



Universidade Federal de Goiás
Instituto de Matemática e Estatística
Programa de Mestrado Profissional em
Matemática em Rede Nacional



Equações Polinomiais: da Equação de 1º Grau à Teoria de Galois

Daniell Ferreira de Oliveira

Goiânia

2017

**TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS
DE TESES E
DISSERTAÇÕES NA BIBLIOTECA DIGITAL DA UFG**

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFMG), regulamentada pela Resolução CEPEC nº 832/2007, sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou *download*, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: **Dissertação** **Tese**

2. Identificação da Tese ou Dissertação:

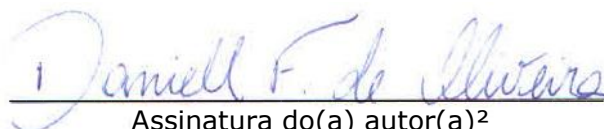
Nome completo do autor: Daniell Ferreira de Oliveira

Título do trabalho: Equações Polinomiais: da Equação do 1º grau à Teoria de Galois

3. Informações de acesso ao documento:

Concorda com a liberação total do documento SIM NÃO¹

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF da tese ou dissertação.


Assinatura do(a) autor(a)²

Ciente e de acordo:


Assinatura do(a) orientador(a)²

Data: 23 / 06 /2017

¹ Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.

Casos de embargo:

- Solicitação de registro de patente
- Submissão de artigo em revista científica
- Publicação como capítulo de livro
- Publicação da dissertação/tese em livro

²A assinatura deve ser escaneada.

Daniell Ferreira de Oliveira

Equações Polinomiais: da Equação de 1º Grau à Teoria de Galois

Trabalho de Conclusão de Curso apresentado ao Instituto de Matemática e Estatística da Universidade Federal de Goiás, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Área de Concentração: Matemática do Ensino Básico

Orientadora: Prof^a. Dr^a. Ivonildes Ribeiro Martins Dias

Goiânia

2017

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Ferreira de Oliveira, Daniell
Equações Polinomiais: da Equação de 1º Grau à Teoria de Galois
[manuscrito] / Daniell Ferreira de Oliveira. - 2017.
105 f.: il.

Orientador: Prof. Dr. Ivonildes Ribeiro Martins Dias .
Dissertação (Mestrado) - Universidade Federal de Goiás, Instituto
de Matemática e Estatística (IME), Programa de Pós-Graduação em
Matemática, Goiânia, 2017.

Bibliografia.

Inclui símbolos, tabelas, lista de figuras.

1. Equações Polinomias. 2. Galois. 3. Grupos. I. , Ivonildes Ribeiro
Martins Dias, orient. II. Título.

CDU 512.5

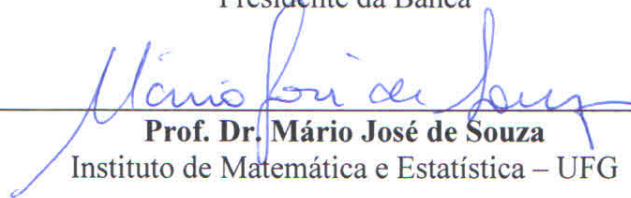
Daniell Ferreira de Oliveira

“Equações Polinomiais: da equação de 1º grau à teoria de Galois”

Trabalho de Conclusão de Curso defendido no Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT/UFG, do Instituto de Matemática e Estatística da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Mestre em Matemática, área de concentração Matemática do Ensino Básico, aprovado no dia 30 de maio de 2017, pela Banca Examinadora constituída pelos seguintes professores:



Profa. Dra. Ivonildes Ribeiro Martins Dias
Instituto de Matemática e Estatística – UFG
Presidente da Banca



Prof. Dr. Mário José de Souza
Instituto de Matemática e Estatística – UFG

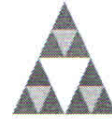


Prof. Dr. Flávio Raimundo de Souza
Membro Externo – IFG/Goiânia




Universidade Federal de Goiás - UFG
Instituto de Matemática e Estatística - IME
Mestrado Profissional em Matemática
em Rede Nacional – PROFMAT/UFG

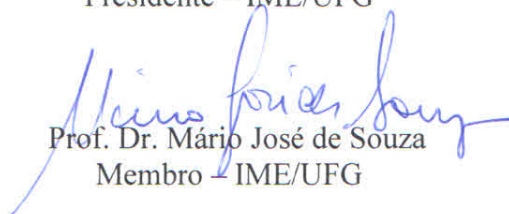
Campus Samambaia – Caixa Postal 131 – CEP: 74.001-970 – Goiânia-GO.
Fones: (62) 3521-1208 e 3521-1137 www.ime.ufg.br



PROFMAT

Ata da reunião da banca examinadora da defesa de Trabalho de Conclusão de Curso do aluno Daniell Ferreira de Oliveira – Aos trinta dias do mês de maio do ano de dois mil e dezessete, às 14:00 horas, reuniram-se os componentes da Banca Examinadora: Profa. Dra. Ivonildes Ribeiro Martins Dias – Orientadora, Prof. Dr. Mário José de Souza – IME/UFG e Prof. Dr. Flávio Raimundo de Souza – IFG/Goiânia, para, sob a presidência da primeira, e em sessão pública realizada no auditório do IME, procederem a avaliação da defesa intitulada **“Equações Polinomiais: da equação de 1º grau à teoria de Galois”**, em nível de mestrado, área de concentração Matemática do Ensino Básico, de autoria de Daniell Ferreira de Oliveira, discente do Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal de Goiás. A sessão foi aberta pela presidente da banca, Profa. Dra. Ivonildes Ribeiro Martins Dias, que fez a apresentação formal dos membros da banca. A seguir, a palavra foi concedida ao autor do TCC que, em 30 minutos, procedeu à apresentação de seu trabalho. Terminada a apresentação, cada membro da banca arguiu o examinando, tendo-se adotado o sistema de diálogo sequencial. Terminada a fase de arguição, procedeu-se à avaliação da defesa. Tendo em vista o que consta na Resolução nº. 1075/2012 do Conselho de Ensino, Pesquisa, Extensão e Cultura (CEPEC), que regulamenta os Programas de Pós-Graduação da UFG, e procedidas as correções recomendadas, o trabalho foi **APROVADO** por unanimidade, considerando-se integralmente cumprido este requisito para fins de obtenção do título de **MESTRE EM MATEMÁTICA**, na área de concentração Matemática do Ensino Básico pela Universidade Federal de Goiás. A conclusão do curso dar-se-á quando da entrega, na secretaria do IME, da versão definitiva do trabalho, com as devidas correções supervisionadas e aprovadas pelo orientador. Cumpridas as formalidades de pauta, às 15:00 horas, a presidência da mesa encerrou a sessão e, para constar, eu, Chaiane de Medeiros Rosa, secretária do PROFMAT/UFG, lavrei a presente ata que, após lida e aprovada, segue assinada pelos membros da Banca Examinadora em quatro vias de igual teor.


Profa. Dra. Ivonildes Ribeiro Martins Dias
Presidente – IME/UFG


Prof. Dr. Mário José de Souza
Membro – IME/UFG


Prof. Dr. Flávio Raimundo de Souza
Membro – IFG/Goiânia

Todos os direitos reservados. É proibida a reprodução total ou parcial deste trabalho sem a autorização da universidade, do autor e do orientador.

Daniell Ferreira de Oliveira graduou-se em Licenciatura em Matemática pela Universidade Federal de Goiás (Campus de Goiânia) em 2006, especializou-se em Estatística pela Universidade Federal de Lavras-MG em 2008, atualmente é professor do Ensino Básico nas redes pública e privada em Goiânia e também no Ensino Superior em instituição privada do mesmo município.

Dedico este trabalho à minha família e aos amigos que me apoiaram e compreenderam os momentos de ausência.

Agradecimentos

Agradeço primeiramente à Deus pela vida, saúde e disposição. Aos meus familiares pelo apoio incondicional. Em especial à minha esposa Jaqueline por entender os momentos de ausência. À prof^a. Dr^a. Ivonildes pelas orientações ministradas e a todos os professores do PROFMAT-UFG que contribuíram imensamente com seus ensinamentos.

Resumo

Este trabalho tem como objetivo aperfeiçoar a compreensão de professores de Matemática no que tange à solução de equações polinomiais por meio de radicais, com enfoque na Teoria de Galois. O leitor encontra neste, um pouco da história da vida de Galois, as resoluções por radicais de equações de grau $n \leq 4$, as teorias de grupos, anéis e corpos, bem como a Teoria de Galois.

Palavras-chave

Equações Polinomiais. Galois. Grupos.

Abstract

This paper aims to improve the understanding of Mathematics teachers regarding the solution of polynomial equations by means of radicals, focusing on the theory of Galois. The reader find in this document a little of Galois's life story, radical resolutions of degree $n \leq 4$ equations, group, ring and body theories, as well as Galois Theory.

Keywords

Polynomial Equations. Galois. Groups.

