theta = \frac{a_1 b_1 + \cdots + a_n b_n}{a_1' b_1' + \cdots + a_m' b_m'}.$$

Os termos b_i e b_i' claramente são separáveis sobre M, visto que seus polinômios minimais são $x - b_i$ e $x - b_i'$ respectivamente, que são separáveis. Similarmente, como os elementos a_i e a_i' são todos separáveis sobre K por hipótese, eles são raízes de algum polinômio separável em $K[x] \subseteq M[x]$, portanto são separáveis em M.

Por fim, como a soma, produto, e divisão de elementos separáveis também é um elemento separável (Corolário 3.13), segue que θ é separável sobre M. □

3.2 EXTENSÕES NORMAIS

Enquanto extensões separáveis garantem o maior número de imersões em corpos algebricamente fechados, a condição de normalidade é criada a fim de garantir que tais imersões possam todas ser vistas como automorfismos. O nome faz referência à condição de normalidade de subgrupos, relação que será mais profundamente explorada no Teorema Fundamental da Teoria de Galois.

Definiremos essas extensões, primeiramente, com uma condição um pouco mais simples que a explicitada no parágrafo anterior.

Definição 3.18. Uma extensão L/K algébrica é dita ser normal se ela é fechada sobre conjugados. Isto é, para todo $\theta \in L$, o polinômio minimal de θ se decompõe em fatores lineares em $L[x]$, ou, equivalentemente, se todos os conjugados de θ sobre K estão em L.

Exemplo 3.19. Como já vimos no Exemplo 2.23, a extensão

$$\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}$$

não é fechada sobre $\mathbb{Q}$-conjugados, visto que $\sqrt{1-\sqrt{2}}$ é um conjugado de $\sqrt{1+\sqrt{2}}$ sobre $\mathbb{Q}$, porém não está em $\mathbb{Q}(\sqrt{1+\sqrt{2}})$, já que é um valor complexo.

Exemplo 3.20. Toda extensão quadrática é normal. De fato, seja $K(\sqrt{\alpha})/K$ tal extensão, e $a + b\sqrt{\alpha} \in K(\alpha)$ um elemento qualquer. Então, como $a + b\sqrt{\alpha}$ é raiz do polinômio $(x-a)^2 - \alpha b^2$, o único conjugado possível de $a + b\sqrt{\alpha}$ é $a - b\sqrt{\alpha}$, que é a outra raiz desse polinômio, que também está em $K(\sqrt{\alpha})$.

Exemplo 3.21. Seja L/K uma extensão normal e M um corpo intermediário de L/K, isto é, $K \subseteq M \subseteq L$. Nessas condições, L/M também será separável.

Isso se dá pois, pelo Teorema 3.22, L deve ser o corpo de raízes sobre K de alguma família de polinômios $S \subseteq K[x]$. Ou seja, $L = K(\mathfrak{R})$, onde $\mathfrak{R}$ é o subconjunto das raízes dos polinômios S, em algum fecho algébrico de K.

Nessas condições, pode-se observar que $K(\mathfrak{R}) = M(\mathfrak{R})$. De fato, a inclusão $\subseteq$ é clara, visto que $K \subseteq M$, e como $K(\mathfrak{R})$, e a inclusão $\supseteq$ ocorre pela definição de $M(\mathfrak{R})$, pois $K(\mathfrak{R})$ é um corpo que contém tanto M quanto $\mathfrak{R}$.

Aqui temos algumas equivalências da condição de normalidade, que justificam os comentários feitos no início da sessão.

Teorema 3.22. Seja L/K uma extensão algébrica, e K^{alg} um fecho algébrico de L, então as seguintes condições são equivalentes:

(i) L/K é normal.

(ii) L/K é o corpo de raízes de alguma família de polinômios de $K[x]$.

(iii) Toda K-imersão de L em K^{alg} induz um K-automorfismo de L.

(iv) Para qualquer extensão M/L, todo K-automorfismo de M induz um K-automorfismo de L.

(v) Qualquer K-automorfismo de K^{alg} induz um K-automorfismo de L.

Demonstração. (i) $\Longrightarrow$ (ii). Basta tomar L como o corpo de raízes dos polinômios minimais de seus elementos.

(ii) $\Longrightarrow$ (iii). Denote momentaneamente o conjunto de raízes de um polinômio $f(x) \in K[x]$ por $V(f(x))$. Por hipótese, existe uma família de polinômios $S \subseteq K[x]$ tal que $L = K(\Lambda)$, onde Λ é o

conjunto de raízes de S dado por $\bigcup_{f(x)\in S} V(f(x))$. Assim, para qualquer K-imersão $\sigma : L \to K^{\text{alg}}$. Assim,

$$\sigma(\Lambda) = \sigma(\bigcup_{f(x)\in S} V(f(x))) = \bigcup_{f(x)\in S} \sigma(V(f(x))) = \bigcup_{f(x)\in S} V(f(x)) = \Lambda.$$

Ou seja, σ permuta Λ, e como σ também preserva K, devemos ter que $\sigma(K(\Lambda)) = K(\Lambda)$, e segue o resultado.

(iii) $\Longrightarrow$ (iv). Qualquer K-automorfismo $\sigma : M \to M$ pode ser estendido a uma K-imersão $i \circ \sigma : M \to M^{\text{alg}}$, onde $i : M \to M^{\text{alg}}$ é a inclusão. Assim $i \circ \sigma|_L$ será um K-automorfismo de L por hipótese, já que M^{alg} é um fecho algébrico de L.

(iv) $\Longrightarrow$ (v) Basta tomar $M = K^{\text{alg}}$.

(v) $\Longrightarrow$ (i) Seja $\alpha \in L$ um elemento qualquer, e $\beta \in K^{\text{alg}}$ um conjugado de α, devemos mostrar que $\beta \in L$. Temos, pela Lema Fundamental, uma imersão $\sigma : L \to K^{\text{alg}}$ onde $\sigma(\alpha) = \beta$. Essa imersão pode ser estendida para um automorfismo de K^{alg}, e, portanto, devemos ter que $\beta = \sigma(\alpha) \in \sigma(L) \subseteq L$ por hipótese. □

Proposição 3.23. Seja L/K uma extensão normal e LM/M um transporte paralelo dessa extensão. Então, LM/M também é normal.

Demonstração. Como L/K é normal, L é o corpo de raízes de algum conjunto de polinômios $S \subseteq K[x]$ sobre K, então LM é o corpo de raízes do mesmo conjunto $S \subseteq M[x]$ sobre M, e, portanto, LM/M é normal pelo item (ii) do teorema anterior. □

Exemplo 3.24. A extensão $\mathbb{Q}(\zeta_n, \sqrt[n]{a})/\mathbb{Q}$ é normal, onde $\zeta_n = e^{2\pi i/n}$ e $a \in \mathbb{Q}$. De fato, $\mathbb{Q}(\zeta_n, \sqrt[n]{a})$ é o corpo de raízes do polinômio $x^n - a$ sobre $\mathbb{Q}$, pelo Exemplo 2.43. Em particular, a extensão $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ é, também, normal.

Exemplo 3.25. A extensão $K(x_1, \ldots, x_n)/K(e_1, \ldots, e_n)$ é normal, pois é o corpo de raízes do polinômio $x^n - e_1 x^{n-1} + \cdots + (-1)^n e_n$.

Teorema 3.26. Seja L/K uma extensão normal finita. Então $\mathrm{Aut}(L/K)$ age transitivamente sobre conjugados, isto é, se $\alpha, \beta \in L$ são conjugados entre si, então existe um K-automorfismo σ de L onde $\sigma(\alpha) = \beta$.

Demonstração. Seja K^{alg} um fecho algébrico de L. Pelo Lema Fundamental, existe uma K-imersão $\sigma : K(\alpha) \to L$ onde $\sigma(\alpha) = \beta$, essa K-imersão σ pode ser estendida a uma K-imersão $\tilde{\sigma} : L \to K^{\mathrm{alg}}$ pelo Teorema 2.73. Além disso, pelo Teorema 3.22, $\tilde{\sigma}$ induz um K-automorfismo de L. Como $\tilde{\sigma}$ é uma extensão de σ, o resultado está provado. □

Teorema 3.27. Sejam $L \supseteq M \supseteq K$ corpos com L/K e M/K normais. Então, existe um morfismo sobrejetor $\mathrm{Aut}(L/K) \twoheadrightarrow \mathrm{Aut}(M/K)$, dada por $\sigma \mapsto \sigma|_M$. Além disso, temos um isomorfismo

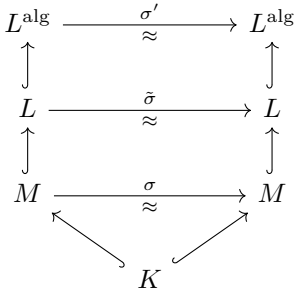
$$\frac{\mathrm{Aut}(L/K)}{\mathrm{Aut}(L/M)} \cong \mathrm{Aut}(M/K).$$

Demonstração. A aplicação está bem definida pelo item (iv) do Teorema 3.22. Além disso, ela é claramente um morfismo, visto que ela apenas restringe o domínio de cada automorfismo em $\mathrm{Aut}(L/K)$, o que não muda em nada a operação de composição.

Para ver que ela é sobrejetora, note que todo K-automorfismo σ de M pode ser estendido, pelo Corolário 2.75 a um K-automorfismo de L^{alg}, digamos σ', onde L^{alg} é algum fecho algébrico de L (portanto, também é um fecho algébrico de M).

Como L/K é normal, esse K-automorfismo σ' de L^{alg} induzirá um K-automorfismo $\tilde{\sigma}$ de L que estende σ, pelo item (v) do Teorema 3.22. Ou seja, todo K-automorfismo de M pode ser visto como a restrição de um K-automorfismo de L, portanto a aplicação é sobrejetora,

como queríamos.



Agora, para o isomorfismo, basta aplicar o Teorema do Isomorfismo para grupos, visto que a núcleo da aplicação $\sigma \mapsto \sigma|_M$ é composto, precisamente, pelos automorfismos de L que preservam M, ou seja, $\mathrm{Aut}(L/K)$.

□

3.3 EXTENSÕES GALOISIANAS E O TEOREMA FUNDAMENTAL

Até agora foi falado sobre as extensões e seus grupos de automorfismos, porém, não foi falado sobre como que esses grupos de automorfismos podem nos ajudar na investigação das propriedades das respectivas extensões de corpos. A parte que ainda não foi mencionada é que a estrutura de nosso grupo de automorfismos se reflete na estrutura de nossa extensão, e vice-versa, porém elas nem sempre são idênticas, isso não é verdade, porém, nas extensões galoisianas, onde há uma relação muito profunda entre seu grupo de automorfismos e a relação.

Falaremos um pouco sobre o caso geral antes, em extensões genéricas, a forma com que essa estrutura se reflete se dá da seguinte forma

Proposição 3.28. Seja L/K uma extensão de corpos e $\mathrm{Aut}(L/K)$ seu

grupo de automorfismos, então cada corpo intermediário $L \supseteq M \supseteq K$ está associado a um subgrupo de $\mathrm{Aut}(L/K)$, reciprocamente, cada subgrupo de $\mathrm{Aut}(L/K)$ é associado a um corpo intermediário da extensão L/K, de forma com que essas associações trocam a ordem entre corpos intermediários e subgrupos, ou seja, são aplicações decrescentes, do ponto de vista de conjuntos parcialmente ordenados.

Demonstração. Seja M um corpo intermediário de L/K, então podemos identificar esse corpo com um subgrupo de $\mathrm{Aut}(L/K)$ simplesmente fazendo a aplicação $M \mapsto \mathrm{Aut}(L/M)$ e, reciprocamente, podemos associar cada subgrupo $H \leq \mathrm{Aut}(L/K)$ a um corpo intermediário pela aplicação $H \mapsto L^H$, onde L^H denota o corpo dos elementos fixos sob os automorfismos H. É fácil ver que essas aplicações invertem a ordem, já que se $N \subseteq M$ são corpos intermediários de L/K, então, claramente, todo morfismo que fixa M também fixará N, ou seja, $\mathrm{Aut}(L/N) \geq \mathrm{Aut}(L/M)$. Do outro ponto de vista, se $K \leq H$ são subgrupos de $\mathrm{Aut}(L/K)$, todo elemento fixo pelos automorfismos em H também serão fixos pelos automorfismos em K, portanto $L^K \supseteq L^H$. □

O principal problema teórico de tais associações, entretanto, é que nem sempre elas são bem comportadas. A aplicação que associa corpos intermediários a subgrupos $M \mapsto \mathrm{Aut}(L/M)$ (na notação da proposição acima), por exemplo, geralmente falha em ser injetora.

Para ilustrar isso, considere a extensão $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Já foi visto no Exemplo 2.58 que ela tem grupo de automorfismo trivial. Ou seja, tal associação com certeza manda todos os corpos intermediários pro mesmo lugar.

Já a outra aplicação, que associa subgrupos do grupo de automorfismos até corpos intermediários, falha, geralmente, em ser sobrejetora, o mesmo exemplo pode ser usado.

As extensões galoisianas são precisamente as extensões que é possível fazer o estudo "bem comportado" dessas associações, que é o ponto central do Teorema Fundamental da Teoria de Galois. Começaremos então definindo essas extensões.

Definição 3.29. Uma extensão L/K é dita ser galoisiana, ou de Galois, se ela é normal e separável. Em extensões galoisianas, escrevemos $\mathrm{Gal}(L/K)$ ao invés de $\mathrm{Aut}(L/K)$ para indicar seu grupo de automorfismos.

Perceba que, se uma extensão L/K é galoisiana, e $K \subseteq M \subseteq L$ é um corpo intermediário, então L/M também será uma extensão galoisiana. De fato, a separabilidade de L/M está garantida pelo Teorema 3.14, e, como L/K é normal, L/M também deve ser.

Nesse trabalho nos atentaremos mais ao caso de extensões finitas, até porque o Teorema Fundamental, da forma que será apresentado, não será válido para o caso de extensões infinitas. Generalizaremos, porém, tudo o que for possível para o caso de extensões galoisianas infinitas.

O seguinte teorema nos auxiliará bastante no cálculo dos corpos fixos por grupos de automorfismos, que faremos mais a frente no Exemplo. Além disso, é um resultado necessário para a demonstração do Teorema Fundamental.

Proposição 3.30 (Truque das Órbitas)**.** Seja L/K uma extensão qualquer, $H \leq \mathrm{Aut}(L/K)$, $\theta \in L$, e $\Lambda = H \cdot \theta = \{\sigma(\theta) : \sigma \in H\}$ sua órbita. Então, dado que Λ é um conjunto finito, temos que

$$f(x) = \prod_{\beta \in \Lambda} (x - \beta) \in L^H[x].$$

Além disso, o polinômio minimal de θ divide $f(x)$.

Demonstração. Basta notar que qualquer elemento de H permuta Λ, logo os coeficientes de são fixos pelos automorfismos de H. □

Teorema 3.31. Seja L/K uma extensão finita de corpos, então as seguintes condições são equivalentes:

(i) L/K é galoisiana.

(ii) L é o corpo de raízes de algum polinômio separável $f(x) \in K[x]$.

(iii) $|\mathrm{Aut}(L/K)| = [L : K]$.

(iv) $L^{\mathrm{Aut}(L/K)} = K$.

Demonstração. (i) $\implies$ (ii). Pelo Teorema do Elemento Primitivo, existe $\theta \in L$ tal que $L = K(\theta)$. Assim, o polinômio minimal de θ será separável, e L pode ser considerado o seu corpo de raízes.

(ii) $\implies$ (i). L/K é normal, pois é o corpo de raízes de $f(x)$ (Teorema 3.22). Ademais, L é gerado pelas raízes de $f(x)$, que são separáveis sobre K, logo L é separável pelo Corolário 3.12.

(i) $\implies$ (iii). Existem exatamente $[L : K]$ imersões de L em K^{alg} pela separabilidade da extensão, e cada uma delas induz um K-automorfismo de L, pelo item (iii) do Teorema 3.22.

(iii) $\implies$ (iv). Suponha, por contrapositiva, que $L^{\mathrm{Aut}(L/K)} = K_0 \supsetneq K$, então, claramente, todo K-automorfismo de L é também um K_0-automorfismo, e vice-versa. Logo, $|\mathrm{Aut}(L/K)| = |\mathrm{Aut}_{K_0}(L)| \leq [L : K_0] < [L : K]$.

(iv) $\implies$ (i). Seja $\theta \in L$ um elemento qualquer, devemos mostrar que seu polinômio minimal, digamos $m(x)$, é separável, e se decompõe em lineares em L. Seja Λ a órbita de θ sobre $\mathrm{Aut}(L/K)$, assim, pelo Truque das Órbitas, temos que

$$f(x) = \prod_{\beta \in \Lambda} (x - \beta) \in L^{\mathrm{Aut}(L/K)}[x] = K[x]$$

onde $m(x) \mid f(x)$. Como $f(x)$ se fatora em lineares em $L[x]$, e é separável, segue que o mesmo é verdade para $m(x)$, e segue o resultado. □

Proposição 3.32. Seja LM/M um transporte pararelo de uma extensão L/K. Então, se L/K é galoisiana, LM/M também é. Além disso, $\mathrm{Gal}(LM/M)$ é isomorfo a um subgrupo de $\mathrm{Gal}(L/K)$.

Demonstração. Pelas Proposições 3.17 e 3.23, então LM/M é separável e normal, portanto é galoisiana.

Para a segunda parte, considere o morfismo $\mathrm{Gal}(LM/M) \to \mathrm{Gal}(L/K)$ dado por $\sigma \mapsto \sigma|_L$. Essa aplicação está bem definida, visto que qualquer morfismo σ preserva conjugados sobre M, que são também são conjugados sobre K. Logo, se $\theta \in L$, também temos que $\sigma(\theta) \in L$, pois L é fechado sobre K-conjugados por hipótese. A aplicação é, também, um morfismo, pois apenas restringe o domínio.

Por fim, para mostrar a injetividade, suponha que $\sigma|_L = \mathrm{id}$, com $\sigma \in \mathrm{Gal}(LM/M)$. Então, como σ preserva tanto M quanto L ponto a ponto, σ também preserva LM ponto a ponto. Assim, $\sigma = \mathrm{id}$ e, portanto, a aplicação é injetor, pois seu núcleo é composto apenas pela identidade. □

Estamos então prontos para demonstrar o principal teorema desse capítulo.

Teorema 3.33 (Teorema Fundamental da Teoria de Galois)**.** Seja L/K uma extensão galoisiana finita e $G = \mathrm{Gal}(L/K)$. Então,

(i) existe uma correspondência decrescente entre as extensões intermediárias $L \supseteq M \supseteq K$ e os subgrupos $H \leq G$, dada por

$$M \mapsto \mathrm{Gal}(L/M) \text{ ou } L^H \hookleftarrow H.$$

(ii) $[L^N : L^H] = [H : N]$ para $N \leq H \leq G$.

(iii) L^N/L^H é galoisiana $\iff$ $N \trianglelefteq H$, com $\mathrm{Gal}(L^N/L^H) \cong H/N$.

Demonstração. Vamos mostrar que a correspondência é bijetora mostrando que as composições

$$M \mapsto \mathrm{Gal}(L/M) \mapsto M^{\mathrm{Gal}(L/M)} \quad H \mapsto L^H \mapsto \mathrm{Gal}(L/L^H)$$

resultam na identidade, ou seja, que $M^{\mathrm{Gal}(L/M)} = M$, e $\mathrm{Gal}(L/L^H) = H$.

Para ver que $L^{\mathrm{Gal}(L/M)} = M$, perceba que, como a extensão L/K é galoisiana, a extensão L/M também será, como visto no Exemplo 3.21. Assim, a igualdade dos conjuntos segue diretamente pelo Teorema 3.31.

Vamos agora mostrar que $\mathrm{Gam}(L/L^H) = H$. Note que qualquer automorfismo em H certamente preserva L^H, visto que L^H denota precisamente o conjunto dos elementos de L que são preservados pelos automorfismos em H. Ou seja, $H \leq \mathrm{Gal}(L/L^H)$.

Perceba também que, como a extensão L/L^H deve ser finita, esses grupos também devem ser finitos. Assim, para mostrar a igualdade entre eles, basta mostrar que ambos tem a mesma cardinalidade.

Com efeito, como L/L^H também é galoisiana (mesmo argumento usado para L/M anteriormente), temos, pelo Teorema 3.31, que $[L : L^H] = |\mathrm{Gal}(L/L^H)|$. Além disso, como L/L^H é finita e separável, temos, pelo Teorema do Elemento Primitivo, que $L = L^H(\theta)$ para algum $\theta \in L$. Assim, pelo Truque das Órbitas, seu polinômio minimal $m(x)$ divide $f(x) = \prod_{\beta \in H \cdot \theta} (x - \beta)$. Ou seja,

$$|\mathrm{Gal}(L/L^H)| = [L : L^H] = \deg(m(x)) \leq \deg(f(x)) = |H \cdot \theta| \leq |H|.$$

Assim, a correspondência está provada.

Para provar que $[L^N : L^H] = [H : N]$, basta notar que

$$[L^N : L^H] = \frac{[L : L^H]}{[L : L^N]} = \frac{|\mathrm{Gal}(L/L^H)|}{|\mathrm{Gal}(L/L^N)|} = \frac{|H|}{|N|} = [H : N].$$

Por fim, vamos mostrar que L^N/L^H é galoisiana $\iff N \trianglelefteq H$. Se L^N/L^N é galoisiana, então, pelo Teorema 3.27, temos um morfismo sobrejetor $\mathrm{Gal}(L/L^H) \twoheadrightarrow \mathrm{Gal}(L^N/L^H)$, dada por $\sigma \mapsto \sigma|_{L^N}$. Além disso, o núcleo desse morfismo é $\mathrm{Gal}(L/L^N)$. Assim, como o núcleo de um morfismo de grupos é sempre um subgrupo normal do domínio, temos que $N = \mathrm{Gal}(L/L^N) \trianglelefteq \mathrm{Gal}(L/L^H) = H$.

Suponha, reciprocamente, que $N \trianglelefteq H$. Como L^N/L^H já é separável (é uma extensão intermediária de uma extensão separável), basta mostrar que também é normal. Para isso, considere $\theta \in L^N$ um elemento qualquer. Devemos, então, mostrar que todos os conjugados de θ sobre L^H também estão em L^N.

Como L/L^H é normal, temos, pela ação transitiva sobre conjugados (Teorema 3.26), que todos os conjugados de θ sobre L^H são da forma $h(\theta)$ para algum $h \in \mathrm{Gal}(L/L^H) = H$. Além disso, já que θ é fixo sobre a ação de N, e $h^{-1}nh \in N$ para qualquer $h \in H$ e $n \in N$, temos que

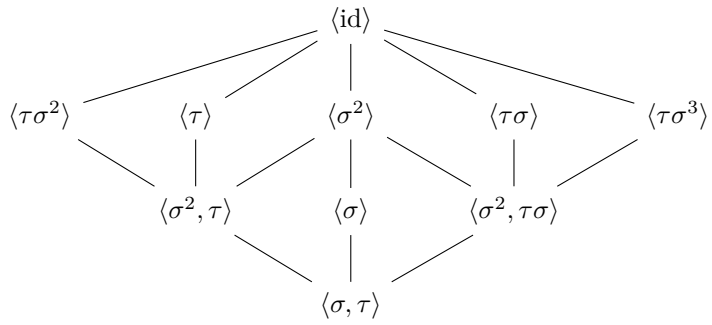
$$h^{-1}nh(\theta) = \theta \implies nh(\theta) = h(\theta).$$

Ou seja, todo conjugado de θ é fixo sobre os automorfismos de N e, portanto, pertencem a L^N. □

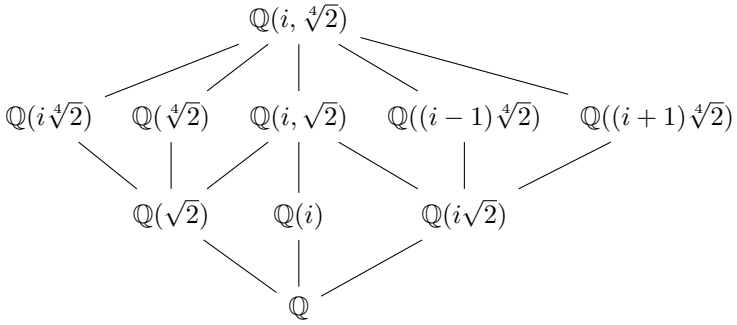
Vamos ilustrar o teorema com alguns exemplos.

Exemplo 3.34. Vimos, no Exemplo 3.24 que a extensão $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}$ é normal. Ela também é separável, pois a característica dos corpos é 0. Também, no Exemplo 2.70, visto que seu grupo de Galois é isomorfo a D_8, gerado por $\sigma : \sqrt[4]{2} \mapsto i\sqrt[4]{2}, i \mapsto i$ e $\tau : \sqrt[4]{2} \mapsto \sqrt[4]{2}, i \mapsto -i$. Dessa

forma, o reticulado de subgrupos de $\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q})$ é



onde τ e σ são definidos da mesma forma que no Exemplo 2.70. Perceba também que o índice de grupos consecutivos, no diagrama, é 2. Assim, pelo Teorema Fundamental da Teoria de Galois, tal extensão corresponde ao diagrama de subcorpos



onde cada uma das extensões tem grau 2.

É possível adivinhar grande parte desses corpos, se sabermos de antemão que eles são, de fato, extensões intermediárias. Por exemplo, sabemos que os corpos

$$\mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(i),\ \mathbb{Q}(i\sqrt{2}),\ \mathbb{Q}(i\sqrt[4]{2}),\ \mathbb{Q}(\sqrt[4]{2}),\ \mathbb{Q}(i, \sqrt{2})$$

são todos corpos intermediários da extensão $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}$, portanto devem corresponder a algum grupo do diagrama.

Para descobrir qual dos grupos que eles correspondem, basta encontrar o "maior" grupo (que se encontra o mais abaixo possível no diagrama de Hasse) que fixa seus geradores. Isso é uma tarefa fácil, porém exaustiva em natureza. Vamos fazer para cada um dos corpos mencionados.

Para $\mathbb{Q}(\sqrt{2})$, percebe-se que $\sqrt{2}$ é um ponto fixo de σ^2, visto que

$$\sigma^2(\sqrt{2}) = \sigma^2((\sqrt[4]{2})^2) = \sigma^2(\sqrt[4]{2})^2 = (-\sqrt[4]{2})^2 = \sqrt{2}.$$

É claro, também, que $\sqrt{2}$ é um ponto fixo de τ, visto que $\sqrt[4]{2}$ também é. Assim, $\mathbb{Q}(\sqrt{2})$. Entretanto, $\sqrt{2}$ não é um ponto fixo de σ, pois

$$\sigma(\sqrt{2}) = \sigma(\sqrt[4]{2})^2 = (i\sqrt[4]{2})^2 = -\sqrt{2} \neq \sqrt{2}.$$

Assim, $\mathbb{Q}(\sqrt{2})$ está contido no corpo $\mathbb{Q}(i, \sqrt[4]{2})^{\langle\sigma^2,\tau\rangle}$ e não está contido em $\mathbb{Q}(i, \sqrt[4]{2})^{\langle\sigma,\tau\rangle} = \mathbb{Q}$. Como não há um corpo intermediário entre esses corpos no diagrama, devemos ter que $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(i, \sqrt[4]{2})^{\langle\sigma^2,\tau\rangle}$.

Para $\mathbb{Q}(i)$, podemos perceber que i é fixo por σ, e $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. Logo, $\mathbb{Q}(i)$ deve corresponder ao grupo $\langle\sigma\rangle$. Similarmente, como $\mathbb{Q}(i\sqrt{2})$ também é uma extensão quadrática de $\mathbb{Q}$, ele deve corresponder a um dos subgrupos de ordem 4 doa diagrama. Como $\langle\sigma^2, \tau\rangle$ e $\langle\sigma\rangle$ já correspondem a outros corpos, a única opção restante é $\langle\sigma^2, \tau\sigma\rangle$.

Para $\mathbb{Q}(i, \sqrt{2})$, veja que ele é um subcorpo próprio de $\mathbb{Q}(i, \sqrt[4]{2})$ e contém os três corpos $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(i), \mathbb{Q}(i\sqrt{2})$. O único corpo, diferente de $\mathbb{Q}(i, \sqrt[4]{2})$, que pode conter esses três corpos simultaneamente, segundo o diagrama, é o corpo fixo por $\langle\sigma^2\rangle$. Logo, $\mathbb{Q}(i, \sqrt{2})$ corresponde a esse grupo.

É imediato ver que $\sqrt[4]{2}$ é fixo por τ, porém não é fixo por σ^2. Logo, $\mathbb{Q}(\sqrt[4]{2})$ está contido em $\mathbb{Q}(i, \sqrt[4]{2})^{\langle\tau\rangle}$ porém não está contido em $\mathbb{Q}(i, \sqrt[4]{2})^{\langle\sigma^2,\tau\rangle}$. Portanto, devemos ter que $\mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}(i, \sqrt[4]{2})^{\langle\tau\rangle}$.

O corpo $\mathbb{Q}(i\sqrt[4]{2})$ é uma extensão quadrática de $\mathbb{Q}(\sqrt{2})$ ($i\sqrt[4]{2}$ quando elevado ao quadrado é $-\sqrt{2}$), portanto, deve corresponde a

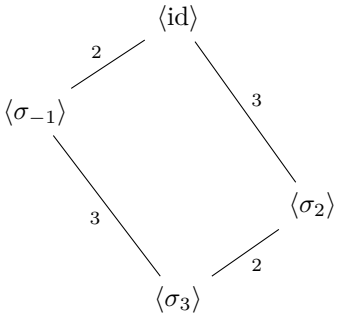
um dos grupos $\langle\tau\sigma^2\rangle, \langle\tau\rangle, \langle\sigma^2\rangle$. Porém, como o único grupo restante entre esses é $\langle\tau\sigma^2\rangle$, visto que os outros grupos já correspondem a outros corpos.

Os únicos corpos estranhos, nesse caso, são $\mathbb{Q}((i-1)\sqrt[4]{2})$ e $\mathbb{Q}((1+i)\sqrt{2})$, esses dois foram encontrados utilizando o Truque das Órbitas. A ideia é pegar um elemento que está em $\mathbb{Q}(i, \sqrt[4]{2})$, um bom candidato é $i\sqrt[4]{2}$, e descobrir sua órbita sobre algum dos grupos, aquele que se deseja encontrar o corpo correspondente.

Nesse caso, vamos pegar $\langle\tau\sigma\rangle$. A órbita de $i\sqrt[4]{2}$ sob a ação de $\langle\tau\sigma\rangle$ é $\{i\sqrt[4]{2}, -\sqrt[4]{2}\}$. Logo, pelo Truque das Órbitas, a soma desses elementos está em $\mathbb{Q}(i, \sqrt[4]{2})^{\langle\tau\sigma\rangle}$. Entretanto, essa some não está em $\mathbb{Q}(i, \sqrt[4]{2})^{\langle\sigma^2,\tau\sigma\rangle}$, pois não é fixo por σ^2, por exemplo. Além disso, como $i\sqrt{2} = -[(1-i)\sqrt[4]{2}]^2/2 \in \mathbb{Q}((1-i)\sqrt[4]{2})$, segue que $\mathbb{Q}(i, \sqrt[4]{2})^{\langle\tau\sigma\rangle} = \mathbb{Q}(i\sqrt{2}, (1-i)\sqrt[4]{2}) = \mathbb{Q}((1-i)\sqrt[4]{2})$.

A extensão $\mathbb{Q}((1+i)\sqrt[4]{2})$ é descoberta de forma análoga, utilizando a órbita de $i\sqrt[4]{2}$ sob o grupo $\langle\tau\sigma^3\rangle$.

Exemplo 3.35. A extensão $\mathbb{Q}(\zeta)/\mathbb{Q}$, onde $\zeta = e^{2\pi i/7}$, é galoisiana, já que é normal pelo Exemplo 3.24, e tem grupo de Galois isomorfo a $(\mathbb{Z}/7\mathbb{Z})^*$, dado pelos $\mathbb{Q}$-automorfismos σ_a onde $\sigma_a(\zeta) = \zeta^a$, pelo Exemplo 2.69. É fácil verificar que $(\mathbb{Z}/7\mathbb{Z})^*$ é cíclico, gerado por $\overline{3}$. Assim, é isomorfo a $\mathbb{Z}/6\mathbb{Z}$, e temos o reticulado de subgrupos



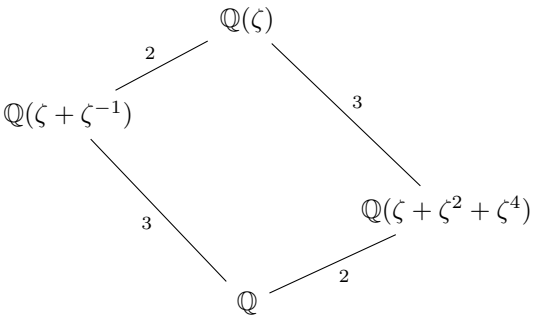
onde os números em cada aresta representam o grau dos subgrupos respectivos.

Para descobrir quais são os subcorpos correspondentes, podemos usar o Truque das Órbitas para descobrir os elementos primitivos de cada um dos corpos fixos. Tendo isso em mente, vamos descobrir a órbita de ζ pela ação dos grupos $\langle\sigma_{-1}\rangle$ e $\langle\sigma_2\rangle$. A órbita de ζ sobre $\langle\sigma_1\rangle$ é $\{\zeta, \zeta^{-1}\}$, somando esses valores, temos que $\zeta+\zeta^{-1} \in \mathbb{Q}(\zeta)^{\langle\sigma_{-1}\rangle}$, pelo Truque das Órbitas.

Além disso, perceba que $\zeta+\zeta^{-1}$ não é fixo sobre a ação de σ_3, já que $\sigma_3(\zeta+\zeta^{-1}) = \zeta^3+\zeta^{-3} = 2\cos(1080°/7) \neq 2\cos(360°/7) = \zeta+\zeta^{-1}$. Ou seja, $\zeta + \zeta^{-1} \notin \mathbb{Q}^{\langle\sigma_3\rangle} = \mathbb{Q}$. Isso prova que $\mathbb{Q}^{\langle\sigma_{-1}\rangle} = \mathbb{Q}(\zeta + \zeta^{-1})$.