Lista de Figuras

1.1	Quadrado da Soma de Dois Termos	5
1.2	Évariste Galois (1811 - 1832)	12
2.1	Homomorfismo de Grupos	20
2.2	Quadrado Q	27
2.3	Diagrama: Anel dos Quatérnios	33
3.1	Reticulado de Subgrupos	75
3.2	Reticulado de Corpos Intermediários	77
3.3	Reticulado de Subgrupos D_4	82
3.4	Reticulado de Corpos Intermediários D_4	84

Sumário

Resumo	i
Abstract	ii
Lista de Figuras	iii
Introdução	1
1 A História das Equações e da Vida de Galois	3
1.1 A Equação de 1º Grau	4
1.2 A Equação de 2º Grau	4
1.3 A Equação de 3º Grau	6
1.4 A Equação de 4º Grau	10
1.5 Equações de Grau Maior do que 4	11
1.6 A vida de Evariste Galois	11
2 Grupos, Subgrupos, Anéis e Corpos	14
2.1 Grupos e Subgrupos	14
2.1.1 Grupos	14
2.1.2 Gerador de um Grupo	15
2.1.3 Exemplos de Grupos Abelianos	15
2.1.4 Subgrupos	16
2.1.5 Classe Lateral	18
2.1.6 Subgrupo Normal	19
2.1.7 Grupo Quociente	19
2.1.8 Homomorfismo de Grupos	20
2.1.9 Grupos de Permutações	24

2.1.10	Grupos Diedrais	26
2.2	Anéis	29
2.2.1	Definições e Exemplos	29
2.2.2	Homomorfismo de Anéis	34
2.3	O Corpo de Fração de um Anel de Integridade	37
2.4	Anéis de Polinômios	39
2.5	Polinômios sobre o Corpo Racional	45
2.6	Extensões de Corpos	47
3	Raízes de Polinômios e a Teoria de Galois	53
3.1	Raízes de Polinômios	53
3.2	Os Elementos da Teoria de Galois	61
3.3	Exemplos Utilizando a Teoria de Galois	71
3.4	Resolução por Radicais	85
3.4.1	A Insolubilidade do Polinômio Geral de Grau $n \geq 5$	87
	Considerações Finais	89
	Referências Bibliográficas	90

Introdução

O estudo de equações polinomiais se faz presente na vida escolar dos estudantes desde muito cedo. No Brasil, em geral, os alunos começam a estudar equações de 1º grau no 7º ano, por volta dos 12 anos de idade. No 8º ano aprimoram o estudo de expressões algébricas, para no 9º ano conhecerem métodos para resolver equações de 2º grau e também as de 4º grau do tipo biquadradas. Quando vão para o Ensino Médio é esperado que eles dominem a resolução de equações de 1º e 2º grau para assim aprenderem alguns métodos de resolução de equações polinomiais de graus superiores. Apesar do uso exaustivo de equações a partir do 7º ano, pouco se fala sobre a história de como ocorreu o desenvolvimento das formas de resolução que utilizamos hoje.

Pensando nisso, este trabalho visa aprimorar os conhecimentos de professores de Matemática do Ensino Básico referentes à resolução de equações polinomiais, bem como ampliar tal conhecimento fazendo o estudo de grupos, corpos, anéis e da Teoria de Galois.

No capítulo 1 abordamos histórias relacionadas à resoluções de equações de 1º a 4º grau escritas na forma geral, mostramos o desenvolvimento das fórmulas resolutivas dessas equações, expomos os estudiosos que tentaram desenvolver fórmulas resolutivas para equações de grau maior do que 4 e finalizamos o capítulo com a história da vida de Evariste Galois, um importante teórico para álgebra moderna.

Já no capítulo 2 apresentamos definições e propriedades envolvendo grupos, subgrupos, anéis e corpos, falamos sobre homomorfismo, grupos de permutação e grupos diedrais, procurando exemplificar todos os casos possíveis. Nas Seções 2.4 e 2.5, abordamos conceitos envolvendo polinômios e terminamos o capítulo discorrendo sobre Extensões de Corpos.

Trouxemos no início do capítulo 3 conceitos e propriedades envolvendo raízes de polinômios, aprimorando o caminho para o estudo da teoria que trata da solubilidade de equações de grau maior do que 4 por meio de radicais. Posteriormente, apresentamos

à Teoria de Galois e dois exemplos envolvendo-a. No final deste capítulo, tratamos da insolubilidade de uma equação polinomial geral de grau $n \geq 5$.

Capítulo 1

A História das Equações e da Vida de Galois

De acordo com [1], a primeira referência de resolução de equações que se têm notícias está no papiro de Rhind, escrito pelos egípcios a cerca de 1650 a.C.. Como esses povos não utilizavam a notação algébrica para resolver equações, há relatos de que eles as resolviam através de métodos complexos e cansativos. Já os gregos, em meados do século III d.C., solucionavam suas equações através de Geometria e, nesse contexto, Diofanto de Alexandria se destacou contribuindo para elaboração de conceitos teóricos e práticos para a resolução de equações. Conta a história que na lápide do túmulo de Diofanto foi escrita a seguinte equação que relata a idade com que faleceu, no caso 84 anos.

“Aqui jaz Diofanto. Maravilhosa habilidade. Pela arte da álgebra a lápide nos diz sua idade: Deus deu um sexto da vida como infante, um duodécimo mais como jovem, de barba abundante; e ainda uma sétima parte antes do casamento; em cinco anos nasce-lhe o rebento. Lastima! O filho do mestre e sábio do mundo se vai. Morreu quando da metade da idade final do pai. Quatro anos a mais de estudos consolam-no do pesar; Para então, deixando a terra, também ele alívio encontrar.”

No século IX d.C. os árabes promoveram o progresso na resolução das equações, onde para representar valores desconhecidos o chamavam de “coisa”, palavra que é pronunciada em árabe como *xay*. Talvez seja por isso que até hoje a letra x seja a mais

utilizada como incógnita nas equações em geral.

O árabe Al-Khowarizmi, considerado o matemático árabe de maior expressão daquela época, resolveu e discutiu equações de vários tipos, sendo que em um de seus livros, o Al-jabr wa-1 mugābalaḥ, encontra-se algumas explicações claras sobre resoluções de equações.

Foi no século XVI d.C. que as equações passaram a ser escritas com símbolos matemáticos e letras. O francês François Viète foi quem introduziu essa forma de escrever equações, sendo inclusive considerado o “pai da Álgebra”. Viète estudou as equações através de expressões gerais como $ax + b = 0$.

No decorrer do trabalho falamos sobre resolução de equações por meio de radicais, isso quer dizer que as resoluções devem ser expostas utilizando apenas os coeficientes das equações e as operações de adição, subtração, multiplicação, divisão, potenciação e radiciação. A maioria das deduções de fórmulas resolutivas de equações polinomiais a seguir podem também ser encontradas em [3].

1.1 A Equação de 1º Grau

A equação algébrica de primeiro grau, escrita da forma moderna, $ax + b = 0$, onde x é a incógnita e a e b são números reais e $a \neq 0$, tem como solução $x = -\frac{b}{a}$. Essa solução é obtida fazendo operações válidas em ambos os membros da igualdade, afim de conservá-la. Ou seja,

$$ax + b = 0 \Leftrightarrow ax + b - b = 0 - b \Leftrightarrow ax = -b \Leftrightarrow \frac{ax}{a} = \frac{-b}{a} \Leftrightarrow x = \frac{-b}{a}.$$

1.2 A Equação de 2º Grau

Segundo [8], as equações de 2º grau são atualmente resolvidas através de uma expressão atribuída ao indiano Bháskara. Mas existiram outros povos que também desenvolveram métodos para solucionar equações desse tipo. Antes de Cristo, os Babilônios e os Egípcios utilizam símbolos e textos para resolver equações de 2º grau, enquanto os gregos conseguiram concluir suas resoluções utilizando-se de métodos geométricos. Não só Bháskara, mas também os indianos Shidhara e Bramagupta contribuíram com o estudo da resolução de equações de 2º grau, sendo Shidhara o primeiro a indicar

uma fórmula para resolver equações biquadradas. Os árabes foram representados por Al-Khowarizmi, que fez representações geométricas influenciado por Euclides e desenvolveu um método geométrico para resolver equações desse tipo. Mas foi o francês Viète que modernizou a escrita algébrica da resolução de uma equação de 2º grau $ax^2 + bx + c = 0$, cujos coeficientes a , b e c são números reais e $a \neq 0$, a qual utilizamos até hoje. Isto é,

$$x = \frac{-b \pm \sqrt{b^2 - 4.a.c}}{2a}.$$

A dedução da fórmula acima pode ser obtida através da utilização de procedimentos algébricos válidos e o produto notável conhecido como quadrado da soma de dois termos, dado por

$$(a + b)^2 = a^2 + 2ab + b^2.$$

Para $a > 0$ e $b > 0$, o quadrado da soma é ilustrado geometricamente através da figura abaixo.

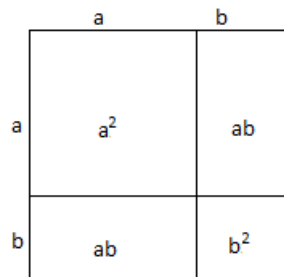


Figura 1.1: Quadrado da Soma de Dois Termos

Dedução da fórmula de resolução da equação de 2º grau. Iniciando a partir da equação de segundo grau, $ax^2 + bx + c = 0$, dividimos ambos os membros da igualdade por a ,

$$\frac{ax^2 + bx + c}{a} = \frac{0}{a} \Leftrightarrow x^2 + \frac{b}{a}x + \frac{c}{a} = 0.$$

Completamos quadrado para aparecer o trinômio quadrado perfeito, que ao ser fatorado torna-se o produto notável quadrado da soma de dois termos. Para isso, somamos e subtraímos $\frac{b^2}{4a^2}$.

$$x^2 + \frac{b}{a}x + \frac{b^2}{4a^2} - \frac{b^2}{4a^2} + \frac{c}{a} = 0 \Leftrightarrow \left(x^2 + \frac{b}{a}x + \frac{b^2}{4a^2}\right) - \frac{b^2}{4a^2} + \frac{c}{a} = 0 \Leftrightarrow$$

$$\Leftrightarrow \left(x + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a} = 0.$$

Somamos $\frac{b^2}{4a^2} - \frac{c}{a}$ em ambos os membros da igualdade, obtemos

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

No segundo membro reduzimos os termos ao mesmo denominador. Isto é,

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

Para finalizar, considerando que $b^2 - 4ac$ é positivo, podemos extrair a raiz quadrada de ambos os membros da igualdade, observando que a raiz quadrada pode ter dois resultados, um positivo e outro negativo. Posteriormente, somamos $-\frac{b}{2a}$ também em ambos os membros da igualdade, assim

$$\sqrt{\left(x + \frac{b}{2a}\right)^2} = \pm \sqrt{\frac{b^2 - 4ac}{4a^2}} \Leftrightarrow x + \frac{b}{2a} = \pm \frac{\sqrt{b^2 - 4ac}}{2a} \Leftrightarrow$$

$$\Leftrightarrow x + \frac{b}{2a} - \frac{b}{2a} = -\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2a} \Leftrightarrow x = -\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2a} \Leftrightarrow$$

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

1.3 A Equação de 3º Grau

De acordo com [7], até o fim do século XV a resolução de equações cúbicas não eram conhecidas. Dois matemáticos da Renascença que se dedicaram ao estudo de equações cúbicas foram Nicolo Fontana de Brescia (1500-1557), também conhecido como Tartaglia, e Gerolamo Cardano (1501-1576). Cardano, em seu livro, *Ars Magna*, escreveu que o bolonhês Scipione del Ferro descobrira um método para resolver equações do tipo $x^3 + px = q$, $x^3 = px + q$ e $x^3 + q = px$, com p e q positivos.