Perceba também que a órbita de ζ sobre σ_2 é $\{\zeta, \zeta^2, \zeta^4\}$. Assim, novamente pelo Truque das Órbitas, $\zeta + \zeta^2 + \zeta^4 \in \mathbb{Q}^{\langle\sigma_2\rangle}$. Veja, entretanto, que esse elemento não é fixo sobre a ação de $\langle\sigma_3\rangle$, pois $\sigma_3(\zeta+\zeta^2+\zeta^4) = \zeta^3+\zeta^6+\zeta^5 \neq \zeta+\zeta^2+\zeta^4$. De fato, se esses elementos fossem iguais, $x^6 + x^5 - x^4 + x^3 - x^2 - x$ seria um polinômio que tem ζ como raiz. Entretanto, isso não pode ocorrer, pois ele não é um múltiplo de, $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, que é o polinômio minimal de ζ sobre $\mathbb{Q}$. Assim, podemos concluir que $\mathbb{Q}(\zeta)^{\langle\sigma_2\rangle} = \mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$.

Assim temos o diagrama de subcorpos correspondente, pelo Teorema Fundamental, dado por



Exemplo 3.36 (Teorema Fundamental do Cálculo)**.** Com as ferra-

mentas que desenvolvemos até agora, é possível mostrar que os complexos são algebricamente fechados. Para fazer isso, basta mostrar que qualquer polinômio de coeficientes reais e irredutível em $\mathbb{C}[x]$, digamos $f(x)$, deve necessariamente ter grau 1, pelo Teorema 2.47 e Lema 2.49. Para tal, vamos relembrar dois fatos importantes da análise:

(i) $\mathbb{C}$ não admite extensões de grau 2 (quadráticas), visto que é sempre possível extrair a raiz quadrada de elementos em $\mathbb{C}$.

(ii) $\mathbb{R}$ não admite extensões de grau ímpar, visto que o polinômio minimal de um elemento primitivo de qualquer extensão finita de $\mathbb{R}$ não pode ser um polinômio de grau ímpar, já que esses polinômios sempre tem raiz real pelo Teorema do Valor Intermediário.

Dessa forma, suponha por absurdo que $f(x) \in \mathbb{R}[x]$ é um polinômio irredutível em $\mathbb{C}[x]$ (logo seu grau é ≥ 4), e K seu corpo de raízes sobre $\mathbb{R}$. A extensão $K/\mathbb{R}$ é galoisiana (é automaticamente separável, por estarmos em um corpo de característica 0, e é normal pois é um corpo de raízes).

Seja, então, G seu grupo de Galois. Como a extensão é galoisiana, temos que $|G| = [K : \mathbb{R}] \geq 4$, e, como $\mathbb{R}$ não admite extensões de grau ímpar como previamente observado, $[K : \mathbb{R}]$ deve ser par.

Considere então, invocando o primeiro Teorema de Sylow, um 2-grupo $H \leq G$ de tal forma que $[G : H]$ é ímpar, pelo Teorema Fundamental da Teoria de Galois, esses grupos correspondem à cadeia $K^H \supseteq G^H = \mathbb{R}$. Perceba que, como $[G : H] = [K^H : \mathbb{R}]$, que é ímpar, devemos ter que $K^H = \mathbb{R} = K^G$, pois, novamente, $\mathbb{R}$ não admite extensões de grau ímpar. Isso, por sua vez, implica que $H = G$, já que a correspondência de Galois é biunívoca. Assim, $|G|$ é uma potência de 2 maior ou igual a 4.

Ou seja, existem $G \geq N_1 \geq N_2$, pelo Primeiro Teorema de Sylow, subgrupos onde $[G : N_1] = 2$ e $[N_1 : N_2] = 2$. Portanto, $[L^{N_1} : \mathbb{R}] = [L^{N_1} : L^G] = 2$, o que implica que $L^{N_1} \cong \mathbb{C}$, pelo Exemplo 2.66. Além disso, temos que $[L^{N_2} : \mathbb{C}] = [L^{N_2} : L^{N_1}] = 2$, mas isso é um absurdo, pois $\mathbb{C}$ não admite extensões quadráticas.

Logo, todo polinômio de $\mathbb{R}[x]$ que é irredutível em $\mathbb{C}[x]$ deve, necessariamente, ter grau 1 o que nos diz que $\mathbb{C}$ é algebricamente fechado.

Em geral, se o grupo de Galois de uma extensão possui algum nome especial, a extensão em si recebe o mesmo nome. Por exemplo, extensões galoisianas com grupo de Galois abeliano são chamadas de extensões abelianas. Similarmente, extensões com grupo de galoi solúvel são chamadas de extensões solúveis, e assim por diante.

4 EXTENSÕES CICLOTÔMICAS

Nesse capítulo, estudaremos as extensões ditas ciclotômicas, que tem uma grande importância no estudo das extensões abelianas (galoisianas com grupo de galois abeliano). De uma certa forma, são as extensões abelianas mais primordiais. Também, as propriedades dessas extensões nos permite desenvolver uma das aplicações iniciais mais interessantes da Teoria de Galois: a caracterização dos polígonos regulares construtíveis, que será vista no capítulo seguinte.

4.1 RAÍZES DA UNIDADE

Iniciamos essa seção com a definição do grupo de raízes da unidade, que terá papel central nesse capítulo.

Definição 4.1. Seja K um corpo, denotamos por $\mu_n(K)$ o conjunto das raízes n-ésimas da unidade de K. Em outras palavras, raízes do polinômio $x^n - 1 \in K[x]$.

Denotaremos, aqui, o grupo dos elementos inversíveis de um anel A, sob a operação de multiplicação, por A^x.

Proposição 4.2. $\mu_n(K)$ é um subgrupo de $K^\times$.

Demonstração. Ora, basta verificar que o produto de raízes n-ésimas da unidade é, também, uma raiz n-ésima da unidade, e que o inverso de uma raiz n-ésima também será uma raiz n-ésima.

O primeiro fato segue diretamente, pois se ω_1, ω_2 são n-ésimas raízes da unidade, então $(\omega_1\omega_2)^n = \omega_1^n\omega_2^n = 1$.

O inverso de uma raiz n-ésima também é uma raiz, visto que, para qualquer $\omega \in \mu_n(K)$, temos que

$$\omega\omega^{-1} = 1 \implies \omega^n(\omega^{-1})^n = 1 \implies (\omega^{-1})^n = 1 \implies \omega^{-1} \in \mu_n(K).$$

□

Definição 4.3. Seja K um corpo. Dizemos que um elemento $\zeta_n \in K$ é um raiz n-ésima primitiva da unidade se ele tem ordem n em $\mu_n(K)$.

Note que, nas condições da definição acima, ζ_n deve ser um gerador de $\mu_n(K)$.

Observação 4.4. Note que para que exista uma raiz n-ésima primitiva da unidade em um corpo K, é necessário que $\mu_n(K)$ tenha n elementos distintos, logo o polinômio $x^n - 1$ deve ser separável, que por sua vez implica que $\text{mdc}(x^n - 1, nx^{n-1}) = 1 \implies nx^{n-1} \neq 0 \implies \text{char}(K) \nmid n$. Portanto, toda vez que se assume a existência de uma raiz primitiva n-ésima $\zeta_n \in K$, também assume-se implicitamente que $\text{char}(K)$ não é um fator primo de n, pois, caso contrário, teríamos um absurdo.

Teorema 4.5. Sejam K um corpo, ζ_n uma raiz n-ésima primitiva da unidade em K e ω uma raiz n-ésima da unidade. Então,

ω é primitiva n-ésima $\iff$ $\omega = \zeta_n^k$ para algum k com $\text{mdc}(n, k) = 1$.

Demonstração. ($\implies$). Faremos por contrapositiva. Suponha que $\omega = \zeta_n^k$ onde $\text{mdc}(n, k) = d > 1$, nesse caso, a ordem de ω é no máximo $n/d < n$, já que $\omega^{n/d} = (\zeta_n^n)^{k/d} = 1$, portanto, ω não é uma raiz primitiva n-ésima

($\impliedby$). Basta notar que

$$(\zeta_n^k)^m = 1 \iff n \mid mk \iff n \mid m$$

já que n e k são relativamente primos. Logo, a menor de suas potências positivas que resultam em 1 é precisamente n. □

Como consequência direta, temos o seguinte corolário.

Corolário 4.6. Em um corpo K, ou existem exatamente $\varphi(n)$ raízes n-ésimas primitivas da unidade, ou não existem nenhuma.

Lema 4.7. Seja $n \in \mathbb{N}$ um natural qualquer. Então, $\sum_{d|n} \varphi(d) = n$, onde φ é a função totiente de Euler.

Demonstração. Considere o grupo $\mu_n(\mathbb{C})$. Para cada divisor d de n, há uma raiz primitiva da unidade d-ésima, dada por $e^{2\pi i/d}$. Ou seja, pelo corolário anterior, há precisamente $\varphi(d)$ elementos de ordem d em $\mu_n(\mathbb{C})$ se d é um divisor de n. Também, caso d não divida n, não haverá elementos de ordem d, pelo Teorema de Lagrange. Ou seja, se contarmos a quantidade de elementos pela ordem de cada, temos que $|\mu_n(\mathbb{C})| = \sum_{d|n} \varphi(d)$.

Por outro lado, sabemos que $\mathbb{C}$ é algebricamente fechado, portanto contém todas as raízes do polinômio $x^n - 1$. Esse polinômio é separável, pois $\text{mdc}(x^n - 1, nx^{n-1}) = 1$. Então, necessariamente, $|\mu_n(\mathbb{C})| = n$, e o resultado segue diretamente. □

Teorema 4.8. Em um corpo K, todo subgrupo finito de $K^\times$ é cíclico.

Demonstração. Seja $G \leq K^\times$ um subgrupo finito qualquer de ordem n. Então, pelo Teorema de Lagrange, todo elemento de G é uma raiz n-ésima da unidade. Suponha, por absurdo, que G não é cíclico, ou seja, que não tem elementos de ordem n. Então, contando a quantidade de elementos de G pela ordem de cada um, teríamos, pelo resultado anterior, que

$$|G| \leq \sum_{\substack{d|n \\ d \neq n}} \varphi(d) < \sum_{d|n} \varphi(d) = n.$$

Isso é um absurdo, pois temos que $|G| = n$ por hipótese. □

Utilizando esse teorema, podemos demonstrar o teorema do elemento primivo no caso finito.

Corolário 4.9 (Teorema do Elemento Primitivo - Caso Finito)**.** Toda extensão L/K onde L é finito, é, também, simples.

Demonstração. Perceba que $L^\times$ é um subgrupo multiplicativo finito de L e, pelo teorema anterior, é gerado por um elemento $\theta \in L$. Segue, então, que $L = K(\theta)$ □

Teorema 4.10. Seja n um inteiro e K um corpo onde $\text{char}(K)$ não divide n. Então, existe uma extensão de K que contém uma raiz n-ésima primitiva da unidade.

Demonstração. Basta considerar o corpo de raízes do polinômio $x^n - 1$ sobre K, tal polinômio é claramente separável pelo critério da derivada, assim todas as n-ésimas raízes da unidade devem ser distintas em L, isso necessariamente implica que temos uma raiz de ordem n, caso contrário não teríamos raízes suficientes, pelo mesmo raciocínio da demonstração anterior. □

Proposição 4.11. Seja L/K uma extensão algébrica, e $\zeta_n \in L$ uma raiz primitiva n-ésima da unidade. Então, os conjugados de ζ_n sobre K devem também ser raízes primitivas n-ésimas da unidade.

Demonstração. Seja $\alpha \in L$ um conjugado de ζ_n sobre K. Pelo Lema Fundamental, deve existir uma imersão de $K(\zeta_n)$ até L onde $\sigma(\zeta_n) = \alpha$. Como ζ_n é uma raiz de $x^n - 1$, $\sigma(\zeta_n) = \alpha$ também deve ser. Além, como $\sigma(\zeta_n)^k = \sigma(\zeta_n^k) \neq 1$ se $1 \leq k < n$ (lembre que σ é injetora), devemos ter que $\alpha^k \neq 1$ para qualquer $k \in \{1, \ldots, n-1\}$. Portanto, α também é uma raiz primitiva n-ésima da unidade. □

4.2 EXTENSÕES CICLOTÔMICAS

Definição 4.12. Uma extensão da forma $K(\zeta_n)/K$, onde ζ_n é uma raiz primitiva n-ésima da unidade, é dita ser uma extensão ciclotômica.

Proposição 4.13. Um corpo K admite uma extensão ciclotômica se, e somente se, $\mathrm{char}(K)$ não divide n.

Demonstração. A ida segue da Observação 4.4, e a volta do Teorema 4.10. □

Observação 4.14. A partir desse momento, toda vez que fizermos menção a uma extensão ciclotômica $K(\zeta_n)/K$, assume-se implicitamente que a característica do corpo K não é um fator de n.

Proposição 4.15. Sejam L/K uma extensão de corpos e $\zeta_n, \zeta_n' \in L$ raízes primitivas n-ésimas da unidade, então $K(\zeta_n) = K(\zeta_n')$. Ou seja, a extensão ciclotômica independe da escolha de raiz primitiva.

Demonstração. Basta observar que qualquer raiz primitiva n-ésima da unidade deve gerar as outras raízes primitivas n-ésimas da unidade, portanto $\zeta_n \in K(\zeta_n')$ e $\zeta_n' \in K(\zeta_n)$, e o resultado segue diretamente pelas definições de $K(\zeta_n)$ e $K(\zeta_n')$. □

Teorema 4.16. Toda extensão ciclotômica $K(\zeta_n)/K$ é galoisiana, com grupo de Galois isomorfo a algum subgrupo de $(\mathbb{Z}_n)^\times$.

Demonstração. Como $\mathrm{char}(K)$ não divide n, o polinômio $x^n - 1$ é separável, e $K(\zeta_n)$ é o corpo de raízes desse polinômio sobre K (já que ζ_n gera todas as outras raízes de $x^n - 1$).

Vamos agora mostrar que a aplicação dada por $(\zeta_n \mapsto \zeta_n^a) \mapsto a \pmod n$ é um morfismo injetor de $\mathrm{Gal}(K(\zeta_n)/K)$ até $(\mathbb{Z}_n)^\times$.

O fato de que a aplicação é bem definida segue de (4.5) e (4.11), já que $a \pmod n$ será de fato inversível em $\mathbb{Z}_n$ pois a deve ser relativamente primo a n, portanto, inversível em $\mathbb{Z}_n$. É fácil checar que a aplicação é um homomorfismo.

Resta mostrar que a aplicação é injetora. Suponha que $a \pmod n = 1 \pmod n$, assim devemos ter que $a = qn + 1$ para algum $q \in \mathbb{Z}$, e,

portanto, $\zeta_n^a = \zeta_n^{qn+1} = (\zeta_n^n)^k \zeta_n = \zeta_n$, assim, a aplicação $(\zeta_n \mapsto \zeta_n^a)$ se reduz à aplicação identidade. □

Corolário 4.17. Toda extensão ciclotômica é abeliana.

Proposição 4.18. Seja L/K uma extensão e $\zeta_m, \zeta_n, \zeta_{mn} \in L$ raízes primitivas da unidade, com $\text{mdc}(m,n) = 1$, então $K(\zeta_m, \zeta_n) = K(\zeta_{mn})$.

Demonstração. Perceba que ζ_n, ζ_m são também raízes mn-ésimas da unidade, logo $\zeta_n, \zeta_m \in K(\zeta_{mn}) \implies K(\zeta_n, \zeta_m) = K(\zeta_n)K(\zeta_m) \subseteq K(\zeta_{nm})$. Para mostrar a recíproca, perceba que $\zeta_n\zeta_m$ tem ordem igual a $\text{mmc}(m,n) = mn$ (já que eles são relativamente primos), logo é uma raiz mn-ésima primitiva da unidade, assim $\zeta_{mn} \in K(\zeta_n, \zeta_m) = K(\zeta_n)K(\zeta_m)$ (pois $\zeta_m\zeta_n$ gerará ζ_{mn} por ser primitiva). □

4.3 POLINÔMIOS CICLOTÔMICOS

Definição 4.19. Seja $\mathcal{P}_n$ o conjunto de raízes n-ésimas primitivas da unidade em $\mathbb{C}$. O polinômio $\prod_{\zeta \in \mathcal{P}_n} (x - \zeta) \in \mathbb{C}[x]$ é dito ser o n-ésimo polinômio ciclotômico, denotado por $\Phi_n(x)$.

Proposição 4.20. Seja $n \in \mathbb{N}$ um natural qualquer. Então, $\prod_{d|n} \Phi_d(x) = x^n - 1$.

Demonstração. Ora, basta organizar os fatores de $x^n - 1$ a partir de seus mdc's com n, da seguinte forma:

$$x^n - 1 = \prod_{i=1}^{n} (x - \zeta_n^i) = \prod_{d|n} \left(\prod_{\substack{\text{mdc(k,n)= d} \\ 1 \leq k \leq n}} (x - \zeta_n^k) \right) = \prod_{d|n} \Phi_d(x).$$

□

Proposição 4.21. O n-ésimo polinômio ciclotômico $\Phi_n(x)$ tem coeficientes inteiros, para qualquer $n \in \mathbb{N}$.