O método a seguir foi apresentado por Viète para resolver uma equação de 3º grau. Para mais detalhes veja [3].

Seja F um corpo contendo o corpo dos racionais \mathbb{Q} , ou seja, $F \supset \mathbb{Q}$, definiremos corpos no Capítulo 2, e seja $f(x) = ax^3 + bx^2 + cx + d$ um polinômio de grau 3 cujos coeficientes $a, b, c, d \in F$ e $a \neq 0$, façamos a substituição de x por $y + h$. Assim,

$$f(x) = ax^3 + bx^2 + cx + d$$

torna-se

$$\begin{aligned} f(y+h) &= a(y+h)^3 + b(y+h)^2 + c(y+h) + d \\ f(y+h) &= a(y^3 + 3y^2h + 3yh^2 + h^3) + b(y^2 + 2yh + h^2) + c(y+h) + d \\ f(y+h) &= ay^3 + 3ay^2h + 3ayh^2 + ah^3 + by^2 + 2byh + bh^2 + cy + ch + d \\ f(y+h) &= ay^3 + (3ah+b)y^2 + (3ah^2 + 2bh + c)y + ah^3 + bh^2 + ch + d. \end{aligned}$$

Temos que o coeficiente de y^2 é $3ah + b$. Tomando $h = -\frac{b}{3a}$ e fazendo a divisão da equação $f(y+h) = 0$ por a , obtemos de

$$f(y+h) = ay^3 + (3ah+b)y^2 + (3ah^2 + 2bh + c)y + ah^3 + bh^2 + ch + d$$

que

$$0 = \frac{ay^3}{a} + \frac{(3a(-\frac{b}{3a}) + b)y^2}{a} + \frac{(3a(-\frac{b}{3a})^2 + 2b(-\frac{b}{3a}) + c)y}{a} + \frac{a(-\frac{b}{3a})^3 + b(-\frac{b}{3a})^2 + c(-\frac{b}{3a}) + d}{a}$$

$$0 = y^3 + 0y^2 + \frac{(3a(-\frac{b}{3a})^2 + 2b(-\frac{b}{3a}) + c)}{a}y + \frac{a(-\frac{b}{3a})^3 + b(-\frac{b}{3a})^2 + c(-\frac{b}{3a}) + d}{a}$$

$$0 = y^3 + py + q, \text{ onde}$$

$$p = \frac{(3a(-\frac{b}{3a})^2 + 2b(-\frac{b}{3a}) + c)}{a} \text{ e } q = \frac{a(-\frac{b}{3a})^3 + b(-\frac{b}{3a})^2 + c(-\frac{b}{3a}) + d}{a}.$$

Podemos admitir que $y^3 + py + q = 0$, com $p, q \in F$ é irredutível em F , ou seja, o polinômio não pode ser fatorado como um produto de fatores lineares em F , pois caso

contrário teria uma raiz em F e as demais raízes seriam de um polinômio de grau 2 com coeficientes em F .

Na equação $y^3 + py + q = 0$, substituímos $y = z + \frac{k}{z}$ resultando em:

$$\left(z + \frac{k}{z}\right)^3 + p\left(z + \frac{k}{z}\right) + q = 0$$

$$z^3 + 3z^2\frac{k}{z} + 3z\left(\frac{k}{z}\right)^2 + \left(\frac{k}{z}\right)^3 + pz + p\frac{k}{z} + q = 0$$

$$z^3 + 3zk + 3\frac{k^2}{z} + \frac{k^3}{z^3} + pz + p\frac{k}{z} + q = 0.$$

Para eliminarmos os termos em z e em $\frac{1}{z}$, utilizamos $k = \frac{-p}{3}$. Logo, a substituição $y = z - \frac{p}{3z}$, leva a equação $y^3 + py + q = 0$ na equação $z^3 - \frac{p^3}{27z^3} + q = 0$. De fato,

$$z^3 + 3zk + 3\frac{k^2}{z} + \frac{k^3}{z^3} + pz + p\frac{k}{z} + q = 0$$

$$z^3 + 3z\left(\frac{-p}{3}\right) + 3\frac{\left(\frac{-p}{3}\right)^2}{z} + \frac{\left(\frac{-p}{3}\right)^3}{z^3} + pz + p\frac{\left(\frac{-p}{3}\right)}{z} + q = 0$$

$$z^3 - zp + \frac{p^2}{3z} - \frac{p^3}{27z^3} + pz - \frac{p^2}{3z} + q = 0$$

$$z^3 - \frac{p^3}{27z^3} + q = 0.$$

Multiplicando ambos os membros da igualdade por z^3 , obtemos

$$z^3 \cdot \left(z^3 - \frac{p^3}{27z^3} + q\right) = 0$$

$$z^6 - \frac{p^3}{27} + qz^3 = 0.$$

Ou ainda,

$$z^6 + qz^3 - \frac{p^3}{27} = 0.$$

Substituindo z^3 por t temos

$$t^2 + qt - \frac{p^3}{27} = 0.$$

Assim, chegamos a uma equação quadrática. Logo,

$$t = \frac{-q \pm \sqrt{-D/27}}{2},$$

onde $D = -(4p^3 + 27q^2)$. Mas, como $t = z^3$, temos

$$z^3 = \frac{-q \pm \sqrt{-D/27}}{2}.$$

Tomando $z_1^3 = \frac{-q + \sqrt{-D/27}}{2}$ e $z_2^3 = \frac{-q - \sqrt{-D/27}}{2}$ observamos que $(z_1 z_2)^3 = -\frac{p^3}{27}$, o que resultaria em $z_1 z_2 = -\frac{p}{3} \omega$, onde ω é a raiz cúbica da unidade.

De acordo com Iezzi [6], para um número complexo $z = r(\cos(\theta) + i\text{sen}(\theta))$, chamamos de *raiz n -ésima* de z e denotamos de $\sqrt[n]{z}$, a um número complexo z_k tal que $z_k^n = z$. Ou seja,

$$\sqrt[n]{z} = z_k \Leftrightarrow z_k^n = z.$$

No caso da raiz n -ésima de z a fórmula geral é dada pela segunda fórmula de Moivre,

$$z_k = \sqrt[n]{r} \left(\cos \frac{\theta + 2k\pi}{n} + i\text{sen} \frac{\theta + 2k\pi}{n} \right).$$

Assim, a raiz n -ésima da unidade a fórmula geral fica reduzida a:

$$\omega_k = \cos \frac{2k\pi}{n} + i\text{sen} \frac{2k\pi}{n}.$$

Ou ainda, para $k = 1$, tem-se

$$\omega = \cos \frac{2\pi}{n} + i\text{sen} \frac{2\pi}{n}.$$

Usando essa fórmula, obtemos que as raízes n -ésimas da unidade são dadas por $1, \omega, \omega^2, \dots, \omega^{n-1}$.

Em nosso caso, como $n = 3$, temos $\omega = \cos \frac{2\pi}{3} + i\text{sen} \frac{2\pi}{3} \in \mathbb{C}$ e trocando, z_2 por ωz_2 ou $\omega^2 z_2$ se necessário, concluimos que $z_1 \cdot z_2 = -\frac{p}{3}$ e as raízes cúbicas da equação $y^3 + py + q = 0$ são:

$$y_1 = z_1 + z_2, y_2 = \omega z_1 + \omega^2 z_2 \text{ e } y_3 = \omega^2 z_1 + \omega z_2.$$

Deste modo,

$$y_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}},$$

$$y_2 = \omega \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \omega^2 \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}},$$

$$y_3 = \omega^2 \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \omega \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}.$$

1.4 A Equação de 4º Grau

De modo semelhante, veja [3], a equação de 4º grau do tipo $ax^4 + bx^3 + cx^2 + dx + e = 0$ pode ser reduzida a uma equação do tipo

$$y^4 + py^2 + qy + r = 0$$

Utilizando argumentos que a priori foram utilizados por Descartes, escolhamos u , v e w de forma que a equação reduzida acima fique da forma $\left(y^2 + \frac{u}{2}\right)^2 - (vy + w)^2 = 0$, de onde decorrem as seguintes relações:

- i) $p = u - v^2$;
- ii) $q = -2vw$;
- iii) $r = \frac{u^2}{4} - w^2$.

Isolando u na expressão i) temos $u = p + v^2$ e isolando w na expressão ii) encontramos $w = -\frac{q}{2v}$. Fazendo a substituição de u e w em iii) obtemos a seguinte expressão:

$$r = \frac{u^2}{4} - w^2 \Rightarrow r = \frac{(p + v^2)^2}{4} - \left(-\frac{q}{2v}\right)^2 \Rightarrow r = \frac{p^2 + 2pv^2 + v^4}{4} - \frac{q^2}{4v^2}.$$

Multiplicando ambos os membros da igualdade por $4v^2$, temos

$$4v^2r = p^2v^2 + 2pv^4 + v^6 - q^2,$$

donde temos

$$v^6 + 2pv^4 + (p^2 - 4r)v^2 - q^2 = 0.$$

Nos cálculos acima obtemos uma equação cúbica em v^2 . Assim, podemos dizer que uma equação de 4º grau reduz-se a uma cúbica, logo suas raízes também são dadas por uma expressão utilizando radical.

1.5 Equações de Grau Maior do que 4

A questão que surge agora é: será que as equações de grau maior do que 4 também são solúveis por meio de radicais? Conforme [3], muitos foram os estudiosos que pesquisaram o assunto. Dentre eles temos Euler que apesar dos esforços não conseguiu solucionar tal questão, mas encontrou novos métodos para resolver equações de grau 4. Outro teórico que pesquisou sobre o assunto foi Lagrange, que em 1770, observou que os argumentos utilizados para equações de grau 3 e 4 poderiam ser unificados e mostrou que o mesmo não era eficiente para equações de grau 5. Em 1813, Ruffini apresentou uma demonstração da impossibilidade de resolver equações de grau maior que 4 por meio de radicais, porém sua demonstração apresentava muitas imperfeições. Abel, em 1824, conseguiu provar que a equação geral de grau 5 não é solúvel por meio de radicais, no entanto, sua demonstração não deixou especificado se polinômios de grau maior que 5 podem ser solúveis por meio de radicais.

Foi em 1843, através de uma carta direcionada à Academia de Ciências de Paris, que findou-se a procura por tal demonstração. Nela, Joseph Liouville informou que o trabalho deixado por Evariste Galois apresentava um método para decidir se um polinômio de grau maior do que 4 é ou não solúvel por meio de radicais.

1.6 A vida de Evariste Galois

De acordo com [2] e [7], Galois nasceu em Burge-la-Keine, nas proximidades de Paris, em 25 de outubro de 1811, cidade na qual teve seu pai, Nicolas Gabriel Galois,

como prefeito em meados de 1815. Viveu com seus pais até os 12 anos, período no qual teve sua mãe como única professora. Dela herdou o interesse pela ciência e de seu pai absorveu as ideias liberais que estavam em evidência no momento, decorrentes da volta triunfante de Napoleão ao poder. Em 1823 ingressou no Liceu de Douville-Grand, onde, como outros gênios, se interessou muito por determinados assuntos (relacionados à Matemática), no entanto, quando lhe propunham estudos que não eram de seu interesse, ele nem os lia. Aos 15 anos frequentou a disciplina de matemáticas preparatórias, neste período leu toda a geometria de Legendre e estudou a obra de Lagrange, situação que o instigou a investigar sobre a resolução de equações de quinto grau. Em 1827 tentou ingressar pela primeira vez na Escola Politécnica, por onde circulavam os principais matemáticos franceses da época, contudo, seu ingresso foi recusado. No ano seguinte tentou novamente, no entanto, teve o infortúnio de ser avaliado pelo Monsieur Dinet, que novamente o reprovou, uma vez que não entendeu suas ideias e não acreditou nos resultados apresentados. Na ocasião, Dinet discordou de um dos passos apresentados por Galois, que estava correto, e não se safou de levar uma esponja na cara.



Figura 1.2: Évariste Galois (1811 - 1832)

Sucessivas foram as tragédias e confusões na vida de Evariste Galois. Em 1829, ocorreu o suicídio de seu pai após forte briga com inimigos monarquistas. A partir desse momento, Galois tornou-se impetuoso pela causa republicana. Como não teve êxito na Escola Politécnica, ingressou na Escola Normal Superior, porém, em 1831, em razão de suas causas políticas, publicou um ataque ao diretor da instituição, que culminou em sua expulsão. Imediatamente alistou-se na Guarda Nacional, que fora rapidamente desativada pelo decreto do rei Luís Filipe, com o qual costumava travar enfrentamentos, razão que o levou sucessivas vezes à prisão. Na cadeia ficou em estado depressivo, e até tentou suicídio.

Em 1832, pouco antes de sua sentença, houve um surto de cólera na cadeia onde

estava. Por esse motivo, foi transferido para uma casa de saúde, onde conheceria uma mulher que seria a causa de sua morte. Evariste se apaixonou por Stéphanie-Félicie Poterine, filha de um respeitado médico, que era comprometida com um cidadão chamado Pescheux d'Herbinville e que descobriu o interesse de Galois. Como Pescheux era um exímio atirador, desafiou Galois para um duelo.

Percebendo a enrascada que entrara, Galois elaborou, na véspera de seu duelo, um testamento científico, com o intermédio do matemático Chevalier. Reuniu às pressas seus estudos, escrevendo na margem a frase símbolo de seu desespero: *“não tenho tempo, não tenho tempo”*.

No dia 30 de maio de 1832, pela manhã, Galois foi ao duelo. Alvejado, ficou no hospital até o dia seguinte, quando morreu. Mal sabia ele que deixaria em 60 páginas um legado para a Matemática, em especial para a Álgebra Moderna, e seria mais tarde considerado um dos mais criativos pensadores que a ciência já teve.

Capítulo 2

Grupos, Subgrupos, Anéis e Corpos

Neste capítulo apresentamos algumas definições que são fundamentais para o entendimento da Teoria de Galois. Para um aprofundamento no estudo de grupos, subgrupos, anéis e corpos veja [3], [4] e [5].

2.1 Grupos e Subgrupos

A estrutura de grupos é uma das mais importantes estruturas algébricas da Matemática. Seguem nesta seção algumas definições e propriedades relevantes sobre grupos, subgrupos, corpos, homomorfismo, dentre outras. Além disso, no final desta, falaremos e exemplificaremos os grupos de permutações e os grupos diedrais.

2.1.1 Grupos

Definição 2.1.1. *Seja G um conjunto de elementos, não vazio, dizemos que $(G, *)$ é um grupo se nele estiver definida uma operação binária $(*)$, que denotamos por $a * b$, que lê-se “ a operado com b ”, e tenha as seguintes propriedades:*

- i) Se $a, b \in G$ então $a * b \in G$ (Propriedade do Fechamento)*
- ii) Se $a, b, c \in G$ então $(a * b) * c = a * (b * c)$ (Propriedade Associativa)*
- iii) Existe um elemento $e \in G$ tal que $a * e = e * a = a$ (Existência do Elemento Neutro)*

iv) Para todo $a \in G$ existe $a^{-1} \in G$ tal que $a * a^{-1} = a^{-1} * a = e$ (*Existência do Elemento Inverso*)

Note que, para se ter um grupo não é necessário que ocorra a propriedade comutativa, no entanto, se ela ocorrer, dizemos que ele é um *Grupo Abelian*, ou seja, dados $a, b \in G$ para que o grupo seja abeliano é necessário que $a * b = b * a$.

A partir de agora, denotamos um grupo de $(G, *)$ ou simplesmente de G .

Definição 2.1.2. *Se G é um grupo, então:*

- (a) *O elemento neutro de G é único.*
- (b) *Todo $a \in G$ tem um único inverso em G .*
- (c) *Para todo $a \in G$, $(a^{-1})^{-1} = a$.*
- (d) *Para todo $a \in G$ temos que $(a * b)^{-1} = b^{-1} * a^{-1}$.*

2.1.2 Gerador de um Grupo

Dizemos que um grupo G é gerado pelos elementos $\alpha_1, \alpha_2, \dots, \alpha_n$, se qualquer elemento de G puder ser escrito como um número finito de operações entre esses elementos. Denotamos $G = \langle \alpha_1, \alpha_2, \dots, \alpha_n \rangle$.

A ordem de um grupo finito G é o número de elementos do conjunto, que denotaremos $|G|$. Assim, se um grupo G tiver n elementos, dizemos que $|G| = n$. Caso um grupo tenha infinitos elementos, dizemos que ele tem ordem infinita.

2.1.3 Exemplos de Grupos Abelianos

Exemplo 2.1.3. *O conjunto $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ é um grupo abeliano infinito, munido da operação de adição ou multiplicação.*

Exemplo 2.1.4. *O Grupo $B = \{-1, 1\}$ é um grupo abeliano multiplicativo de ordem 2.*

2.1.4 Subgrupos

Definição 2.1.5. Um subconjunto não vazio H de um grupo G é chamado de subgrupo de G , se, com relação a operação em G , o próprio H forma um grupo. Um subgrupo H de G será denotado por $H \leq G$.

Segue da Definição 2.1.5 e das propriedades de grupo que, para que H seja um subgrupo de G é necessário que ele obedeça as seguintes condições:

- i) $e \in H$;
- ii) Se $a, b \in H$ então $a * b \in H$.
- iii) $\forall a \in H$ então $a^{-1} \in H$.

Proposição 2.1.6. Se $H \neq \emptyset$, então $H \leq G$ se, e somente se, quaisquer que sejam $a, b \in H$ tem-se que $a * b^{-1} \in H$.

Demonstração. Inicialmente, se $H \leq G$, então por (i), temos que $e \in H$, logo $H \neq \emptyset$. Se $b \in H$ então, por (iii), $b^{-1} \in H$, assim se $a, b \in H$, temos $a, b^{-1} \in H$ e, por (ii), $a * b^{-1} \in H$.

Por outro lado, se $H \neq \emptyset$ e $a * b^{-1} \in H$, então existe $a \in H$ e $e = a * a^{-1} \in H$. Agora, se $a \in H$, temos que $a^{-1} = e * a^{-1} \in H$ e, se $a, b \in H$, segue que $a, b^{-1} \in H$ e assim, $a * b = a * (b^{-1})^{-1} \in H$, o que demonstra a proposição. \square

A partir desse momento usamos a notação multiplicativa, substituindo $x * y$ por $x.y$ ou, simplesmente, por xy . O elemento neutro por e_G ou somente por e . No caso da notação aditiva, normalmente usada quando o grupo é abeliano, o elemento neutro é denotado por 0 e o inverso de x é o $-x$, que é conhecido como simétrico de x .

Para demonstração de um exemplo envolvendo subgrupos, que aparece a seguir em forma de lema, e também para exemplos futuros é importante entendermos o que é uma relação de equivalência. Assim, sendo A um conjunto qualquer e \sim uma relação entre pares de elementos de A , se $a, b \in A$, de forma que a relaciona-se com b então denotamos por $a \sim b$.