Demonstração. Demonstraremos por indução forte em n. Temos que $\Phi_1(x) = x - 1$, logo o resultado é válido para $n = 1$. Suponha, agora, que o resultado seja verdadeiro para todo $d < n$. Pela identidade $\left(\prod_{\substack{d|n \\ d \neq n}} \Phi_d(x) \right) \Phi_n(x) = x^n - 1$, e pelo fato de que $\prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)$ é mônico, segue que $\Phi_n(x) \in \mathbb{Z}[x]$ pelo algoritmo da divisão. □

O seguinte significa que todo polinômio ciclotômico é palíndromo, isto é, seus coeficientes, quando lidos de trás pra frente, resultam na mesma sequência de quando lidos normalmente.

Proposição 4.22. Para qualquer polinômio ciclotômico $\Phi_n(x)$, temos que $\Phi_n(x) = x^{\varphi(n)} \Phi_n(x^{-1})$.

Demonstração. Seja ζ_n uma raiz de $\Phi_n(x)$. Como ζ_n^{-1} também é uma raiz n-ésima primitiva da unidade, ela também é uma raiz de $\Phi_n(x)$. Assim, $\Phi_n(x)$ e $x^{\varphi(n)} \Phi_n(x^{-1})$ são ambos polinômios de grau $\varphi(n)$ que compartilham as mesmas raízes, e como $x^{\varphi(n)} \Phi_n(x)$ é mônico (pois o último coeficiente de $\Phi(x)$ é 1), segue que eles devem ser iguais. □

Teorema 4.23. $\Phi_n(x)$ é irredutível em $\mathbb{Q}[x]$.

Demonstração. Seja $\zeta_n \in \mathbb{C}$ uma raiz primitiva n-ésima qualquer da unidade, e $f(x) \in \mathbb{Z}[x]$ o fator irredutível, no DFU $\mathbb{Z}[x]$, de $\Phi_n(x)$ onde $f(\zeta_n) = 0$. Note que, nessas condições, $f(x)$ é necessariamente mônico, pois $\Phi_n(x)$ também é. Assim, existe $g(x) \in \mathbb{Z}[x]$ não nulo e também mônico onde $\Phi_n(x) = f(x)g(x)$. Perceba também que $g(\zeta_n) \neq 0$, pois $\Phi_n(x)$ é separável.

Queremos mostrar que os restantes das raízes primitivas (ou seja, os números ζ_n^a onde $\text{mdc}(a, n) = 1$) são também raízes de $f(x)$, o

que implicaria que $f(x) = \Phi_n(x)$. Assim, como $\Phi(x)$ é tem coeficientes relativamente primos (pois é mônico), a sua irredutibilidade em $\mathbb{Z}[x]$ implicará na irredutibilidade em $\mathbb{Q}[x]$.

Para isso, considere um primo p onde p não divide n. Dessa forma, ζ_n^p é uma raiz primitiva n-ésima da unidade, portanto $\Phi_n(\zeta_n^p) = 0$. Isso, por sua vez, implica que, ou $f(\zeta_n^p) = 0$, ou $g(\zeta_n^p) = 0$. Queremos mostrar que o segunda caso não pode ocorrer.

Então suponha, por absurdo, que $g(\zeta_n^p) = 0$. Assim, como $f(x)$ é o polinômio minimal de ζ_n, temos que $f(x)|g(x^p)$. Ou seja, existe $h(x) \in \mathbb{Z}[x]$ tal que $f(x)h(x) = g(x^p)$.

Reduzindo essa equação módulo p, temos que $\overline{f}(x)\overline{h}(x) = \overline{g}(x^p) = (\overline{g}(x))^p$ em $(\mathbb{Z}/p\mathbb{Z})[x]$ (já que expoentes múltiplos de p se distribuem sobre a soma em corpos de característica p). Como $(\mathbb{Z}/p\mathbb{Z})[x]$ é um DFU (pois é um domínio euclidiano) e $\overline{f}(x)$ é definitivamente não constante (por ser mônico), todo fator primo de $\overline{f}(x)$ deve aparecer na fatoração de $\overline{g}(x)$ ao menos uma vez.

Assim, $\overline{f}(x)$ e $\overline{g}(x)$ tem um divisor comum, digamos $k(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$. Logo existem $m_1(x), m_2(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ onde $\overline{f}(x) = m_1(x)k(x)$ e $g(x) = m_2(x)k(x)$. Portanto, $x^n - 1 = k(x)m_1(x)k(x)m_2(x)$ em $(\mathbb{Z}/p\mathbb{Z})[x]$. Mas isso é um absurdo, pois $x^n - 1$ é separável em $(\mathbb{Z}/p\mathbb{Z})[x]$, logo não poderia ter fatores repetidos de $k(x)$.

Ou seja, se p é um primo que não divide n, devemos ter que $f(\zeta_n^p) = 0$. Para o caso geral, onde a é um número relativamente primo a n qualquer, considere a fatoração prima de a, digamos $p_1 \cdots p_m$ (primos não necessariamente distintos). Como a é relativamente primo a n por hipótese, nenhum dos fatores primos p_i dividem n, assim temos,

indutivamente, que

$$\begin{aligned} f(\zeta_n) = 0 &\implies f(\zeta_n^{p_1}) = 0 \\ &\implies f(\zeta_n^{p_1 p_2}) = 0 \\ &\implies \vdots \\ &\implies f(\zeta_n^{p_1 \cdots p_m}) = f(\zeta_n^a) = 0, \end{aligned}$$

como queríamos. E isso prova o teorema. □

Corolário 4.24. Temos que:

(i) $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$,

(ii) $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}_n)^\times$,

(iii) $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$ se $\mathrm{mdc}(n, m) = 1$.

Demonstração. (i) Como o polinômio ciclotômico Φ é irredutível em $\mathbb{Q}[x]$, ele é o polinômio minimal de ζ sobre $\mathbb{Q}$, assim, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(\Phi_n(x)) = \varphi(n)$.

(ii) Sabemos, pelo Teorema 4.16, que o grupo de Galois da extensão $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ é isomorfo a algum subgrupo de $(\mathbb{Z}/n\mathbb{Z})^\times$, além disso, temos que $|\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = |\mathbb{Z}/n\mathbb{Z}|$, mas isso só pode ocorrer se $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}$.

(iii) Como $[\mathbb{Q}(\zeta_n, \zeta_m)/\mathbb{Q}] = \varphi(nm) = \varphi(n)\varphi(m) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}][\mathbb{Q}(\zeta_n) : \mathbb{Q}]$, o resultado segue do Teorema 2.38. □

Não podemos finalizar o estudo das extensões ciclotômicas dos racionais sem fazer uma menção a um dos resultados mais fundamentais sobre ela: o Teorema de Kronecker-Weber. Esse teorema nos diz que toda extensão abeliana de $\mathbb{Q}$ está contida em alguma extensão ciclotômica de $\mathbb{Q}$.

Isso que justifica a fala, no início do capítulo, que afirma que as extensões ciclotômicas são as extensões abelianas mais fundamentais que tem, ao menos no caso racional.

A demonstração desse teorema utiliza ferramentas significantemente mais avançadas do que as que desenvolvemos até agora, por isso apenas enunciaremos esse teorema, sem demonstração.

Teorema 4.25 (Teorema de Kronecke-Weber)**.** Seja $K/\mathbb{Q}$ uma extensão abeliana. Então, para algum $n \in \mathbb{N}$, temos que $K \subseteq \mathbb{Q}(\zeta_n)$

O teorema não é, em geral, necessariamente verdade quando o corpo base da extensão não é $\mathbb{Q}$.

5 CONSTRUÇÕES COM RÉGUA E COMPASSO

5.1 PONTOS E NÚMEROS CONSTRUTÍVEIS

Nesta seção abordaremos uma aplicação clássica da Teoria de Galois, a classificação dos números, ângulos, e polígonos regulares construtíveis por régua e compasso no plano euclidiano, que tem uma profunda e surpreendente relação com os primos de Fermat.

Identificaremos o plano com $\mathbb{R}^2$, munido com a métrica euclidiana usual, e postulamos as seguintes construções possíveis com régua e compasso:

(i) Dados pontos $A = (x_1, y_1)$ e $B = (x_2, y_2)$, é possível traçar a reta $r(A, B) = \{(x, y) \in \mathbb{R}^2 : (y_1 - y_2)(x - x_1) - (x_1 - x_2)(y - y_1) = 0\}$.

(ii) Dado um ponto $O = (h, k)$ e dois pontos A, B que tem distância r entre eles, podemos traçar a circunferência de raio r centrada em O, $c(O, r) = \{(x, y) \in \mathbb{R}^2 : (x - h)^2 + (y - k)^2 = r^2\}$.

Observação 5.1. Perceba que, por meio de manipulações algébricas triviais, pode-se observar que equações que definem esses conjuntos apresentam coeficientes que dependem apenas das coordenadas dos pontos A, B e O, ou seja, estão no corpo gerado pelas suas coordenadas.

Dadas essas ferramentas, investigaremos o que é possível construir no plano a partir de um segmento unitário dado. Vamos supor, sem perda de generalidade, que tal segmento unitário tem extremidades nos pontos $(0, 0)$ e $(1, 0)$. Para tornar essa noção de construtibilidade mais precisa, utilizaremos a seguinte definição recursiva.

Definição 5.2. Um ponto $P \in \mathbb{R}^2$ é dito ser construtível se

- $P = (0, 0)$ ou $P = (1, 0)$,

- P é a intersecção de retas e circunferências, traçadas a partir de pontos construtíveis.

Definimos também os números construtíveis,

Definição 5.3. Um número $\alpha \in \mathbb{R}$ é dito ser construtível se existe um segmento com extremidades construtíveis de comprimento $|\alpha|$, ou seja, se existem $A, B \in \mathbb{R}^2$ construtíveis tal que $d(A, B) = |\alpha|$.

O seguinte teorema nos diz que a noção de construtibilidade para números e pontos em $\mathbb{R}^2$ são, de certa forma, equivalentes.

Proposição 5.4. Um ponto $(\alpha, \beta) \in \mathbb{R}^2$ é construtível se, e somente se, α, β são números construtíveis.

Demonstração. ($\Longrightarrow$) Basta descer a perpendicular ao eixo x, que é claramente construtível, que passa por (α, β), assim a intersecção dessa perpendicular com o eixo x será $(\alpha, 0)$, e temos que $d(O, (\alpha, 0)) = \alpha$ e $d((\alpha, 0), (\alpha, \beta)) = \beta$, onde O é a origem, logo α e β são números construtíveis.

($\Longleftarrow$) Trace a circunferência de raio $|\alpha|$ centrada na origem, um dos pontos em que essa circunferência interseccionará o eixo x é no ponto $(\alpha, 0)$, a partir daí, trace a perpendicular r ao eixo x que passa por $(\alpha, 0)$, e trace uma circunferência de raio $|\beta|$ com centro em $(\alpha, 0)$, essa circunferência interseccionará a reta r em dois pontos, um deles é ponto desejado (α, β). □

Teorema 5.5. Se $\alpha, \beta \in \mathbb{R}$ são números construtíveis, então $\alpha \pm \beta$, $\alpha\beta$, α/β $(y \neq 0)$ e $\sqrt{|\alpha|}$ também são, assim, os números construtíveis formam um subcorpo de $\mathbb{R}$, que não admite extensões quadráticas reais.

Demonstração. Vamos supor, sem perda de generalidade, que $\alpha > \beta > 0$. Se α e β são números construtíveis, então existem pontos

construtíveis $A_1, A_2, B_1, B_2 \in \mathbb{R}^2$ onde $d(A_1, A_2) = \alpha$ e $d(B_1, B_2) = \beta$. Para criar um segmento construtível de medida $\alpha \pm \beta$, basta construir uma circunferência de raio β centrada em A_2. Essa circunferência terá intersecção com a reta $r(A_1, A_2)$ em dois pontos, digamos C_1, C_2. Assim, teremos que o segmento A_1C_1 tem medida $\alpha + \beta$, e o segmento A_1C_2 tem medida $\alpha - \beta$.

Para criar um segmento de medida $\alpha\beta$, considere os pontos construtíveis $(1, 0)$, $(0, \alpha)$ e $(\beta, 0)$, pela Proposição 5.4. A partir desses pontos, construa uma reta paralela à reta $r((1, 0), (0, \alpha))$ que passa pelo ponto $(\beta, 0)$. Essa reta interseccionará o eixo y em um ponto C. Com alguns cálculos básicos de semelhança de triângulos, é possível descobrir que $C = (0, \alpha\beta)$, e, portanto, $\alpha\beta$ é um número construtível pela Proposição 5.4.

O mesmo raciocínio é usado para criar um segmento de medida α/β, onde podemos considerar os pontos construtíveis $(1, 0)$, $(0, \alpha)$ e $(\beta, 0)$ e construir a reta paralela à reta $r((0, \alpha), (\beta, 0))$ que passa por $(1, 0)$. Assim essa reta interseccionará o eixo y no ponto $(0, \alpha/\beta)$ que, de novo, é facilmente verificável com alguns cálculos básicos envolvendo semelhança de triângulo, assim α/β também será construtível.

Por fim, para criar um segmento de medida $\sqrt{\alpha}$, considere os pontos construtíveis $A = (-1, 0)$ e $B = (0, \alpha)$. Trace a circunferência cujo centro é o ponto médio entre esses dois pontos, e o raio é a metade da distância entre esses pontos (lembre que é sempre possíel construir o ponto médio enre dois pontos). Essa circunferência terá uma intersecção com o eixo y. Afirmamos que essa intersecção se dá no ponto $C = (0, \sqrt{\alpha})$ e, portanto, $\sqrt{\alpha}$ será construtível.

De fato, pelo Teorema do Ângulo Inscrito, o ângulo $\angle ACB$ é um ângulo reto. Daí, é fácil ver que os triângulos AOC e COB são semelhantes, portanto,

$$|OC|/1 = \alpha/|OC| \implies |OC| = \sqrt{\alpha},$$

o que completa a demonstração. □

Lema 5.6. Sejam

- $P_1, \ldots, P_n$ pontos construtíveis.
- K o corpo gerado pelas coordenadas desses pontos.
- $Q = (h, k)$ um ponto construido a partir dos pontos P_i.
- L a extensão de K gerada pelas coordenadas de Q.

Nessas condições, temos que $[L : K] \leq 2$.

Demonstração. Como Q é um ponto construtível a partir dos pontos P_i, existem 3 possibilidades:

(i) Q é a intersecção entre duas retas.

(ii) Q é a intersecção entre uma reta e uma circunferência.

(iii) Q é a intersecção entre duas circunferências.

No caso (i), Q é a solução de um sistema linear da forma

$$\begin{cases} a_1x + b_1y = c_1 \\ a_2x + b_2y = c_2, \end{cases}$$

onde as equação são linearmente independentes (já que são retas definitivamente não paralelas) com coeficientes em K (pela Observação 5.1). Como a solução de um sistema linear determinado sempre pertence ao corpo dos coeficientes (basta fazer a eliminação gaussiana), segue que $L = K$. Portanto, $[L : K] = 1$.

Em (ii), Q é a solução de um sistema não-linear da forma

$$\begin{cases} x^2 + y^2 + a_1x + b_1y = c_1 \\ a_2x + b_2y = c_2, \end{cases}$$

onde a primeira equação representa a circunferência, e a segunda a reta. Novamente, todos os coeficientes estão em K, com $(a_2, b_2) \neq (0, 0)$. Aqui, podemos isolar uma das variáveis da segunda equação, desde que seja não nula. Digamos que tal coeficiente é a_2. Assim, obtemos que $x = (c_2 - b_2 y)/a_2$.

Substituindo x na primeira equação, obtemos uma equação de segundo grau em y, cuja solução, digamos k, está no próprio corpo K, ou em uma extensão quadrática de K. De fato, para obter a solução de uma equação de segundo grau devemos, no máximo, extrair uma raiz quadrada. Como $h = (c_2 - b_2 k)/a_2$, h também está nesse corpo, segue que $[L : K] \leq 2$, como queríamos.

No caso (iii), Q é a solução de um sistema da forma

$$\begin{cases} x^2 + y^2 + a_1 x + b_1 y = c_1 \\ x^2 + y^2 + a_2 x + b_2 y = c_2 \end{cases}$$

Subtraindo a segunda primeira equação da segunda, obtemos um sistema equivalente, com estrutura igual ao sistema do item (ii), logo segue o resultado. □

Teorema 5.7. Um número $\alpha \in \mathbb{R}$ é construtível se, e somente se, existe uma cadeia de extensões quadráticas reais

$$K_s \supseteq \cdots \supseteq K_1 \supseteq K_0 = \mathbb{Q}$$

onde $\alpha \in K_s$.

Demonstração. ($\Longrightarrow$) Seja $\alpha \in \mathbb{R}$ um número construtível $P_1, \cdots, P_n \in \mathbb{R}^2$ os pontos cuja construção é necessária para criar um segmento de tamanho $|\alpha|$ com extremidades P, Q. Considere, então, a cadeia de extensões

$$K_n \supseteq \cdots \supseteq K_1 \supseteq K_0 = \mathbb{Q},$$

onde K_i é obtido ao fazer a adjunção das coordanas de P_i ao corpo K_{i-1}, onde $i \in \{1, \ldots, n\}$. Pelo Lema 5.6 cada uma dessas extensões ou é trivial, ou é quadrática, e as coordenadas de P e Q estão em K_n. Assim, para obter um corpo que contém α, basta fazer a adjunção, se necessário, de $|\alpha| = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2}$, onde $P = (p_1, p_2)$ e $Q = (q_1, q_2)$. Ou seja, α está contido no último corpo da cadeia de extensões quadráticas, ou triviais, a seguir

$$K_n(|\alpha|) \supseteq K_n \supseteq \cdots \supseteq K_1 \supseteq K_0 = \mathbb{Q},$$

Desconsiderando as extensões triviais nessa cadeia, o resultado segue. ($\Longleftarrow$) Como os números construtíveis são fechados por raízes quadradas reais, como mostra o Teorema 5.5, essas extensões devem todas ser compostas de números construtíveis. □

Corolário 5.8. Se $\alpha \in \mathbb{R}$ é um número construtível, então $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ é necessariamente uma potência de 2.