Definição 2.1.7. Relação de Equivalência - Dados x, x' e $x'' \in A$, dizemos que \sim é uma Relação de Equivalência em A se ocorrem as seguintes propriedades:

- i) $x \sim x$ - (Propriedade Reflexiva);

ii) Se $x \sim x'$ então $x' \sim x$ - (Propriedade Simétrica);

iii) Se $x \sim x'$ e $x' \sim x''$ então $x \sim x''$ - (Propriedade Transitiva).

Definição 2.1.8. Se A é um conjunto e \sim é uma relação de equivalência em A , então a classe de equivalência de $a \in A$ é o conjunto denotado por $[a] = \{x \in A | a \sim x\}$.

Duas classes de equivalência são disjuntas ou distintas. Logo, A é a união disjunta dessas classes de equivalências, que é uma partição. Assim, definimos o conjunto das classes de equivalência dessa relação de equivalência como o conjunto $A/\sim = \{[a] : a \in A\}$.

Definição 2.1.9. Seja G um grupo, H um subgrupo de G . Para $a, b \in G$, dizemos que $a \equiv b \pmod{H}$ se $a.b^{-1} \in H$.

Denotaremos o conjunto das classes de equivalência da Definição 2.1.9 por G/H .

Exemplo 2.1.10. A relação $a \equiv b \pmod{H}$ é uma Relação de Equivalência.

Demonstração. Devemos observar se ocorrem as três propriedades da Relação de Equivalência. Dados $a, b, c \in H$, temos

1. $a \equiv a \pmod{H}$

De fato, como H é um subgrupo de G , $e \in H$ e $aa^{-1} = e$, logo $aa^{-1} \in H$, o que implica que $a \equiv a \pmod{H}$.

2. $a \equiv b \pmod{H} \Rightarrow b \equiv a \pmod{H}$

Suponhamos que $a \equiv b \pmod{H}$, ou seja, que $ab^{-1} \in H$, assim $(ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1}$. Portanto, $ba^{-1} \in H$, o que implica que $b \equiv a \pmod{H}$.

3. $a \equiv b \pmod{H}$ e $b \equiv c \pmod{H} \Rightarrow a \equiv c \pmod{H}$

Suponhamos que $a \equiv b \pmod{H}$ e $b \equiv c \pmod{H}$, logo $ab^{-1} \in H$ e $bc^{-1} \in H$. Como H é um subgrupo de G temos que $(ab^{-1})(bc^{-1}) \in H$, mas $(ab^{-1})(bc^{-1}) = a(b^{-1}b)c^{-1} = aec^{-1} = ac^{-1}$. Logo, $ac^{-1} \in H$ o que implica que $a \equiv c \pmod{H}$.

□

2.1.5 Classe Lateral

Definição 2.1.11. *Seja H um subgrupo de G e seja $a \in G$, então o conjunto $Ha = \{ha \mid h \in H\}$ é denominado classe lateral à direita de H em G . O conjunto $aH = \{ah \mid h \in H\}$ é denominado classe lateral à esquerda de H em G .*

Lema 2.1.12. *Para todo $a \in G$, temos $Ha = \{x \in G \mid a \equiv x \pmod{H}\}$.*

Demonstração. Seja $[a] = \{x \in G \mid a \equiv x \pmod{H}\}$. Inicialmente, mostramos que $Ha \subset [a]$. Realmente, se $h \in H$, então $a(ha)^{-1} = a(a^{-1}h^{-1}) = h^{-1}$, que pertence a H , pois H é um subgrupo de G . Pela definição de congruência, isto implica que $ha \in [a]$, e então $Ha \subset [a]$.

Considere agora, que $x \in [a]$. Assim $ax^{-1} \in H$, então $(ax^{-1})^{-1} = xa^{-1} \in H$. Ou seja, $xa^{-1} = h$ para algum $h \in H$. Multiplicando ambos os membros por a pela direita, temos que $x = ha$, o que implica que $x \in Ha$. Logo $[a] \subset Ha$ e, portanto, $[a] = Ha$. \square

A notação G/\sim é utilizada para relação de equivalência \sim . No caso da congruência módulo H é G/H , e este é o conjunto de todas as classes laterais à direita de H em G . Logo, G é a união disjunta das classes laterais distintas.

Lema 2.1.13. *Existe uma correspondência bijetora entre duas quaisquer classes laterais à direita de H em G .*

Demonstração. Dado um elemento $ha \in Ha$, com $h \in H$, associamos um elemento $hb \in Hb$. Está aplicação evidentemente é sobrejetora. Também é injetora, pois se $h_1b = h_2b$, com $h_1, h_2 \in H$, então $h_1 = h_2$ e portanto, $h_1a = h_2a$. \square

Teorema 2.1.14. Teorema de Lagrange - *Se H é um subgrupo de G , onde G é grupo finito, então a ordem $|H|$ é divisor da ordem $|G|$.*

Demonstração. Vimos que $G = \bigcup Ha$, assim $|G| = \sum |Ha|$, mas pelo Lema 2.1.13 para todo $a \in G$, $|Ha| = |H|$, logo $|G| = k|H|$, onde k é o número de classes laterais distintas. Ou seja, $|H| \mid |G|$. \square

Assim, k é denominado o índice de H em G e é a cardinalidade do conjunto G/H .

2.1.6 Subgrupo Normal

Definição 2.1.15. *Seja N um subgrupo de G . O conjunto N é dito um Subgrupo Normal de G se para todo $g \in G$ e $n \in N$ tivermos $gng^{-1} \in N$. Analogamente, podemos dizer que N é normal se $Ng = gN$, para todo $g \in G$.*

Seja N um subgrupo normal de G com $a, b \in G$. Definimos a operação $(Na)(Nb) = Nab$. De fato, como N é normal em G temos que $aN = Na$, portanto,

$$NaNb = N(aN)b = N(Na)b = NNab = Nab.$$

Com o resultado obtido acima podemos enunciar o seguinte lema:

Lema 2.1.16. *Um subgrupo N de G é um subgrupo normal de G se, e somente se, o produto de duas classes laterais à direita de N em G também resulta em uma classe lateral à direita de N em G .*

2.1.7 Grupo Quociente

Teorema 2.1.17. *Se G é um grupo e N é um subgrupo normal de G , então G/N , com a operação $Na.Nb = Nab$, também é um grupo, denominado Grupo Quociente.*

Demonstração. Seja $x = Na$, $y = Nb$ e $z = Nc$ com $a, b, c \in G$. Para G/N ser um grupo deve obedecer as seguintes propriedades:

(i) Se $x, y \in G/N$ então $xy \in G/N$ (fechamento)

Temos que $xy = (Na)(Nb) = Nab$ e $Nab \in G/N$. Logo $xy \in G/N$.

(ii) Se $x, y, z \in G/N$ então $(xy)z = x(yz)$ (associatividade)

Temos que $(xy)z = (NaNb)Nc = (Nab)Nc = N(ab)c$, ao mesmo tempo, $x(yz) = Na(NbNc) = Na(Nbc) = Na(bc)$. Mas $(ab)c = a(bc)$, pois $a, b, c \in G$ que é associativo. Logo, $(xy)z = N(ab)c = Na(bc) = x(yz)$.

(iii) Existe um elemento $N = Ne \in G/N$, tal que $xN = Nx = x$. (Existência do elemento neutro)

Se $x \in G/N$, isto é, $x = Na$, então $xN = NaNe = Nae = Na = x$ e $Nx = NeNa = Nea = Na = x$. Assim, Ne é o elemento neutro de G/N .

(iv) Para todo $x \in G/N$ existe um elemento $x^{-1} \in G/N$ tal que $x.x^{-1} = x^{-1}.x = Ne$ (Elemento inverso)

Seja $x^{-1} = Na^{-1} \in G/N$. Assim $x.x^{-1} = NaNa^{-1} = Naa^{-1} = Ne$. Analogamente, $x^{-1}x = Na^{-1}Na = Na^{-1}a = Ne$. Portanto, $x^{-1} = Na^{-1}$ é o inverso de $x = Na$ em G/N .

□

Proposição 2.1.18. *Sejam G um grupo e N um subgrupo normal de G . Se G é um grupo abeliano então G/N também é abeliano.*

Demonstração. Sejam $x = Na$ e $y = Nb$ com a e $b \in G$. Se $x, y \in G/N$ então $xy = (Na)(Nb) = Nab = Nba = (Nb)(Na) = yx$. Portanto, se G é abeliano então G/N também é abeliano.

□

Segue diretamente do Teorema 2.1.14 que,

Propriedade 2.1.19. *Se G é um grupo finito e N um subgrupo normal de G , então $|G/N| = \frac{|G|}{|N|}$.*

2.1.8 Homomorfismo de Grupos

Definição 2.1.20. *Dados os grupos (G, \cdot) e (J, \bullet) , chamamos de homomorfismo toda aplicação $f : G \rightarrow J$ tal que, quaisquer que sejam $a, b \in G$:*

$$f(a \cdot b) = f(a) \bullet f(b)$$

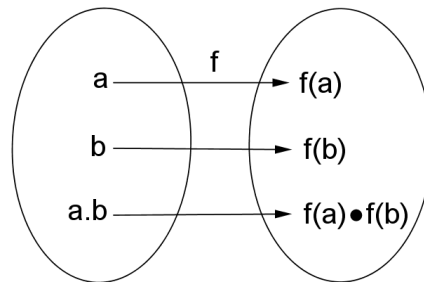


Figura 2.1: Homomorfismo de Grupos

Se $f : G \rightarrow J$ é um homomorfismo, dizemos que f é um homomorfismo de G em J . Agora, se o homomorfismo for dado por $f : G \rightarrow G$, dizemos que f é um homomorfismo em G , chamado de endomorfismo.

Definição 2.1.21. Se $f : G \longrightarrow J$ é um homomorfismo e f também é uma bijeção, então a aplicação é chamada de isomorfismo de G em J . Neste caso, G e J são ditos isomorfos e denotado por $G \cong J$.