Demonstração. Seja K_s o corpo descrito no enunciado do Teorema 5.7. Basta, então, notar que $[\mathbb{Q}(\alpha) : \mathbb{Q}] \mid [K_s : \mathbb{Q}] = 2^s$, logo $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ pode conter apenas fatores de 2 como fatores primos. □

Exemplo 5.9. O número $\sqrt[3]{2}$ não é construtível, visto que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg(x^3 - 2) = 3$. Isso nos diz que o clássico problema da duplicação do cubo é impossível de ser realizado com régua e compasso, visto que criar um cubo com o dobro do volume de um cubo dado equivale a construir um segmento de medida $\sqrt[3]{2}$ vezes maior.

5.2 POLÍGONOS E ÂNGULOS CONSTRUTÍVEIS

Definição 5.10. Dizemos que um âgulo de medida θ é construtível se existem 3 pontos construtíveis, digamos A, B, O, onde a medida do ângulo $\angle AOB$ é θ.

Perceba, entretanto, que a medida do ângulo não é única, sendo consideradas "iguais" se diferem por um múltiplo de 2π. Ou seja, se o ângulo de medida θ é construtível, o ângulo de medida $\theta + 2k\pi$ também é, para qualquer $k \in \mathbb{Z}$.

Proposição 5.11. Se θ_1, θ_2 são as medidas de dois ângulos construtíveis. Então, o ângulo de medida $\theta_1 + \theta_2$ também é.

Demonstração. Basta transportar o ângulo de medida θ_1 de foma que ele seja consecutivo com o ângulo de medida θ_2, assim o ângulo resultante terá medida $\theta_1 + \theta_2$. □

Corolário 5.12. Qualquer combinação $\mathbb{Z}$-linear de medidas de ângulos construtíveis é, também, uma medida de um ângulo construtível.

Teorema 5.13. Um ângulo de medida $\theta \in \mathbb{R}$ é construtível se, e somente se, $\cos(\theta)$ é um número construtível.

Demonstração. ($\implies$) Seja AOB um ângulo de medida θ, e trace uma circunferência c de raio unitário com centro em O. Suponha, sem perda de generalidade, que B está na intersecção da reta OB e a circunferência c, daí, basta descer a perpendicular partindo de B até a reta OC, digamos que a intersecção é no ponto C', daí o segmento OC' claramente terá medida igual a $cos(\theta)$, portanto, é um número construtível.

($\impliedby$) Vamos supor aqui, sem perda de generalidade, que $\theta \in [0\pi/2]$. Sejam O e A as extremidades (construtíveis) do segmento de medida $\cos(\theta)$, trace a reta r perpendicular ao segmento OA que passa por A, e a circunferência unitária centrada em O, e seja B a intersecção entre a circunferência r e a reta r, nesse caso, é claro ver que o ângulo $\angle AOB$ tem medida θ. Para os ângulos de medida fora do intervalo $[0, \pi/2]$, basta repetir o mesmo processo, porém colocando o ângulo de medida $|\cos(\theta)|$ na direção apropriada. □

Para o próximo teorema, relembre que um primo p é chamado de primo de Fermat se existe algum $n \in \mathbb{N}$ onde $p = 2^{2^n} + 1$. Os únicos primos de Fermat conhecidos atualmente são 3, 5, 17, 257 e 65537. Não se sabe se existem mais primos de Fermat ou não. A próxima proposição da uma caracterização um pouco mais simples dos primos de Fermat.

Proposição 5.14. Seja $p \in \mathbb{N}$ um número primo. Então,

$$p \text{ é um primo de fermat} \iff p = 2^k + 1 \text{ para algum } k \in \mathbb{N}.$$

Demonstração. A implicação ($\implies$) segue diretamente da definição. Vamos trabalhar, então, na recíproca. Vamos mostrar que, se $2^k + 1$ é um número primo, então k necessariamente é uma potência de 2.

Suponha, por absurdo, que isso não é verdade, ou seja, existe um número natural $k = rq$, onde q um fator primo ímpar e $1 \leq r < k$. Então, $2^k+1 = 2^{rs}+1$. Além disso, como -1 é raiz de x^s+1 (s é ímpar), devemos ter que $x+1 \mid x^s+1$. Em particular, se substituirmos $x = 2^r$, obtemos que $2^r + 1 \mid 2^{rs} + 1$. Por fim, como $1 < 2^r + 1 < 2^k + 1$, isso implica que $2^k + 1$ tem um divisor próprio diferente de 1, um absurdo. □

Teorema 5.15. As proposições a seguir são equivalentes:

(i) Um polígono de n lados é construtível.

(ii) Um ângulo de medida $2\pi/n$ é construtível.

(iii) O grau da extensão ciclotômica $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ é uma potência de 2.

(iv) n tem apenas potências de 2 e primos de Fermat ímpares de multiplicadade 1 em sua fatoração prima.

Demonstração. (i) $\iff$ (ii). Segue direto da definição que construir um polígono regular de n lados equivale a construir um ângulo de $2\pi/n$ em seu centro.

(ii) $\iff$ (iii) Se um ângulo de medida $2\pi/n$ é construtível, então $\cos(2\pi/n)$ será um número construtível, assim $[\mathbb{Q}(\cos(2\pi/n)) : \mathbb{Q}]$ é uma potência de 2, pela caracterização dos números construtíveis, e como

$$\begin{aligned}[\mathbb{Q}(\zeta_n) : \mathbb{Q}] &= [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\cos(2\pi/n))][\mathbb{Q}(\cos(2\pi/n)), \mathbb{Q}] \\ &= 2[\mathbb{Q}(\cos(2\pi/n)), \mathbb{Q}]\end{aligned}$$

segue que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ também será.

Considere, agora, o caso onde $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ é uma potência de 2 (pois a cardinalidade de G é uma potência de 2). Como $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ é uma extensão galoisiana (Teorema 4.16), deverá existir, pelo Teorema Fundamental (Teorema 3.33), uma cadeia de grupos

$$\langle \mathrm{id} \rangle \trianglelefteq H \trianglelefteq G,$$

que corresponde à cadeia de corpos

$$\mathbb{Q}(\zeta_n) \supseteq \mathbb{Q}(\cos(2\pi/n)) \supseteq \mathbb{Q},$$

onde $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ e $|H| = 2$ (a normalidade $H \trianglelefteq G$ na cadeia de grupos segue do fato de que G é abeliano, também pelo Teorema 4.16).

Então, pela recíproca do Teorema de Lagrange para grupos abelianos, existem $H_1, \cdots, H_{n-1}$ de tal forma que

$$\langle \mathrm{id} \rangle \trianglelefteq H = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G,$$

onde cada par consecutivo de subgrupos tem índice 2, e isso, novamente pela correspondência de Galois, irá corresponder a uma cadeia

de extensões quadráticas

$$\mathbb{Q}(\zeta_n) \supseteq \mathbb{Q}(\cos(2\pi/n)) = K_0 \supseteq K_1 \supseteq \cdots \supseteq K_n = \mathbb{Q}.$$

Logo $\cos(2\pi/n)$ é construtível, pela caracterização dos números construtíveis (Teorema 5.7). Ou seja, é possível construir um ângulo de medida $2\pi/n$ (Teorema 5.13).

(iii) $\iff$ (iv). Suponha, primeiramente, que n seja par, e seja $2^{\alpha}p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ sua fatoração prima. Como $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n) = 2^{\alpha-1}p_1^{\alpha_1-1}\cdots p_k^{\alpha_k-1}(p_1-1)\cdots(p_k-1)$, dizer que $[\mathbb{Q}(\zeta_n):\mathbb{Q}]$ é uma potência de 2 equivale a dizer que $\alpha_i = 1$ e $p_i - 1$ é uma potência de 2 para cada $i \in \{1, \cdots, k\}$. Em outras palavras, cada p_i é um primo de Fermat pela Proposição 5.14. Caso n seja ímpar, o argumento é análogo, basta ignorar os fatores de 2. □

Como consequência desse resultado, podemos caracterizar os ângulos de medida, em grau, inteira e racional.

Teorema 5.16. Um ângulo de medida n° é construtível $\iff 3 \mid n$, onde $n \in \mathbb{N}$.

Demonstração. Dizer que um ângulo de medida n° é construtível equivale a dizer que um ângulo de medida $\text{mdc}(n, 360)^\circ$ é construtível.

De fato, se o ângulo de n° é construtível, o Teorema de Bézout garante a existência de inteiros a, b onde $na + 360b = \text{mdc}(n, 360)$. Como as medidas dos ângulos construtíveis são fechados por combinações $\mathbb{Z}$-lineares, pelo Teorema 5.12, segue que, se n° é construtível, $\text{mdc}(n, 360)^\circ$ também será. Para a recíproca, perceba que, se o ângulo de medida $\text{mdc}(n, 360)^\circ$ é construtível, o ângulo de medida n° também será, visto que $\text{mdc}(n, 360) \mid n$.

Escreva, então, $m = \text{mdc}(n, 360)$. Como m divide 360, o ângulo de medida m° é construtível se, e somente se, o polígono regular de $360/m$ lados é construtível. Isso equivale a dizer que $360/m$ possui

apenas potências de 2 e primos de Fermat de multiplicidade 1 em sua fatoração prima,

Como 360 se fatora em $2^3 \cdot 3^2 \cdot 5$, m deve cancelar, ao menos, uma das potências de 3 dessa fatoração, ou seja, equivale a dizer que $3 \mid m$. E, pela definição de mdc, devemos ter que $3 \mid m$ se, e somente se, $3 \mid n$, visto que 3 é um fator de 360. Isso completa a demonstração. □

Teorema 5.17. Um ângulo de medida racional (em graus) $(p/q)°$, com $p, q \in \mathbb{Z}$ relativamente primos, é construtível $\iff$ $3 \mid p$ e q contém apenas fatores de 2 e primos de Fermat de multiplicidade 1, com excessão de 3 e 5, em sua fatoração prima.

Demonstração. Seja $m = \text{mdc}(p, 360q)$. Perceba que, como $\text{mdc}(p, q) = 1$, então $m = \text{mdc}(p, 360)$. Assim pelo Teorema de Bézout, existem $a, b \in \mathbb{Z}$ tal que $ap + bq360 = m$. Dividindo essa equação por p, temos que $a\frac{p}{q} + b360 = \frac{m}{q}$.

Nessas condições, como $m \mid p$, temos que construir um ângulo de medida $(p/q)°$ equivale a construir um ângulo de medida $(m/q)°$. Isso, por sua vez equivale a construir um polígono regular de $360q/m$ lados, já que $m \mid 360°$. Isso equivale a dizer, pelo teorema anterior, que $3 \mid p$ e q não tem fatores de 3 ou 5, pois 360 já possui esses primos de Fermat. □

Finalizaremos esse capítulo com a resolução de um problema clássico, que afirma que é impossível trissectar ângulos com régua e compasso. Na verdade, é impossível dividir em mais de duas partes iguais, em geral, salvo as potências de 2, obtidas através de bisseções sucessivas.

Teorema 5.18. É sempre possível dividir um ângulo em p partes iguais ($p \in \mathbb{N}$ primo) $\iff$ $p = 2$. Ou seja, em geral, é apenas possível fazer bissecções sucessivas de ângulos.

Demonstração. Considere, por exemplo, um ângulo, construtível, de medida $3°$, assim, para qualquer primo $p \neq 2$, o ângulo de medida $(3/p^2)°$ não é construtível, pelo teorema anterior, ou seja, não é possível fazer divisores sucessivas de um ângulo construtível em p partes iguais. Além disso, caso $p = 2$, sabemos, pela construção da bissecção de ângulos, que é possível dividir um ângulo em 2 partes iguais sempre. □

6 EXTENSÕES CÍCLICAS E SOLUBILIDADE POR RADICAIS

Nesse capítulo estudaremos outra aplicação clássica da Teoria de Galois, que é, na verdade, a razão pela qual foi criada: a resolução de equações polinomiais por meio de fórmulas que utilizam apenas, no máximo, radicais.

Para o estudo de tal tema, primeiro precisamos desenvolver um pouco mais a teoria de extensões radicais, que, dadas certas condições, coincide com o estudo de extensões cujo grupo de Galois é cíclico. Essas extensões onde tais condições são equivalentes são ditas ser extensões de Kummer, e serão o primeiro objeto de estudo desse capítulo.

6.1 EXTENSÕES DE KUMMER

Iniciamos a seção introduzindo a noção de resolventes de Lagrange, que serão de grande utilidade, tanto do ponto de vista teórico, quanto do ponto de vista prático, quando deduzirmos as fórmulas para equações polinomiais.

Definição 6.1. Seja L/K uma extensão cíclica de ordem n, σ um gerador de seu grupo de Galois, $\omega \in K$ uma raiz n-ésima da unidade e $\theta \in L$ um elemento qualquer. Definimos o resolvente de Lagrange (ω, θ) por

$$(\omega, \theta) = \theta + \omega\sigma(\theta) + \omega^2\sigma^2(\theta) + \cdots + \omega^{n-1}\sigma^{n-1}(\theta).$$

Proposição 6.2. Seja K um corpo que tenha uma raiz primitiva n-ésima ζ, L/K uma extensão cíclica de ordem n, σ um gerador de seu grupo de Galois e $\theta \in L$. Então,

(i) $\sigma((\omega, \theta)) = \omega^{-1}(\omega, \theta)$ para qualquer $\omega \in \mu_n(K)$.

(ii) $(1, \theta) \in K$.

(iii) $(\omega, \theta)^n \in K$ para qualquer $\omega \in \mu_n(K)$.

(iv) $\sum_{i=0}^{n-1} (\zeta^i, \theta) = n\theta$.

Demonstração. (i).

$$\begin{aligned}\sigma((\omega,\theta)) = \sigma\left(\sum_{i=0}^{n-1}\omega^i\sigma^i(\theta)\right) &= \sum_{i=0}^{n-1}\omega^i\sigma^{i+1}(\theta)\\ &= \omega^{-1}\sum_{i=0}^{n-1}\omega^{i+1}\sigma^{i+1}(\theta)\\ &= \omega^{-1}(\omega,\theta).\end{aligned}$$

(ii) e (iii). Basta notar que $(1, \theta)$ e (ω, θ) são fixos por σ, pertencem a $L^{\mathrm{Gal}(L/K)} = K$.

(iv)

$$\sum_{i=0}^{n-1}(\zeta^i,\theta) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1}\zeta^{ij}\sigma^j(\theta) = \sum_{j=0}^{n-1}\left(\sum_{i=0}^{n-1}(\zeta^j)^i\right)\sigma^j(\theta) = n\theta,$$

já que $\sum_{i=0}^{n-1}(\zeta^j)^i = 0$ se $j > 0$, pois toda raiz n-ésima da unidade ($\neq 1$) é raiz de $1 + x + x^2 + \cdots + x^{n-1} \in K[x]$. □

O resolvente de Lagrange será importante para tornar algumas demonstrações que serão feitas a seguir menos volumosas. Também terão um papel fundamental, por contra de suas propriedades algébricas, na dedução das fórmulas para a resolução de equações polinomiais mais adiante, na seção 6.2.

Definição 6.3. Uma extensão L/K é dita ser uma extensão de Kummer se $L = K(\beta)$ onde $\beta^n \in K$, e K contém uma raiz primitiva n-ésima da unidade ζ_n, para algum $n \in \mathbb{N}$.

Note que nestas condições, $\mathrm{char}(K)$ não pode dividir n, visto que raízes primitivas n-ésimas não existiriam nesse caso.

Teorema 6.4. Toda extensão de Kummer é galoisiana, com grupo de Galois cíclico.

Demonstração. Seja $K(\beta) \supseteq K$ uma extensão de Kummer, onde $\beta^n, \zeta_n \in K$ para algum n. Perceba que $K(\beta)/K$ é galoisiana, já que é o corpo de raízes do polinômio $x^n - \beta^n = \prod_{i=0}^{n-1}(x - \zeta_n^i \beta)$. Afirmamos que $\mathrm{Gal}(K(\beta)/K)$ é isomorfo a algum subgrupo de $\mu_n(K)$, portanto, será cíclico.