Vejam alguns exemplos de homomorfismo de grupos:

Exemplo 2.1.22. Sejam $(\mathbb{R}, +)$ e (\mathbb{R}^*, \cdot) dois grupos com as operações usuais de adição e multiplicação de números reais. A aplicação definida por $f : \mathbb{R} \longrightarrow \mathbb{R}^*$ tal que $f(x) = 2^x$ é um homomorfismo.

De fato, tomemos $a, b \in \mathbb{R}$, assim temos $f(a+b) = 2^{a+b} = 2^a \cdot 2^b = f(a) \cdot f(b)$. Então, pela Definição 2.1.20 temos que f é um homomorfismo. E ainda, como $f(a) = 2^a$ é sempre positivo para todo $a \in \mathbb{R}$, temos que a imagem de f não é todo \mathbb{R}^* , logo f não é um homomorfismo sobrejetor, mas é um homomorfismo injetor, pois se $f(m) = f(n)$ temos $2^m = 2^n$ que implica $m = n$.

Exemplo 2.1.23. A aplicação $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$ definida por $f(x) = 3x$ é um homomorfismo de \mathbb{Z} .

De fato, pois dados $x, y \in \mathbb{Z}$ temos $f(x+y) = 3 \cdot (x+y) = 3x + 3y = f(x) + f(y)$.

Nesse caso, f também é uma aplicação injetora, pois se $f(m) = f(n)$ temos $3m = 3n \Rightarrow m = n$, mas não é sobrejetora pois $Im(f) = \{0, \pm 3, \pm 6, \pm 9, \dots\} \neq \mathbb{Z}$.

Exemplo 2.1.24. A aplicação $f : (\mathbb{R}_+^*, \cdot) \longrightarrow (\mathbb{R}, +)$ definida por $f(x) = \log x$ é um homomorfismo de \mathbb{R}_+^* em \mathbb{R} .

De fato, pois dados $x, y \in \mathbb{R}_+^*$ temos, $f(xy) = \log(xy) = \log(x) + \log(y) = f(x) + f(y)$.

Nesse caso, f é uma aplicação injetora, pois se $f(m) = f(n)$ temos $\log(m) = \log(n) \Rightarrow m = n$, e também é uma aplicação sobrejetora pois $Im(f) = \mathbb{R}$. Logo, f é um isomorfismo, pois trata-se de uma aplicação bijetora.

Definição 2.1.25. [Núcleo de um Homomorfismo]. Seja $f : G \longrightarrow J$ um homomorfismo definimos o núcleo de f , tal que para $x \in G$, temos $f(x) = \bar{e}$ onde \bar{e} é o elemento neutro de J .

Denotamos o núcleo de f por N_f , ou seja, $N_f = \{x \in G \mid f(x) = \bar{e}\}$

Definição 2.1.26. A definição de potência em um grupo G é dada por, $x^n = e$ se $n = 0$, $x^n = x^{n-1}x$, se $n > 0$, $x^n = (x^{-1})^{-n}$, $n < 0$.

Teorema 2.1.27. Seja $f : (G, *) \rightarrow (J, \star)$ um homomorfismo de grupos. Sendo e o elemento neutro de G e \bar{e} o elemento neutro de J , temos que

i) $f(e) = \bar{e}$.

ii) $f(x)^{-1} = f(x^{-1})$;

iii) $f(x)^n = f(x^n)$.

Demonstração. i) Existe $x \in G$ tal que $x = x * e$. Assim, $f(x) = f(x * e) = f(x) \star f(e)$. O que implica que $f(e) = \bar{e}$.

ii) Existe $x \in G$ tal que $e = x * x^{-1}$. Assim, $f(e) = f(x * x^{-1}) = f(x) \star f(x^{-1})$. Logo, $f(x^{-1}) = \frac{f(e)}{f(x)} = f(x)^{-1}$;

iii) Pela Definição 2.1.26 se $n > 0$, então $f(x^n) = f(x^{n-1} * x) = f(x^{n-1}) \star f(x) = f(x^{n-2} * x) \star f(x) = f(x^{n-2}) \star f(x) \star f(x) = f(x^{n-3} * x) \star \dots \star f(x) = \overbrace{f(x) \star \dots \star f(x)}^n = f(x)^n$ e se $n < 0$ então $f(x^n) = f((x^{-1})^{-n})$, mas como por ii) $f(x^{-1}) = f(x)^{-1}$, então $f(x^n) = f((x^{-1})^{-n}) = [f(x)^{-1}]^{-n} = f(x)^n$.

□

Teorema 2.1.28. [Teorema do Isomorfismo]. *Seja ψ um homomorfismo de G em \bar{G} com núcleo K , onde G e \bar{G} têm como identidades, respectivamente e e \bar{e} . Então,*

a) $\psi(G) = \{\psi(g) \mid g \in G\}$ é um subgrupo de \bar{G} .

b) $K = \{g \in G \mid \psi(g) = \bar{e}\}$ é um subgrupo normal de G e mais, ψ é injetiva $\Leftrightarrow K = \{e\}$.

c) $G/K \cong \psi(G)$

Demonstração. a) Inicialmente, $\bar{e} = \psi(e) \in \psi(G)$, pelo Teorema 2.1.27, temos $\psi(G) \neq \emptyset$. Temos ainda que, se $\psi(g_1), \psi(g_2) \in \psi(G)$ então $\psi(g_1) \cdot (\psi(g_2))^{-1} = \psi(g_1) \cdot \psi(g_2^{-1}) = \psi(g_1 \cdot g_2^{-1}) \in \psi(G) \forall g_1, g_2 \in G$. Assim, pela Proposição 2.1.6, temos que $\psi(G)$ é um subgrupo de \bar{G} .

b) Temos que $e \in K$, pois $\psi(e) = \bar{e}$. Temos também que, dados $g_1, g_2 \in K$, $\psi(g_1 g_2) = \psi(g_1) \cdot \psi(g_2) = \bar{e} \cdot \bar{e} = \bar{e}$, logo $g_1 g_2 \in K$. E ainda, se $g \in K$, então $\psi(g^{-1}) = \psi(g)^{-1} = (\bar{e})^{-1} = \bar{e}$, assim $g^{-1} \in K$. Agora, se $k \in K$ e $g \in G$, temos $\psi(g^{-1} \cdot k \cdot g) = \psi(g^{-1}) \cdot \psi(k) \cdot \psi(g) = \psi(g^{-1}) \cdot \bar{e} \cdot \psi(g) = (\psi(g))^{-1} \cdot \psi(g) = \bar{e}$, ou seja, $g^{-1} \cdot k \cdot g \in K$ para todo $k \in K$ e para todo $g \in G$. Assim, K é um subgrupo normal de G .

Agora, se $x, y \in G$, então

$$\psi(x) = \psi(y) \Leftrightarrow \psi(x) \cdot (\psi(y))^{-1} = \bar{e} \Leftrightarrow \psi(x \cdot y^{-1}) = \bar{e} = \psi(e) \Leftrightarrow xy^{-1} \in K.$$

- c) Seja $G' = G/K$. Vamos definir $\psi' : G' \rightarrow \psi(G)$ tal que $g' \rightsquigarrow \psi(g)$. Inicialmente ψ' está bem definida pois, $g' = h' \Rightarrow gh^{-1} \in K \Rightarrow \psi(gh^{-1}) = \bar{e} \Rightarrow \psi(g) = \psi(h)$. Temos que $\psi'(G') = \psi(G)$ e portanto a função é sobrejetiva.

Observe que, se $x' = Kx$ e $y' = Ky$, então $x'y' = KxKy = Kxy = (xy)'$. Assim, se $x', y' \in G' = G/K$ temos, $\psi'(x'y') = \psi'[(xy)'] = \psi(xy) = \psi(x)\psi(y) = \psi'(x') \cdot \psi'(y')$, ou seja, ψ' é um homomorfismo sobrejetivo. E ainda, $\psi'(x') = \bar{e} \Leftrightarrow \psi(x) = \bar{e} \Leftrightarrow x \in K \Leftrightarrow x' = \bar{e}$. Daí segue que, que o núcleo de ψ' é trivial pois o $\bar{e} = Ke = K$ e ψ' é injetiva. Assim, ψ' é um isomorfismo de G' sobre $\psi(G)$ e portanto $G/K \cong \psi(G)$. □

Teorema 2.1.29. [Teorema da Correspondência]. *Seja ψ um homomorfismo sobrejetor de G em G' com núcleo $K = K_\psi$, então:*

- (a) *Para cada H , $H \leq G$, tem-se $H' = \psi(H) = \{\psi(h) : h \in H\} \leq G'$. Mais ainda, se H é um subgrupo normal de G , então H' é um subgrupo normal de G' .*
- (b) *Para cada H' , $H' \leq G'$, o único subgrupo S de G contendo K tal que $\psi(S) = H'$ é $\psi^{-1}(H')$. Se H' é um subgrupo normal de G então $\psi^{-1}(H')$ é um subgrupo normal de G .*

Demonstração. Considerando $\hat{\psi} = \psi|_H = H \rightarrow G'$ a restrição de ψ ao subgrupo de G , temos que $\hat{\psi} : H \rightarrow G'$ é ainda um homomorfismo e pelo Teorema 2.1.28 segue que $H' = \psi(H)$ é um subgrupo normal de G' .

Agora, seja H um subgrupo normal de G . Se $g' \in G'$ temos $g' = \psi(g)$ para algum $g \in G$. Assim, para todo $h' \in H' = \psi(H)$ existe $h \in H$ tal que $\psi(h) = h'$ e para todo $g' \in G$ existe $g \in G$ tal que $g' = \psi(g)$. Segue que,

$$g'^{-1} \cdot h' \cdot g' = \psi(g)^{-1} \cdot \psi(h) \cdot \psi(g) = \psi(g^{-1} \cdot h \cdot g).$$

Como H é um subgrupo normal de G então $g^{-1} \cdot h \cdot g \in H$ temos,

$$g'^{-1} \cdot h' \cdot g' = \psi(g^{-1} \cdot h \cdot g) \in \psi(H) \text{ para todo } g' \in G' \text{ e para todo } h' \in H'.$$

Portanto, se H é um subgrupo normal de G então H' é um subgrupo normal de G' .

(b) Como $\psi(K) = \{e\} \subset H'$, claramente $\phi \neq \psi^{-1}(H') \subset N$. Se $a, b \in \psi^{-1}(H')$ então $\psi(a)\psi(b) \in H'$. Isto implica que $\psi(a).\psi(b)^{-1} \in H'$, que por sua vez implica que $ab^{-1} \in \psi^{-1}(H')$. Logo, $\psi^{-1} \leq G$.

Para cada $x \in G$ temos:

$\psi(x^{-1}\psi^{-1}(H')x) = \psi(x^{-1}).\psi(\psi^{-1}(H')).\psi(x) = \psi(x)^{-1}.H'.\psi(x) = H'$. Portanto, $x^{-1}.H'.x \subset \psi^{-1}(H')$ e $\psi(x^{-1}\psi^{-1}(H')x) = \psi^{-1}(H')$. Donde segue que $\psi^{-1}(H')$ é um subgrupo normal de G .

Finalmente, seja $H \leq G$ tal que $K \leq H$ e $\psi(H) = H'$. Assim, $\psi^{-1}(\psi(H)) = \psi^{-1}(H')$. Logo, $H \subset \psi^{-1}(H')$. Se $x \in \psi^{-1}(H')$ então $\psi(x) \in H'$ e existe $h \in H$ tal que $\psi(xh^{-1}) = e$. Assim, $ah^{-1} \in K \leq H$ e $a \in Hh = H$. Logo, $\psi^{-1}(H') \subset H$, consequentemente, $\psi^{-1}(H') = H$. \square

2.1.9 Grupos de Permutações

Uma *permutação* σ sobre um conjunto A é uma função bijetiva de A em A , ou seja, $\sigma : A \rightarrow A$. Utilizaremos a notação $\sigma(x) = y$ para representar a imagem de x pela bijeção σ .

Seja S_A o conjunto de todas as permutações de A sobre A , munido da operação composição de funções, então S_A é um grupo denominado Grupo das Permutações de A . A composição de funções é definida por: Se $f, g \in S_A$ definimos a composição de f por g como sendo $fg = f \circ g$ tal que $fg(x) = f(g(x))$ para todo $x \in A$.

Seja A um conjunto finito com n elementos que denotamos por $A = \{1, 2, \dots, n\}$. Tendo um valor fixo para n o conjunto de todas as permutações sobre o conjunto $\{1, 2, \dots, n\}$ será denotado por grupo S_n .

Para representar as permutações utilizamos a notação de matrizes, onde a 1ª linha corresponde ao domínio e a 2ª linha corresponde à imagem obtida.

Fixando $n = 3$, temos que S_3 é o grupo de todas as permutações sobre o conjunto $A = \{1, 2, 3\}$. Por exemplo,

1. Seja $\sigma_1 : A \rightarrow A$ tal que $\sigma_1(1) = 1$, $\sigma_1(2) = 2$ e $\sigma_1(3) = 3$. Temos,

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

2. Seja $\sigma_2 : A \longrightarrow A$ tal que $\sigma_2(1) = 3$, $\sigma_2(2) = 1$ e $\sigma_2(3) = 2$. Temos,

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

3. Seja $\sigma_3 : A \longrightarrow A$ tal que $\sigma_3(1) = 3$, $\sigma_3(2) = 2$ e $\sigma_3(3) = 1$. Temos,

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

De maneira análoga podemos definir as outras permutações σ_4, σ_5 e σ_6 , obtendo assim o conjunto S_3 abaixo:

$$S_3 = \left\{ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \right. \\ \left. \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}.$$

Assim, sejam $1, \sigma$ e $\tau \in S_3$ tais que $1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ e $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Fazendo as composições das funções observamos que $\sigma^3 = \tau^2 = 1$ e que $\tau\sigma = \sigma^2\tau$. Essa é a estrutura de um grupo S_3 , que denotamos por

$$S_3 = \langle \sigma, \tau \rangle.$$

$$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = 1,$$

$$\tau^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = 1,$$

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\sigma^2\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Além disso, observe ainda que $\sigma\tau \neq \tau\sigma$, o que mostra que o grupo S_3 não é abeliano.

Veja:

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \tau\sigma.$$

2.1.10 Grupos Diedrais

Seja P um polígono regular de n lados e D_n o conjunto das bijeções do plano que mantêm P constante. Dado um plano α , temos

$$D_n = \{f : \alpha \longrightarrow \alpha; \text{ onde } f \text{ é uma bijeção e } f(P) = P\}.$$

Por definição, D_n é um subconjunto de S_n , pois como S_n é o grupo de todas as permutações de um conjunto com n elementos e, nesse caso, D_n são as bijeções que deixam P fixo, então elas apenas fazem uma permutação de seus vértices. Assim,

$$D_n \subseteq S_n.$$

Vamos mostrar que D_n é um subgrupo das bijeções do plano. Temos,

- i) Como $I : \alpha \longrightarrow \alpha$ é uma bijeção tal que $I(P) = P$, então $I \in D_n$.
- ii) As aplicações $f, g \in D_n$ se, e somente se, $f(P) = P$ e $g(P) = P$, então $f \circ g : \alpha \longrightarrow \alpha$ é uma bijeção e $(f \circ g)(P) = f(g(P)) = f(P) = P$. Logo, $f \circ g \in D_n$.
- iii) Se $f \in D_n$, então existe $g : \alpha \longrightarrow \alpha$, tal que $f \circ g = g \circ f = I$, pois é uma bijeção no plano α . Como $f(P) = P$, então

$$P = I(P) = (g \circ f)(P) = g(f(P)) = g(P)$$

Logo, $f^{-1} = g \in D_n$.

Assim, temos que D_n é um subgrupo das bijeções do plano e, portanto, pela Definição 2.1.5, D_n é um grupo. De acordo com [9], o grupo diedral n , denotado por D_n , cuja operação é a composição de funções, é um grupo não abeliano e ocorre para $n \geq 3$. Neles existem $2n$ elementos.

Como exemplo de Grupo Diedral fazemos a construção do D_4 , que é o grupo das simetrias do quadrado Q . No Capítulo 3, um dos exemplos abordando a teoria de Galois, recorre ao Grupo Diedral D_4 .

Exemplo 2.1.30. *Para melhor visualização das bijeções do plano e das imagens dos pontos do quadrado, o mesmo teve seus vértices enumerados de 1 a 4 e foi inscrito num círculo de centro O , conforme a imagem.*

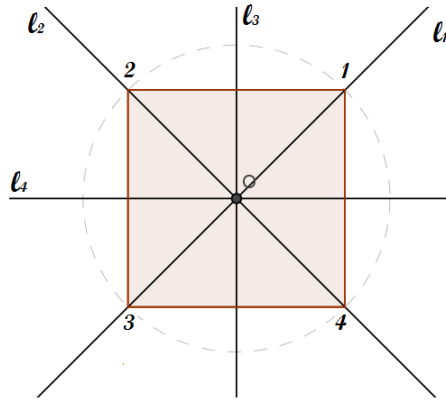
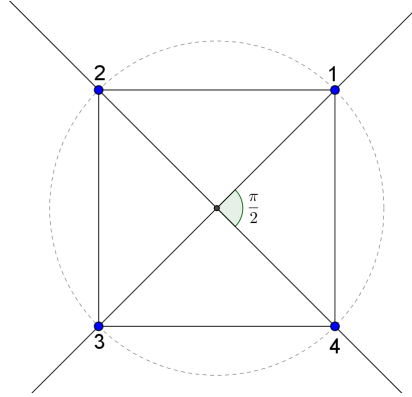


Figura 2.2: Quadrado Q

No quadrado temos 4 retas l_1, l_2, l_3 e l_4 , cujas simetrias no plano em relação a elas deixam o quadrado constante. Sejam S_1, S_2, S_3 e S_4 as simetrias do plano em relação às retas dadas, respectivamente. Essas bijeções possuem a propriedade $S_i(Q) = Q$, com $i = \{1, 2, 3, 4\}$. Como sabemos os ângulos internos, formados pelas diagonais do quadrado medem $\frac{\pi}{2}$, por isso temos quatro rotações feitas no sentido anti-horário em torno de O que deixam Q constante, ou seja, $R_i(Q) = Q$, com $i = \{1, 2, 3, 4\}$, onde R_1 é a rotação $\frac{\pi}{2}$, R_2 é a rotação π , R_3 é a rotação $\frac{3\pi}{2}$ e R_4 é a rotação 2π , ou seja, $R_4 = I$.



Assim, podemos simbolizar as 8 bijeções do plano, que deixam Q constante, por bijeções do conjunto $\{1\ 2\ 3\ 4\}$, que são:

$$\begin{aligned}
 S_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, & S_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \\
 S_3 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, & S_4 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \\
 R_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, & R_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \\
 R_3 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, & R_4 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = I.
 \end{aligned}$$

É possível escrever essas 8 bijeções utilizando $\sigma = S_1$, $\tau = R_1$ e $I = R_4$. Fazendo as composições, observamos que $S_2 = \sigma\tau^2$, $S_3 = \sigma\tau^3$, $S_4 = \sigma\tau$, $R_2 = \tau^2$, $R_3 = \tau^3$, $R_4 = \tau^4 = I$, $S_1^2 = \sigma^2 = I$ e $\tau\sigma = \sigma\tau^3$.

Resumindo, $D_4 = \langle \sigma, \tau \rangle$. Além disso, $D_4 = \{I, \tau, \tau^2, \tau^3, \sigma, \sigma\tau, \sigma\tau^2, \sigma\tau^3\}$.