Para ver isso, considere a aplicação $\mathrm{Gal}(K(\beta) : K) \to \mu_n(K)$ dada por $\sigma \mapsto \sigma(\beta)/\beta$. Essa aplicação está bem definida, já que β é raiz de $x^n - b^n \in K[x]$, logo $\sigma(\beta)$ também deve ser. Ou seja, $\sigma(\beta) = \zeta_n^k \beta$ para algum $k \in \mathbb{Z}$. Isso implica que $\sigma(\beta)/\beta = \zeta_n^k$, que é uma raiz n-ésima da unidade. A aplicação é também um morfismo, já que

$$\frac{\tau\sigma(\beta)}{\beta} = \frac{\tau(\zeta_n^{k_\sigma}\beta)}{\beta} = \frac{\zeta_n^{k_\tau}\zeta_n^{k_\sigma}\beta}{\beta} = \frac{\zeta_n^{k_\tau}\beta}{\beta}\frac{\zeta_n^{k_\sigma}\beta}{\beta} = \frac{\tau(\beta)}{\beta}\frac{\sigma(\beta)}{\beta}.$$

Por fim, note que $\sigma(\beta)/\beta = 1 \implies \sigma(\beta) = \beta \implies \sigma = \mathrm{id}$, ou seja, o núcleo da aplicação consiste apenas na identidade, e segue que a aplicação é injetora. □

Teorema 6.5. Seja K um corpo que tem uma raiz primitiva n-ésima e L/K uma extensão galoisiana, então

$$\mathrm{Gal}(L/K) \text{ é cíclico de ordem } n \implies L/K \text{ é de Kummer.}$$

Demonstração. Seja σ um gerador de $\mathrm{Gal}(L/K)$. Para mostrar que L/K é de Kummer, basta mostrar que é uma extensão radical. Faremos isso mostrando que existe um elemento $\beta \in L$, onde $\sigma(\beta) = \zeta_n\beta$ para alguma raiz primitiva n-ésima ζ_n. Isso mostra o resultado pois teríamos que os conjugados de β sobre K são os elementos da forma

$\sigma^i(\beta) = \zeta_n^i\beta$, com $a \in \{0, \ldots, n-1\}$ que são todos distintos entre si. Portanto o polinômio minimal de β será $\prod_{i=1}^{n}(x - \zeta_n^i\beta) = x^n - \beta^n \in K[x]$. Assim,

$$[K(\beta) : K] = n \implies [L : K(\beta)] = 1 \implies L = K(\beta).$$

Vamos agora à procura de tal elemento.

Para isso, vamos inicialmente olhar para L como um K-espaço vetorial. Considere um elemento qualquer $v \in L$. Sabemos que o resovente de Lagrange (ζ_n^{n-k}, v), pela Proposição 6.2, é um autovetor de σ com autovalor ζ_n^k.

Assim, temos também pela Proposição 6.2 que

$$v = \frac{1}{n}\sum_{k=0}^{n-1}(\zeta_n^{n-k}, v)$$

(lembre que $\mathrm{char}(K)$ não divide n), para qualquer que seja o $v \in L$. Portanto, o conjunto $\mathcal{B} = \{(\zeta_n^{n-k}, v) : v \in L, 0 \leq k < n\}$, composto de autovetores onde seus autovalores são raízes n-ésimas da unidade, é um conjunto gerador do K-espaço L. Logo, esse conjunto deve conter uma base $\{v_1, \cdots, v_n\} \subseteq \mathcal{B}$.

Defina d_i como a ordem (em $\mu_n(K)$) do autovalor de cada v_i. Como todo elemento de L pode ser escrito como uma combinação linear única dos v_i's, então a menor das potências positivas de σ que fixa todos os v_i é $\mathrm{mmc}(d_1, \ldots, d_n)$. Portanto $n = \mathrm{mmc}(d_1, \cdots, d_n)$, pois n é a ordem de σ por hipótese. Assim, o elemento não nulo $v_1 \cdots v_n$ será um autovetor, com autovalor igual a $\zeta_{d_1} \cdots \zeta_{d_n} = \zeta_{\mathrm{mmc}(d_1, \cdots, d_n)}$, onde ζ_k denota uma raiz primitiva k-ésima, e isso completa a demonstração. □

6.2 RESOLUÇÃO DE EQUAÇÕES POLINOMIAIS

essa seção deduziremos as fórmulas para as equações polinomiais de grau 2 e 3 utilizando os métodos desenvolvidos até então.

6.2.1 A equação de segundo grau

Todo estudante sabe como resolver uma equação polinomial de grau 2, porém mostraremos como os métodos desenvolvidos até então podem ser aplicados para sua resolução, como um "aquecimento" para a equação de grau 3.

Caso o leitor não esteja familiarizado com polinômios simétricos e suas propriedades, recomenda-se que seja realizada, primeiramente, a leitura do apêndice B.

Primeiramente, considere um corpo K, onde $\mathrm{char}(K) \neq 2$, e considere a extensão $K(x_1, x_2)/K(e_1, e_2)$ onde e_1, e_2 são os polinômios simétricos elementares nas variáveis x_1, x_2. Já sabemos que essa extensão é galoisiana, pois é o corpo de raízes de $x^2 - e_1 x + e_2$, e seu grupo de Galois é S_2, que age sobre os índices das variáveis x_1, x_2, e é gerado por $\sigma = (1\ 2)$.

Então, defina $\delta = x_1 - x_2$. Perceba que $\Delta = \delta^2$ é invariante sobre a ação de S_2, visto que a única permutação não trivial em S_2 é $(1\ 2)$, que apenas troca o sinal de $\delta = x_1 - x_2$, que não muda o valor da expressão quando elevada ao quadrado.

Portanto, $\delta^2 \in K(x_1, x_2)^{S_2} = K(e_1, e_2)$. Logo, pelo Teorema das Funções Simétricas (Teorema B.11) podemos escrever δ^2 em termos dos polinômios simétricos elementares, utilizando o algoritmo visto no teorema. Obtemos, então, que $\delta^2 = e_1^2 - 4e_2$.

Por outro lado, δ não é fixo sobre a ação de S_3, já que muda de sinal a cada transposição, portanto, $\delta \notin K(e_1, e_2)$, assim temos que $K(x_1, x_2) = K(e_1, e_2, \delta)$, agora nos resta escrever as raízes x_1, x_2 em

termos de e_1, e_2 e δ.

Mas isso é fácil, já que se somarmos as equações $x_1 + x_2 = e_1$ e $x_1 - x_2 = \delta$ obtemos que $x_1 = \frac{e_1+\delta}{2}$ e aplicando σ à igualdade, também temos $x_2 = \frac{e_1-\delta}{2}$, o que nos dá a fórmula geral

$$x_{1,2} = \frac{e_1 \pm \delta}{2} = \frac{e_1 \pm \sqrt{e_1^2 - 4e_2}}{2}.$$

Aplicando essa fórmula à equação geral $ax^2 + bx + c = 0 \iff x^2 + (b/a)x + (c/a) = 0$, podemos identificar os coeficientes $b/a = -e_1$ e $c/a = e_2$, assim obtendo a fórmula tradicional

$$x_{1,2} = \frac{-b/a \pm \sqrt{b^2/a^2 - 4c/a}}{2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

6.2.2 A equação de terceiro grau

Similarmente à seção anterior, considere a extensão

$$M(x_1, x_2, x_3)/M(e_1, e_2, e_3),$$

onde $\mathrm{char}(M) \neq 2, 3$ e M tem uma raiz primitiva terceira da unidade ζ. Tal extensão é galosiana, pois é o corpo de raízes do polinômio separável

$$(x - x_1)(x - x_2)(x - x_3) = x^3 - e_1x^2 + e_2x - e_3$$

com grupo de Galois S_3, que age sobre os índices dos x_i. Por simplicidade, denotaremos $L = M(x_1, x_2, x_3)$ e $K = M(e_1, e_2, e_3)$.

Pelo Teorema Fundamental da Teoria de Galois, a cadeia de subgrupos maximais

$$\langle \mathrm{id} \rangle \trianglelefteq A_3 \trianglelefteq S_3$$

corresponde à cadeia extensões galoisianas

$$L \supseteq L^{A_3} \supseteq K.$$

Não é difícil adivinhar um elemento que gera L^{A_3}, uma escolha fácil é

$$\delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3),$$

que troca de sinal a cada transposição, logo $\delta \in L^{A_3}$ e $\delta \notin L^{S_3} = K$. Daí, $L^{A_3} = K(\delta)$.

Similarmente ao caso anterior, δ^2 é invariante sobre a ação de S_3, portanto $\delta^2 \in M(e_1, e_2, e_3)$. Assim, pelo Teorema das Funções Simétricas (Teorema B.11) podemos escrever δ^2 polinômios elementares

$$\delta^2 = e_1^2e_2^2 - 4e_2^3 - 4e_1^3e_3 - 27e_3^2 + 18e_1e_2e_3.$$

Assim, temos que $\delta = \sqrt{e_1^2e_2^2 - 4e_2^3 - 4e_1^3e_3 - 27e_3^2 + 18e_1e_2e_3}$.

Vamos agora analisar a extensão $K(x_1, x_2, x_3)/K(\delta)$. Essa extensão é também galoisiana, pois é uma sub-extensão superior de $K(x_1, x_2, x_3)/K$, que tem grupo de Galois isomorfo a A_3, que é gerado por $\sigma = (1\ 2\ 3)$. Pela Proposição 6.2, temos que $(1, x_1), (\zeta, x_1)^3, (\zeta^2, x_1)^3 \in K(\delta)$. E, de fato, cada um desses pode ser escrito em termos dos polinômios simétricos elementares e δ da seguinte forma

$$(1, x_1) = x_1 + x_2 + x_3 = e_1,$$

$$(\zeta, x_1)^3 = (x_1 + \zeta x_2 + \zeta^2 x_3)^3 = e_1^3 - \frac{9e_1e_2}{2} + \frac{27e_3}{2} + \frac{3\sqrt{-3}\delta}{2},$$

$$(\zeta^2, x_1)^3 = (x_1 + \zeta^2 x_2 + \zeta x_3)^3 = e_1^3 - \frac{9e_1e_2}{2} + \frac{27e_3}{2} - \frac{3\sqrt{-3}\delta}{2}.$$

Assim, também pela Proposição 6.2 temos que

$$x_1 = \frac{(1, x_1) + (\zeta, x_1) + (\zeta^2, x_1)}{3},$$

$$x_2 = \frac{(1, x_1) + \zeta^2(\zeta, x_1) + \zeta(\zeta^2, x_1)}{3},$$

$$x_3 = \frac{(1, x_1) + \zeta(\zeta, x_1) + \zeta^2(\zeta^2, x_1)}{3}.$$

As igualdades de x_2 e x_3 foram obtidas aplicando o morfismo $\sigma = (1\ 2\ 3)$. Estamos prontos para escrever a fórmula final.

Seja $ax^3 + bx^2 + cx + d = 0$ uma equação polinomial onde $a, b, c, d \in M$ e $a \neq 0$. Então, temos que $x^3+(b/a)x^2+(c/a)x+(d/a) = 0$. Para tornar a equação mais simples, vamos fazer uma translação para nos livrarmos do termo quadrático, assim eliminando boa parte dos termos das expressões anteriores, isso é possível definindo $y = x + \frac{b}{3a}$. Assim, fazendo a substituição, temos que a equação anterior equivale a $y^3 + py + q = 0$, onde

$$p = -\frac{b^2}{3a^2} + \frac{c}{a},$$
$$q = \frac{2b^3}{27a^3} - \frac{bc}{3a^2} + \frac{d}{a}.$$

Tomando $-e_1 = 0, e_2 = p, -e_3 = q$, substituindo e fazendo algumas manipulações algébricas, obtemos,

$$(1, y_1) = 0,$$
$$\delta = \sqrt{-4p^3 - 27q^2} = \frac{-18}{\sqrt{-3}}\sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2},$$
$$(\zeta, y_1) = \sqrt[3]{-\frac{27q}{2} + \frac{3\sqrt{-3}\delta}{2}} = 3\sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}},$$
$$(\zeta^2, y_1) = \sqrt[3]{-\frac{27q}{2} - \frac{3\sqrt{-3}\delta}{2}} = 3\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}}.$$

e, portanto,

$$y_1 = \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} + \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}},$$
$$y_2 = \zeta^2\sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} + \zeta\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}},$$
$$y_3 = \zeta\sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} + \zeta^2\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}}.$$

Assim podemos encontrar as solução x_1, x_2, x_3 utilizando o fato de que $x_i = y_i - \frac{b}{3a}$. Nada amigável!

Exemplo 6.6. Considere o polinômio $x^3 - 7x + 6$. É fácil descobrir utilizando métodos básicos que suas raízes são 1, 2 e -3, por outro lado, se aplicarmos a fórmula, tomando $p = -7$ e $q = 6$, obtemos que as raízes são

$$x_1 = \sqrt[3]{-3 + \frac{10i\sqrt{3}}{9}} + \sqrt[3]{-3 - \frac{10i\sqrt{3}}{9}},$$
$$x_2 = \zeta\sqrt[3]{-3 + \frac{10i\sqrt{3}}{9}} + \zeta^2\sqrt[3]{-3 - \frac{10i\sqrt{3}}{9}},$$
$$x_3 = \zeta^2\sqrt[3]{-3 + \frac{10i\sqrt{3}}{9}} + \zeta\sqrt[3]{-3 - \frac{10i\sqrt{3}}{9}}.$$

utilizando uma calculadora de números complexos (ou muitas manipulações algébricas) temos que essas são de fato as raízes 2, -3, e 1, respectivamente. Ou seja, mesmo em casos simples, a fórmula não se mostra muito útil.

Não será feita a dedução para a fórmula para polinômio de quarto grau, por conta de sua complexidade, porém, a ideia principal é a mesma. Ela seria feita por meio da cadeia

$$\langle \mathrm{id} \rangle \trianglelefteq \langle (1\,2)(3\,4) \rangle \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4,$$

onde $V_4 = \langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle$, e essa cadeia corresponderia a uma cadeia de extensões intermediárias de $M(x_1, x_2, x_3, x_4)/M(e_1, e_2, e_3, e_4)$ todas radicais, pois são de Kummer, visto que os quocientes são todos cíclicos (assumindo que M contém uma raiz 3-ésima primitiva da unidade). Aplicando repetidamente o truque usado com os resolventes de Lagrange e o Teorema das Funções Simétricas (B.11), poderíamos achar expressões para x_1, x_2, x_3, x_4 em função de expressões radicais de e_1, e_2, e_3, e_4.

6.3 O CRITÉRIO DE SOLUBILIDADE

Nessa seção mostraremos a condição necessária e suficiente para a solubilidade de polinômios em corpos de característica 0.

Recomenda-se que o leitor, caso não esteja familiarizado com grupos solúveis, leia o apêndice A antes de inicia a leitura desta seção.

Iniciamos com a seguinte definição.

Definição 6.7. Dizemos que um polinômio $f(x) \in K[x]$, onde K é um corpo, é solúvel por radicais se é possível expressar as raízes de $f(x)$ apenas com radicais e as operações do corpo, utilizando elementos de K. Em linguagem de corpos, isso significa que existe uma sequência de extensões radicais

$$K_n \supseteq K_{n-1} \supseteq \cdots \supseteq K_1 \supseteq K,$$

onde o corpo de raízes de $f(x)$ sobre K está contido em K_n.

Definição 6.8. Seja $f(x) \in K[x]$ e L seu corpo de raízes sobre K. Se L/K é galoisiana, definimos $\mathrm{Gal}(f(x)) = \mathrm{Gal}(L/K)$.

Perceba que em qualquer corpo de característica 0, faz sentido falar sobre o grupo de Galois de qualquer polinômio $f(x)$, pois qualquer corpo de decomposição forma uma extensões galoisiana, visto que a separabilidade já está garantida.

Vamos investigar as consequências da solubilidade por radicais de um polinômio em seu grupo de Galois.

Teorema 6.9. Seja K um corpo de característica 0 e $f(x) \in K[x]$. Então, $f(x)$ é solúvel por radicais em $K \iff \mathrm{Gal}(f(x))$ é solúvel.

Demonstração. ($\implies$) Queremos mostrar que, se F é o corpo de decomposição de $f(x)$, então para qualquer cadeia de extensões radicais

$K_s \supseteq \cdots \supseteq K_1 \supseteq K_0 = K$, onde $F \supseteq K_s$, então $\mathrm{Gal}(F/K)$ é solúvel. Procederemos por indução na quantidade de extensões radicais utilizadas, s. Suponha que $s = 1$, ou seja, $K_1 \supseteq F \supseteq K$, onde K_1/K é uma extensão radical n-ésima, ou seja, $K_1 = K(\sqrt[n]{\beta})$ para algum $\beta \in K$, então podemos fazer a adjução de uma raiz n-ésima primitiva da unidade, obtendo a cadeia $K_1(\zeta_n) \supseteq F(\zeta_n) \supseteq K(\zeta_n) \supseteq K$. É fácil ver que $K_1(\zeta_n) = K(\zeta_n, \sqrt[n]{\beta})$ é uma extensão galoisiana de $K(\zeta_n)$, visto que é o corpo de raízes de $x^n - \beta$, e por ser uma extensão de Kummer, $\mathrm{Gal}(K(\zeta_n, \sqrt[n]{\beta})/K(\zeta_n))$ é cíclica.

($\implies$) Já que $f(x)$ é solúvel, existe uma cadeia de extensões

$$K_n \supseteq \cdots \supseteq K_1 \supseteq K_0 = K,$$

onde $K_{i+1} \supseteq K_i$ é uma extensão radical r_i-ésima e K_s contém o corpo de raízes de $f(x)$, digamos L. Essas extensões não são necessariamente galoisianas, porém podemos fazer com que elas sejam fazendo um simples remendo. Considere o número $r = \mathrm{mmc}(r_0, \ldots, r_{n-1})$, e seja ζ_r uma raiz r-ésima da unidade. Assim, a torre

$$K_s(\zeta_r) \supseteq \cdots \supseteq K_1(\zeta_r) \supseteq K_0(\zeta_r) \supseteq K_0 = K,$$

também é composta por extensões radicais, com $K(\zeta_r) \supseteq K$ ciclotômica (portanto galoisiana e abeliana), e $K_i(\zeta_r) \supseteq K_{i-1}(\zeta_r)$ de Kummer, pois $K_{i-1}(\zeta_r)$ contém a raiz primitiva r_i-ésima da unidade ζ_r^{r/r_i}, logo, também, são galoisianas e cíclicas.

Ainda não é necessariamente verdade que $K_s(\zeta_r) \supseteq K$ é galoisiana, que seria necessário para aplicar o Teorema Fundamental, mas podemos consertar isso. Considere, por exemplo, as extensões

$$K_2(\zeta_r) \supseteq K_1(\zeta_r) \supseteq K(\zeta_r) \supseteq K,$$

por hipótese, $K_2(\zeta_r) = K_1(\zeta_r, \beta_1)$ para algum $\beta_1 \in K_2$ onde $\beta_1^{r_1} \in K_1(\zeta_r)$. Seja $m_1(x)$ o polinômio minimal de $\beta_1^{r_1}$, sobre K. Assim, β_1

é raiz do polinômio $m_1(x^{r_1}) = \prod_{c \in C)} (x^{r_1} - c)$, onde C é o conjunto de conjugados de $\beta_1^{r_1}$. Perceba que todas as outras raízes desse polinômio são raízes r_1-ésimas de algum elemento de $K_1(\zeta_{r_1})$, já que $K_1(\zeta_{r_1}) \supseteq K$ é normal. Adicionando cada uma dessas raízes por vez, obtemos uma sequência de extensões de Kummer (e, portanto, galoisianas e abelianas)

$$K_{2,n_2}(\zeta_r) \supseteq \cdots \supseteq K_{2,1}(\zeta_r) \supseteq K_{2,0}(\zeta_r) = K_2(\zeta_r),$$

com $K_{2,n_2}(\zeta_r) \supseteq K$ galoisiana (é o corpo de raízes de $m_1(x^{r_1})(x^r - 1)$).

Fazendo o compósito de toda a cadeia radical com $K_{2,n_2}(\zeta_r)$ (a partir de $K_3(\zeta_r)$), obtemos a cadeia radical

$$K_s^{(2)}(\zeta_r) \supseteq \cdots \supseteq K_3^{(2)}(\zeta_r) \supseteq K_{2,n_2}(\zeta_r) \supseteq \cdots \supseteq K_{2,1}(\zeta_r) \supseteq \cdots \supseteq K,$$

onde $K_i^{(2)}(\zeta_r) = K_i(\zeta_r)K_{2,n_2}(\zeta_r)$. Exatamente o mesmo argumento pode ser repetido para a cadeia $K_3^{(2)}(\zeta_r) \supseteq K_{2,n_2}(\zeta_r) \supseteq K$, Obtendo uma cadeia de extensões de Kummer $K_{3,n_3}^{(2)}(\zeta_r) \supseteq \cdots \supseteq K_3^{(2)}$, onde $K_{3,n_3}^{(2)}(\zeta_r) \supseteq K$ é galoisiana.

Prosseguindo indutivamente, eventualmente obteremos uma cadeia de extensões de abelianas

$$\begin{array}{ccccc}
K_{s,n_s}^{(s-1)}(\zeta_r) & \supseteq \cdots \supseteq & K_{s,1}^{(s-1)}(\zeta_r) & & \\
\supseteq K_{s-1,n_{s-1}}^{(s-2)}(\zeta_r) & \supseteq \cdots \supseteq & K_{s-1,1}^{(s-2)}(\zeta_r) & & \\
\vdots & \vdots & \vdots & & \\
\supseteq \quad K_{3,n_3}^{(2)}(\zeta_r) & \supseteq \cdots \supseteq & K_{3,1}^{(2)}(\zeta_r) & & \\
\supseteq \quad K_{2,n_2}(\zeta_r) & \supseteq \cdots \supseteq & K_{2,1}(\zeta_r) & \supseteq K_1(\zeta_r) \supseteq K(\zeta_r) \supseteq K, &
\end{array}$$

onde $K_{s,n_s}^{s-1} \supseteq K$ é galoisiana.

Pelo Teorema Fundamental da Teoria de Galois, a cadeia radical acima corresponde a uma cadeia de subgrupos normais

$$\langle \mathrm{id} \rangle = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_m = \mathrm{Gal}(K_{s,n_s}^{(s-1)}/K),$$

onde cada H_i/H_{i-1} é abeliano. Ou seja, $\mathrm{Gal}(K_{s,n_s}^{(s-1)}/K)$ é solúvel. E como $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(K_{s,n_s}^{(s-1)}/K)/\mathrm{Gal}(K_{s,n_s}^{(s-1)}/L)$, segue que o grupo de Galois de $f(x)$ é solúvel, pois é o quociente de um grupo solúvel.

($\Longleftarrow$) Como $\mathrm{Gal}(f(x))$ é um grupo finito (tem cardinalidade no máximo $\deg(f(x))!$, pelo Teorema 2.44), podemos, sem perda de generalidade, assumir que os subgrupos que aparecem na cadeia

$$\langle \mathrm{id} \rangle = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = \mathrm{Gal}(f(x)),$$

são todos maximais, pelo Teorema A.9, portanto, os respectivos quocientes H_i/H_{i-1} são todos simples, isso implica, por sua vez, que são ciclicos, visto que são abelianos por hipótese, e os únicos grupos simultaneamente simples e abelianos são os grupos cíclicos $\mathbb{Z}/p\mathbb{Z}$, com p primo. Pelo Teorema Fundamental da Teoria de Galois, então, tal cadeia de subgrupos corresponde a uma cadeia de extensões galoisianas

$$L = K_0 \supseteq K_1 \supseteq \cdots \supseteq K_n = K,$$

onde $\mathrm{Gal}(K_{i-1}/K_i) = H_i/H_{i-1}$, pelo Teorema Fundamental, que é cíclico. A ideia a partir daqui é fazer com que estas extensões sejam de Kummer, fazendo a adjunção da raiz primitiva necessária, para isso, considere $k_i = |\mathrm{Gal}(K_{i-1})/K_i|$, $k = \prod_{i=1}^{n} k_i$ e a cadeia de transportes paralelos

$$L(\zeta_k) = K_0(\zeta_k) \supseteq K_1(\zeta_k) \supseteq \cdots \supseteq K_n(\zeta_k) = K(\zeta_k) \supseteq K.$$

Cada extensão $K_i(\zeta_k)/K_{i-1}(\zeta_k)$ continua galoisiana, visto que é um transporte paralelo de uma extensão galosiana, e tem uma raiz k_i-ésima primitiva da unidade, a saber ζ_k^{k/k_i}, portanto, cada uma dessas extensões é de Kummer, com excessão da primeira $K(\zeta_k) \supseteq K$, que é ciclotômica. Isso, então, significa que todas as extensões são radicais, portanto, $f(x)$ é solúvel por radicais. $\square$

Note que, se $f(x) \in K[x]$ é um polinômio solúvel em $\mathbb{C}$, isso não necessariamente significa que é possível expressar as raízes de $f(x)$ em termos dos coeficientes, que seria o que entendemos por uma fórmula, mas sim, expressar em termos de qualquer elemento do corpo base K.

Por exemplo, qualquer polinômio em $\mathbb{C}[x]$ é solúvel, pois seu corpo de raízes é o próprio $\mathbb{C}$, já que $\mathbb{C}$ é algebricamente fechado. Isso não necessariamente implica que é possível expressar as raízes por meio dos coeficientes de $f(x)$.

Para um estudo da fórmula fechada para um polinômio qualquer, se faz um estudo das extensões chamadas genéricas, isto é, as extensões da forma $K(x_1, \ldots, x_n)/K(e_1, \ldots, e_n)$, onde e_i é o i-ésimo polinômio simétrico elementar em n variáveis. Essa extensão é galoisiana, pois é o corpo de raízes do polinômio separável (que também chamaremos de polinômio genérico) $f(x) = (x - x_1) \cdots (x - x_n) = x^n - e_1 x^{n-1} + \cdots + (-1)^n e_n \in K(x_1, \ldots, x_n)[x]$. Afirmar que existe uma fórmula para polinômios de grau n no corpo K (que envolve apenas radicais e as operações do corpo) equivale a dizer que esse polinômio genérico $f(x)$ é solúvel. Nosso primeiro passo é o estudo das extensões genéricas.

Teorema 6.10. Seja K um corpo qualquer de característica 0. Então, o polinômio genérico $f(x) = (x - x_1) \cdots (x - x_n) \in K(e_1, \ldots, e_n)[x]$ é solúvel por radicais em $K(e_1, \ldots, e_n) \iff n < 5$

Demonstração. O fato de que os polinômios genéricos de grau 4 ou menos são solúveis em $K(e_1, \ldots, e_n)$ (com n apropriado) já foi mostrado na seção anterior. Já para o polinômio genérico de grau n para $n \geq 5$, seu grupo de Galois será isomorfo a S_n, pelo Exemplo 2.61, que não um grupo solúvel para $n \geq 5$, pelo Teorema A.13. Logo, o polinômio genérico não é solúvel pelo critério de solubilidade. □

Veja que esse fato se reflete de forma direta na dedução das fórmulas, que ocorreu anteriormente. Foi possível encontrar as expressões radicais justamente pela existência de uma cadeia de subgrupos normais, de seu grupo de Galois, onde cada um dos fatores era cíclico. Isso mostra, de uma certa maneira, que o raciocínio utilizado anteriormente é o único possível, do ponto de vista algébrico, com qualquer outro raciocínio para o descobrimento dessas fórmulas sendo ou mais fraco, ou equivalente.

7 CONCLUSÃO

Nesse trabalho foram vistos os principais resultados da Teoria de Galois, que mostram a abrangência e importância dessa teoria. Apesar de ser uma teoria de cunho algébrico, que se estuda, principalmente, a estrutura algébrica de corpo, ela mostra uma relação extremamente profunda entre corpos e grupos, que, quando vistas em um curso introdutório, são estruturas que parecem apenas superficialmente relacionadas.

Essa teoria mostra, também, como que as diferentes áreas da matemática se complementam: no Capítulo 2, as propriedades de espaços vetoriais são essenciais no estudo das extensões finitas. O Capítulo 3 mostra como a derivada formal, uma ferramenta um tanto inesperada, pode ser útil como critério de separabilidade, e como que a estrutura dos grupos de automorfismos de extensões se relacionam com a estrutura da extensão em si. Por fim, os Capítulos 4 e 4 nos mostra como a Teoria dos Números está, também, presente em muitos aspectos das extensões galoisianas.

As principais aplicações vistas no texto são a caracterização dos números e polígonos construtíveis, assim como o critério de solubilidade para polinômios, que mostra que equações polinomiais de grau superior a 4 não tem resolução a partir de fórmulas fechadas.

Alguns temas apropriados para possíveis trabalhos futuros seriam: Teoria Algébrica dos Números, Álgebra Comutativa, Geometria Algébrica, Topologia Algébrica.

REFERÊNCIAS

[1] K. Conrad. *Cyclotomic extensions*. 2015. Disp. em: `https://kconrad.math.uconn.edu/blurbs/galoistheory/cyclotomic.pdf` (acesso em 25/12/2022).

[2] J. Escofier. *Théorie de galois*. 1ª ed. Paris: Masson, 1997.

[3] Y. Jiang. *Galois Theory and the Quintic Equation*. 2018. Disp. em: `https://digitalworks.union.edu/cgi/viewcontent.cgi?article=2207&context=theses` (acesso em 25/12/2022).

[4] S. Martins e E. Tengan. *Álgebra Exemplar*. 1ª ed. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2020.

APÊNDICE A – GRUPOS SOLÚVEIS

Nesse apêndice mostraremos as principais propriedades de grupos solúveis, necessários para o desenvolvimento da teoria no Capítulo 6. Iniciaremos com a definição.

Definição A.1. Um grupo G é dito ser solúvel se existe uma cadeia de subgrupos

$$\langle e\rangle = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G,$$

onde cada grupo quociente H_i/H_{i-1} é abeliano.

Exemplo A.2. Todo grupo abeliano G é solúvel. De fato, basta considerar a cadeia $\langle e\rangle \trianglelefteq G$.

Exemplo A.3. $D_n = \langle \rho, \tau\rangle$ é solúvel para qualquer n, podemos considerar a cadeia $\langle e\rangle \trianglelefteq \langle \rho\rangle \trianglelefteq D_n$.

Proposição A.4. Seja G um grupo solúvel e $H \leq G$ um subgrupo qualquer, então H também é solúvel.

Demonstração. Como G é solúvel por hipótese, existe uma cadeia de subgrupos normais

$$\langle e\rangle \trianglelefteq G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G,$$

onde cada G_i/G_{i-1} é solúvel. Assim, há também uma cadeia de subgrupos normais de H

$$\langle e\rangle = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = H,$$

onde cada $H_i = G_i \cap H$ (é importante relembrar que tomar a intersecção preserva a normalidade entre grupos), e como $H_i/H_{i-1} = (G_i \cap H)/(G_{i-1} \cap H) \cong G_i/G_{i-1}$, que é abeliano, segue o resultado. $\square$

Teorema A.5. Seja G um grupo e $N \trianglelefteq G$. Então, existe uma correspondência biunívoca entre subgrupos normais de G/N e subgrupos normais de G que contém N, dada por $\overline{M} \mapsto \gamma^{-1}(\overline{M})$, onde $\gamma : G \mapsto G/N$ é a projeção canônica.

Demonstração. A aplicação está bem definida, visto que a imagem inversa preserva normalidade, por teoria básica de grupos, e $N = \gamma^{-1}(\{\overline{0}\}) \subseteq \gamma^{-1}(\overline{M})$. Para mostrar que essa aplicação é uma bijeção, note que ela tem inversa dada por $M \mapsto \gamma(M)$. De fato, temos que ambas as composições $\gamma(\gamma^{-1}(\overline{M})) = \overline{M}$ e $\gamma(\gamma^{-1}(M)) = M\text{Ker}(\gamma) = MN = M$, para qualquer $N \leq M \trianglelefteq G$ e $\overline{M} \trianglelefteq G/N$. □

Definição A.6. Um grupo é dito ser simples se ele não tem subgrupos normais, além do grupo trivial e ele mesmo.

Definição A.7. Um subgrupo normal $H \trianglelefteq G$ é dito ser maximal se H é próprio e não há subgrupos normais de G entre H e G.

Proposição A.8. Seja G um grupo e $N \trianglelefteq G$, então

$$N \text{ é maximal } \iff G/N \text{ é simples.}$$

Demonstração. Segue diretamente do Teorema A.5. □

Teorema A.9. Um grupo finito G é solúvel se, e somente se, existe uma cadeia de grupos

$$\langle e \rangle = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G,$$

onde cada G_i/G_{i-1} é cíclico.

Demonstração. Suponha que G seja solúvel, então existe uma cadeia

$$\langle e \rangle = G_{0,0} \trianglelefteq G_{1,0} \trianglelefteq \cdots \trianglelefteq G_{n,0} = G.$$

Se um desses subgrupos não for um subgrupo simples do grupo a direita, podemos adicionar subgrupos maximais na cadeia, até que todos sejam um subgrupo simples do grupo a sua direita, obtendo assim uma cadeia

$$\begin{array}{rcccccccccc}
\langle e\rangle & = & G_{0,0} & \trianglelefteq & G_{0,1} & \trianglelefteq & \cdots & \trianglelefteq & G_{0,m_0} & = & G_{1,0} \\
& = & G_{1,0} & \trianglelefteq & G_{1,1} & \trianglelefteq & \cdots & \trianglelefteq & G_{1,m_1} & = & G_{2,0} \\
& & \vdots & & & & & & \vdots & & \\
& = & G_{n-1,0} & \trianglelefteq & G_{n-1,1} & \trianglelefteq & \cdots & \trianglelefteq & G_{n-1,m_{n-1}} & = & G_{n,0} = G
\end{array}$$

assim, cada quociente consecutivo será um grupo simples. Daí, perceba que $G_{k,i}/G_{k,i-1} \cong [G_{k,i}/G_{k,0}]/[G_{k,i-1}/G_{k,0}]$, portanto, é abeliano, pois $G_{k,i}/G_{k,0}$ e $G_{k,i-1}/G_{k,0}$ são ambos subgrupos de $G_{k+1,0}/G_{k,0}$, que é abeliano por hipótese, e como os únicos grupos simultaneamente simples e abelianos são os cíclicos de ordem prima, segue que cada quociente dessa cadeia é um grupo cíclico de ordem prima. A recíproca é óbvia, e segue direto pela definição. □

Teorema A.10. Seja G um grupo solúvel e $H \trianglelefteq G$ um subgrupo normal, então

$$G \text{ é solúvel} \iff H \text{ e } G/H \text{ são solúveis.}$$

Demonstração. ($\Longrightarrow$) Já foi mostrado na Proposição A.4 que H é solúvel. Como G é solúvel, existe uma cadeia de subgrupos normais

$$\langle e\rangle = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G,$$

onde cada G_i/G_{i-1} é abeliano, para então mostrar que G/H é solúvel, considere a cadeia

$$\langle e\rangle = (G_0H)/H \trianglelefteq (G_1H)/H \trianglelefteq \cdots \trianglelefteq (G_nH)/H = G/H,$$

como os quocientes são da forma

$$[(G_iH)/H]/[(G_{i-1}H)/H] \cong (G_iH)/(G_{i-1}H) \cong G_i/G_{i-1},$$

que são grupos abelianos por hipótese, segue que G/H é solúvel.

($\Longleftarrow$) Por hipótse, existem cadeias

$$\langle e\rangle = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = H,$$

$$\langle e\rangle = G_0/H \trianglelefteq G_1/H \trianglelefteq \cdots \trianglelefteq G_m/H = G/H,$$

onde cada G_i é um subgrupo de G que contém H (isso se dá pelo Teorema A.5), e cada um dos quocientes respectivos de cada cadeia é abeliano. Assim, temos a seguinte cadeia de subgrupos de G

$$\langle e\rangle = H_0 \trianglelefteq \cdots \trianglelefteq H_n = H = G_0 \trianglelefteq \cdots \trianglelefteq G_m = G,$$

o que mostra que G é solúvel, pois cada H_i/H_{i-1} e $G_i/G_{i-1} \cong (G_i/H)/(G_{i-1}/H)$ é solúvel por hipótese. □

Teorema A.11. Um grupo finito simples é solúvel se, e somente se, ele é cíclico de cardinalidade prima.

Demonstração. ($\Longrightarrow$) Suponha que G seja um grupo finito, simples e solúvel. Então, sua cadeia de grupos cujo quociente é abeliano só pode ser $\langle e\rangle \trianglelefteq G$, visto que não há outros subgrupos normais além destes, ou seja, $G/\langle e\rangle \cong G$ deve ser abeliano. Como G é simples, finito, e abeliano, ele deve ter cardinalidade prima, visto que a recíproca do Teorema de Lagrange é verdadeira para grupos abelianos, então se G não tivesse cardinalidade prima, ele teria um subgrupo não trivial normal, pois todo subgrupo é normal em um grupo abeliano.

($\Longleftarrow$) Nesse caso, G deve ser isomorfo a $\mathbb{Z}/p\mathbb{Z}$ para algum p primo, que é solúvel pois é abeliano. □

Teorema A.12. A_5 é um grupo simples

Demonstração. Suponha que A_5 tenha um subgrupo normal próprio não trivial H, então, por Lagrange, a cardinalidade de H deve um

dos números $2, 3, 4, 5, 6, 10, 12, 15, 20, 30$, já que esses são os divisores de $|A_5| = 60$. É simples verificar que A_5 tem 24 elementos de ordem 5, 20 elementos de ordem 3 e nenhum elemento de ordem 15, a partir desse fato, não podemos ter que $|H| = 3, 6, 12$ ou 15, visto que nesse caso $|A_5/H|$ teria cardinalidade relativamente prima a 3, portanto, H deveria conter todos os elementos de ordem 3, o que é um absurdo. Similarmente, se $|H| = 5, 10$ ou 20, $|A_5/H|$ seria relativamente primo a 5, portanto, H deveria conter todos os 20 elementos de ordem 5, também um absurdo. Se $|H| = 30$, então $|A_5/H|$ seria relativamente primo a 3 e 5, portanto, H deveria conter todos os 44 elementos de ordem 3 e 5, absurdo novamente. Se $|H| = 2$ ou 4, então $|A_5/H| = 30$ ou 15, mas nos dois casos A_5/H deveria ter um elemento de ordem 15, pelo primeiro Teorema de Sylow, que por sua vez implica que A_5 deveria ter um elemento de ordem 15, o que é um absurdo. Logo A_5 não pode ter subgrupos normais além do trivial e o próprio A_5. □

Teorema A.13. *S_n não é solúvel para $n \geq 5$.*

Demonstração. Se S_5 fosse solúvel, A_5 também seria, pelo Teorema A.4, e como A_5 é simples, pelo teorema anterior, deveríamos ter pelo Teorema A.11 que A_5 é cíclico de ordem prima, mas isso é claramente um absurdo. No caso geral, basta notar que todo S_n possui um subgrupo isomorfo a S_5 (escolha 5 elementos dos n e considere todas as ermutadações que permutam apenas os 5 elementos escolhidos), e como S_5 não é solúvel, S_n também não pode ser. □

APÊNDICE B – POLINÔMIOS SIMÉTRICOS

Nesse apêndice desenvolvemos a teoria necessária sobre polinômios simétricos para a dedução das fórmulas de resolução de equações de grau 2 e 3, vistas no Capítulo 6. Veremos aqui, como principal resultado, o Teorema das Funções Simétricas, e o algoritmo utilizado para obter as expressões em termos dos polinômios simétricos durante a dedução das fórmulas.

Definição B.1. Um polinômio $f(x_1, \ldots, x_n) \in K[x_1, \cdots, x_n]$, onde K é um corpo (poderia também ser um anel comutativo com unidade) é dito ser um polinômio simétrico se ele é fixo sobre a ação de S_n sobre os coeficientes, ou seja, para qualquer $\sigma \in S_n$, $f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$, denotaremos esse último polinômio, também, como f^σ.

Sempre que o contexto deixar claro, omitiremos o argumento do polinômio, escrevendo apenas f ao invés de $f(x_1, \cdots, x_n)$, por exemplo.

Exemplo B.2. Alguns exemplos de polinômios simétricos são

$$x_1^2x_2^2x_3 + x_1^2x_2x_3^2 + x_1x_2^2x_3^2 + 5x_1x_2x_3 + x_1^2 + x_2^2 + x_3^2,$$

$$x_1^3 + x_2^3 + x_3^3 + 3x_1x_2x_3 + 2x_1x_2 + 2x_1x_3 + 2x_2x_3.$$

Definição B.3. Seja $(k_1, \cdots, k_n) \in \mathbb{Z}_+^n$ uma n-upla e

$$\mathcal{P} = \{(k_{\sigma(1)}, \ldots, k_{\sigma(n)}) : \sigma \in S_n\}$$

o conjunto de suas permutações distintas. Então

$$m_{(k_1,\ldots,k_n)}(x_1, \ldots, x_n) = \sum_{(i_1,\ldots,i_n)\in\mathcal{P}} x_1^{i_1} \cdots x_n^{i_n}$$

Exemplo B.4. Os polinômios do primeiro exemplo podem ser reescritos, respectivamente, da seguinte forma

$$m_{(2,2,1)} + 5m_{(1,1,1)} + m_{(2,0,0)},$$

$$m_{(3,0,0)} + 3m_{(1,1,1)} + 2m_{(1,1,0)}.$$

Esses polinômios recebem esse nome pois, como veremos mais adiante, o Teorema das Funções Simétricas nos garante que todo polinômio simétrico em anel polinomial pode ser escrito em função dos polinômios simétricos elementares.

Exemplo B.5. Alguns exemplos de polinômios simétricos monomiais são

$$m_{(3,3,3)} = x_1^3 x_2^3 x_3^3,$$

$$m_{(5,0,0)} = x_1^5 + x_2^5 + x_3^5,$$

$$m_{(3,2,2)} = x_1^3 x_2^2 x_3^2 + x_1^2 x_2^3 x_3^2 + x_1^2 x_2^2 x_3^3,$$

$$m_{(5,2,1)} = x_1^5 x_2^2 x_3^1 + x_1^5 x_2^1 x_3^2 + x_1^2 x_2^5 x_3^1 + x_1^2 x_2^1 x_3^5 + x_1^1 x_2^5 x_3^2 + x_1^1 x_2^2 x_3^5.$$

A vantagem de definir os polinômios monomiais dessa forma é que eles pode ser usados para escrever os polinômios simétricos gerais em sua função, como veremos nos próximos exemplos e teoremas.

Teorema B.6. Todo polinômio simétrico pode ser escrito como uma combinação linear única dos polinômios simétricos monomiais.

Demonstração. Seja $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ um polinômio simétrico qualquer, provaremos o teorema por indução na quantidade de termos de f. Se f tem apenas um termo, então necessariamente $f(x_1, \ldots, x_n) = ax_1^k \cdots x_n^k$ para algum $a \in K$ e $k \in \mathbb{Z}_+$, visto que esse é claramente o único formato possível para um polinômio simétrico com apenas um termo. Nesse caso, temos simplesmente que $f = am_{(k,\ldots,k)}$.

Suponha agora que f tenha uma quantidade arbitrária de termos, e seja $ax_1^{k_1} \cdots x_n^{k_n}$ o termo de maio grau (sob a ordenação lexicográfica dos expoentes) de f, então, para qualquer $\sigma \in S_n$, $ax_1^{k_{\sigma(1)}} \cdots x_n^{k_{\sigma(n)}}$ será um termo de $f^\sigma = f$, ou seja, $m_{(k_1,\cdots,k_n)}$ é composto apenas por termos de f, assim $f - am_{(k_1,\cdots,k_n)}$ é simétrico e tem, definitivamente, menos termos que f, todos com expoentes 'menores' na ordem lexicográica que o maior termo de $am_{(k_1,\cdots,k_n)}$ (note que mostramos que $am_{(k_1,\cdots,k_n)}$ é necessariamente o único polinômio simétrico monomial com tal propriedade), assim, pela hipótese de indução, $f - am_{(k_1,\cdots,k_n)} = a_1m_1 + \cdots + a_pm_p$ onde os $a_i \in K$ e os m_i são polinômios simétricos monomiais, todos únicos a menos de permutação pela hipótese de indução, logo $f = am_{(k_1,\cdots,k_n)} + a_1m_1 + \cdots + m_p$, o que completa o resultado. □

Perceba que o resultado acima nos dá um algoritmo geral para o cálculo de tal expressão em termos dos polinômios simétricos monomiais.

A família mais importante de polinômios simétricos, porém, são os polinômios simétricos elementares.

Definição B.7. O polinômio

$$e_i(x_1, \ldots, x_n) = \sum_{1 \le j_1 < \cdots < j_i \le n} x_{j_1} \cdots x_{j_i}$$

é dito ser um polinômio simétrico elementar.

Eles recebem esse nome pois, de uma certa forma, eles são os 'únicos' polinômios elementares, qualquer outro polinômio simétrico pode ser escrito em função dos polinômios elementares, esse é o chamado 'Teorema das Funções Simétricas', que provaremos a diante.

Perceba que esses polinômios são um caso particular dos polinômios monomiais, visto que $e_i(x_1, \ldots, x_n) = m_{(1,\ldots,1,0,\ldots,0)}$, onde há n 1's no subscrito de m.

Como um exemplo, veremos como podemos escrever os polinômio monomiais em termos dos polinômios elementares

Exemplo B.8. Vamos calcular alguns dos polinômios monomiais em termos dos polinômios simétricos. O primeiro polinômio monomial seria $m_{(1,0,0)}$, que é claramente igual a $e_1 = e_1(x_1, x_2, x_3)$. Os polinômios monomiais de grau 2 são mais interessantes, temos $m_{(1,1,0)}$, que é igual a e_2, e $m_{(2,0,0)} = x_1^2 + x_2^2 + x_3^2$, para calcular esse em termos dos polinômios elementares, a ideia é primeiro juntar os polinômios simétricos elementares de tal forma que eles possam ser escritos em termos de $m_{(2,0,0)}$ e outros polinômios monomiais de ordem menor, e depois 'reverter' o processo utilizando as expressões encontradas para os polinômios monomiais de ordem menor em termos dos polinômios elementares. Nesse caso, podemos fazer isso elevando e_1 ao quadrado

$$e_1^2 = (x_1 + x_2 + x_3)(x_1 + x_2 + x_3).$$

Poderíamos facilmente expandir essa expressão diretamente, mas também podemos tomar vantagem da simetria dessa expressão para escrevê-la em termos dos polinômios monomiais sem grande esforço algébrico. Por exemplo, o termo x_1^2 aparece apenas uma vez nessa expansão, portanto x_2^2 e x_3^2 também, e assim $m_{(2,0,0)}$ aparecerá com coeficiente 1 na expansão, similarmente, x_1x_2 aparece duas vezes na expansão dos termos, portanto $2x_1x_2$, $2x_1x_3$ e $2x_2x_3$ serão termos desse polinômio quando expandido, o que corresponde a $2m_{(1,1,0)}$, e assim $e_1^2 = m_{(2,0,0)} + 2m_{(1,1,0)}$. Como $m_{(1,1,0)} = e_2$, temos, então, que $m_{(2,0,0)} = x_1^2 + x_2^2 + x_3^2 = e_1^2 - 2e_2$.

Para finalizar o exemplo, vamos calcular os polinômios simétricos monomiais de grau 3 em termos dos polinômios simétricos elementares. Claramente $m_{(1,1,1)} = e_3$, restam, então, $m_{(2,1,0)}$ e $m_{(3,0,0)}$. Para calcular $m_{(2,1,0)}$, considere a seguinte expressão.

$$e_1e_2 = (x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) = m_{(2,1,0)} + 3m_{(1,1,1)}.$$

O termo $m_{(2,1,0)}$ corresponde ao fato de que o termo $x_1^2x_2$ aparece apenas uma vez na expansão, e o termo $3m_{(1,1,1)}$ corresponde ao fato de que $x_1x_2x_3$ aparece três vezes na expansão. Como $m_{(1,1,1)} = e_3$, temos, então, que

$$x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2 = e_1e_2 - 3e_3.$$

Então, o polinômio simétrico monomial $m_{(3,0,0)}$ pode ser obtido elevando e_1 ao cubo, assim

$$(x_1 + x_2 + x_3)^3 = m_{(3,0,0)} + 3m_{(2,1,0)} + 6m_{(1,1,1)}.$$

Os termos à direita, novamente, correspondem a quantidade de vezes que x_1^3, $x_1^2x_2$ e $x_1x_2x_3$ aparecem na expansão do polinômio à esquerda, assim, utilizando as expressões que temos até então para $m_{(2,1,0)}$ e $m_{(1,1,1)}$, temos que

$$\begin{aligned} e_1^3 &= m_{(3,0,0)} + 3(e_1e_2 - 3e_3) + 6e_3 \\ \implies x_1^3 + x_2^3 + x_3^3 &= e_1^3 - 3e_1e_2 + 3e_3. \end{aligned}$$

Perceba que calcular dessa forma é bem mais prático que verificar tradicionalmente que essa equação é verdadeira, visto que expandir o lado direito da equação não seria nada divertido.

Exemplo B.9. Em geral $m_{(i+1,\ldots,i+1,i,\ldots,i)} = e_je_n^i$ (n variáveis), onde j é a quantidade de $i+1$'s no índice. De fato, basta verificar que e_je_n terá $\binom{n}{j}$ termos, todos de grau $ni + j$, um para cada escolha de j expoentes que serão uma unidade maior que os demais, que é precisamente o polinômio $m_{(i+1,\ldots,i+1,i,\ldots,i)}$.

Vamos formalizar o algoritmo visto no exemplo acima, assim, mostrando o Teorema das Funções Simétricas.

Teorema B.10. Todo polinômio simétrico monomial pode ser escritos como expressão polinomial dos polinômios simétricos elementares.

Demonstração. Seja m um polinômio simétrico monomial qualquer de n variáveis e de grau k, vamos provar que m pode ser escrito em termos dos polinômios simétricos elementares por meio de indução no seu índice, sob a ordem lexicográfica, que é uma ordem total que cobre todos os índices possível dado um grau fixo. O menor polinômio simétrico monomial sob a ordem lexicográfica (assumindo ordem decrescente no índice, sem perda de generalidade) é da forma $m_{(i+1,\dots,i+1,i,\dots,i)} = e_j e_n^i$, onde j é a quantidade de $i+1$'s, pelo exemplo anterior, logo o teorema é verdadeiro nesse caso.

Assuma então que $m = m_{(k_1,\dots,k_n)}$ para algum índice qualquer (com $k_1 \geq \cdots \geq k_n$, sem perda de generalidade), então m será o polinômio simétrico monomial de maior índice na combinação linear correspondente a $f = e_1^{k_1-k_2} e_2^{k_2-k_3} \cdots e_{n-1}^{k_{n-1}-k_n} e_n^{k_n}$, visto que o elemento de maior expoente na ordem lexicográfica desse polinômio será precisamente $x_1^{k_1} \cdots x_n^{k_n}$ (para verificar isso, basta multiplicar o termo de maior ordem lexicográfica nos expoentes de cada fator). Assim, $f - m = a_1 m_1 + \cdots + a_p m_p$ para algum conjunto de $a_i \in K$ e polinômios simétricos monomiais m_i com índices de ordem lexicográfica menor que n, portanto $m = f - a_1 m_1 + \cdots + a_p m_p$, e aplicando a hipótese de indução em cada um dos m_i's, segue o resultado. □

Como consequência, temos o importante teorema das funções simétricas, já mencionado.

Teorema B.11. Todo polinômio simétrico pode ser escrito em termos de uma expressão polinomial dos polinômios simétricos elementares (assumindo a mesma quantidade de variáveis nos polinômios simétricos elementares).

Demonstração. Ora, todo polinômio simétrico pode ser escrito como uma combinação linear dos polinômios simétricos monomiais, pelo Teorema B.6, e estes, por sua vez, podem ser escritos em função dos

polinômios simétricos elementares, pelo Teorema B.10, o que conclui o teorema. □