Veja as relações:

$$\begin{aligned}
 \tau^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = R_2, \\
 \tau^3 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = R_3,
 \end{aligned}$$

$$\begin{aligned} \sigma\tau &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = S_4, \\ \sigma\tau^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = S_2, \\ \sigma\tau^3 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = S_3, \\ \tau^4 = \tau^3\tau &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = R_4, \\ \tau\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = S_3 = \sigma\tau^3 \end{aligned}$$

2.2 Anéis

2.2.1 Definições e Exemplos

Definição 2.2.1. *Seja R um conjunto não vazio, chamamos $(R, +, \cdot)$ de anel associativo se nele estiverem definidas duas operações adição e multiplicação, que indicamos por $+$ e \cdot , respectivamente, e que para todo a, b e $c \in R$ tenhamos:*

1. $a + b \in R$ (*Propriedade do Fechamento*)
2. $a + b = b + a$ (*Propriedade Comutativa da Adição*)
3. $(a + b) + c = a + (b + c)$ (*Propriedade Associativa da Adição*)
4. *Em R , existe um elemento 0 , tal que $a + 0 = a$, para todo $a \in R$ (Existência do Elemento Neutro da Adição)*
5. $\exists -a \in R$ tal que $a + (-a) = 0 \forall a \in R$ (*Existência do Elemento Oposto*)
6. $a \cdot b \in R$ (*Propriedade do Fechamento*)
7. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (*Propriedade Associativa da multiplicação*)

8. $a.(b+c) = a.b + a.c$ e $(b+c).a = b.a + c.a$ (*Propriedade Distributiva*)

Podemos notar nos Axiomas de 1 a 5 que $(R, +)$ é um grupo abeliano, que chamamos de adição, os axiomas 6 e 7 nos informam que R é fechado e possui a propriedade associativa com relação a operação $.$, que é denominada de multiplicação, já o Axioma 8 faz uma ligação entre as duas operações em R .

Exemplo 2.2.2. *Seja $\mathbb{Z}(\sqrt{2})$ o conjunto de todos os reais da forma $a + b\sqrt{2}$, com $a, b \in \mathbb{Z}$. Temos que $\mathbb{Z}(\sqrt{2})$ forma um anel com relação à adição e à multiplicação usual de números reais, veja:*

Sejam $a_1 + b_1\sqrt{2}$, $a_2 + b_2\sqrt{2}$ e $a_3 + b_3\sqrt{2} \in \mathbb{Z}(\sqrt{2})$, então:

1. $(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in \mathbb{Z}(\sqrt{2})$. Logo vale a propriedade do fechamento para a adição.
2. $(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} = (a_2 + a_1) + (b_2 + b_1)\sqrt{2} = (a_2 + b_2\sqrt{2}) + (a_1 + b_1\sqrt{2})$. Portanto, vale a propriedade comutativa para a adição.
3. $(a_1 + b_1\sqrt{2}) + [(a_2 + b_2\sqrt{2}) + (a_3 + b_3\sqrt{2})] = (a_1 + b_1\sqrt{2}) + [(a_2 + a_3) + (b_2 + b_3)\sqrt{2}] = (a_1 + a_2 + a_3) + (b_1 + b_2 + b_3)\sqrt{2} = (a_1 + a_2) + a_3 + (b_1 + b_2)\sqrt{2} + b_3\sqrt{2} = [(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})] + (a_3 + b_3\sqrt{2})$. Vale a propriedade associativa para a adição.
4. Em $\mathbb{Z}(\sqrt{2})$, existe o elemento $0 = 0 + 0\sqrt{2}$, tal que $a + b\sqrt{2} + 0 + 0\sqrt{2} = a + b\sqrt{2}$, para todos $a, b \in \mathbb{Z}(\sqrt{2})$. Existe o elemento neutro.
5. O elemento $-a - b\sqrt{2} \in \mathbb{Z}(\sqrt{2})$ é tal que $(a + b\sqrt{2}) + (-a - b\sqrt{2}) = 0 + 0\sqrt{2} = 0$. Existe o elemento oposto.
6. Temos que $(a_1 + b_1\sqrt{2}).(a_2 + b_2\sqrt{2}) = [(a_1.a_2 + 2.b_1.b_2) + (a_1.b_2 + a_2.b_1)\sqrt{2}] \in \mathbb{Z}(\sqrt{2})$. Assim, vale a propriedade do fechamento para a multiplicação.
7. E ainda que $(a_1 + b_1\sqrt{2}).[(a_2 + b_2\sqrt{2}).(a_3 + b_3\sqrt{2})] = a_1.a_2.a_3 + (a_1.a_2.b_3 + a_1.a_3.b_2 + a_2.a_3.b_1 + 2.b_1.b_2.b_3)\sqrt{2} + 2.(a_1.a_3.b_1 + a_2.b_1.b_3 + a_3.b_1.b_2) = [a_1.a_2 + 2.b_1.b_2 + (a_1.b_2 + a_2.b_1)\sqrt{2}].(a_3 + b_3\sqrt{2}) = [(a_1 + b_1\sqrt{2}).(a_2 + b_2\sqrt{2})].(a_3 + b_3\sqrt{2})$. Vale a propriedade associativa para a multiplicação.
8. Por fim, temos que

$$(a_1 + b_1\sqrt{2}).[(a_2 + b_2\sqrt{2}) + (a_3 + b_3\sqrt{2})] =$$

$$\begin{aligned}
&= (a_1 + b_1\sqrt{2}) \cdot [(a_2 + a_3) + (b_2 + b_3)\sqrt{2}] = \\
&= a_1 \cdot (a_2 + a_3) + a_1 \cdot (b_2 + b_3)\sqrt{2} + b_1 \cdot (a_2 + a_3)\sqrt{2} + 2b_1 \cdot (b_2 + b_3) = \\
&= a_1 \cdot a_2 + a_1 \cdot a_3 + a_1 \cdot b_2\sqrt{2} + a_1 \cdot b_3\sqrt{2} + b_1 \cdot a_2\sqrt{2} + b_1 \cdot a_3\sqrt{2} + 2b_1 \cdot b_2 + 2b_1 \cdot b_3 = \\
&= a_1 \cdot (a_2 + b_2\sqrt{2}) + b_1\sqrt{2} \cdot (a_2 + b_2\sqrt{2}) + a_1 \cdot (a_3 + b_3\sqrt{2}) + b_1\sqrt{2} \cdot (a_3 + b_3\sqrt{2}) = \\
&= (a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2}) + (a_1 + b_1\sqrt{2}) \cdot (a_3 + b_3\sqrt{2}). \text{ Indicando que vale a} \\
&\text{propriedade distributiva.}
\end{aligned}$$

Iremos denotar o anel $(R, +, \cdot)$ por R .

Definição 2.2.3. *Seja R um anel. Se para todos $a, b \in R$ tivermos $a \cdot b = b \cdot a$ então chamamos R de anel comutativo.*

Definição 2.2.4. *Se R é um anel comutativo e nele existir um elemento que denotamos por 1 , tal que $a \cdot 1 = 1 \cdot a = a$ para todo $a \in R$, chamamos R de anel com elemento unidade.*

Se R é um anel comutativo, consideramos $a \neq 0 \in R$ um *divisor de zero*, se existir um $b \neq 0 \in R$, tal que $a \cdot b = 0$.

Definição 2.2.5. *Se um anel comutativo e não possuir divisores de zero, dizemos que ele é um anel de integridade.*

Definição 2.2.6. *Se R é um anel comutativo, com elemento unidade e , além disso, os elementos de R , diferentes de 0 , formam um grupo abeliano em relação à multiplicação, então dizemos que R é um corpo.*

Um anel é conhecido como *anel com divisão* se seus elementos não nulos formam um grupo com relação à multiplicação, sendo assim, um corpo é um anel com divisão comutativo.

Assim, dizemos que R é um *corpo* se $(R, +)$ e (R^*, \cdot) são grupos abelianos, com elemento unidade.

Vemos na sequência, alguns exemplos de anéis e corpos.

Exemplo 2.2.7. *O conjunto dos números inteiros \mathbb{Z} com adição e multiplicação usuais é um anel comutativo com elemento unidade, 1 . Observe ainda que \mathbb{Z} não é um corpo, pois não é um grupo em relação à multiplicação, dada a ausência do elemento inverso multiplicativo. \mathbb{Z} é uma anel de integridade.*

Exemplo 2.2.8. *Seja $2\mathbb{Z}$ o conjunto dos inteiros pares, temos que $2\mathbb{Z}$ é um anel comutativo com as operações de adição e multiplicação usuais. Mas $2\mathbb{Z}$ não possui o elemento unidade, logo não é um corpo.*

Exemplo 2.2.9. Seja \mathbb{Q} o conjunto dos números racionais contendo as operações usuais de adição e multiplicação. Esse conjunto é um anel comutativo com elemento unidade. Além disso, \mathbb{Q} é um corpo. De fato,

- i) Dados $a, b \in \mathbb{Q}$ temos que $a.b \in \mathbb{Q}$;
- ii) Dados $a, b, c \in \mathbb{Q}$ temos que $(a.b).c = a.(b.c)$;
- iii) Temos que $1 \in \mathbb{Q}$ e que $a.1 = 1.a = a$, para todo $a \in \mathbb{Q}$;
- iv) Para todo $a \in \mathbb{Q}$, com $a \neq 0$, existe $a^{-1} \in \mathbb{Q}$, tal que $a.a^{-1} = a^{-1}.a = 1$;
- v) Para todo $a, b \in \mathbb{Q}$ temos $a.b = b.a$.

Exemplo 2.2.10. Anel dos quatérnios reais, que foi escrito pela primeira vez pelo matemático irlandês Hamilton.

Seja $\mathbb{Q}t$ o conjunto de todos os símbolos $x_0 + x_1i + x_2j + x_3k$, onde x_0, x_1, x_2 e x_3 são reais. Podemos dizer que dois desses símbolos, $x_0 + x_1i + x_2j + x_3k$ e $y_0 + y_1i + y_2j + y_3k$ são iguais se, e somente se, $x_t = y_t$, para $t = 0, 1, 2, 3$. Para que $\mathbb{Q}t$ seja um anel é necessário definir uma soma (+) e uma multiplicação (.) para seus elementos. Assim, definimos:

1. Para todos $A = x_0 + x_1i + x_2j + x_3k$ e $B = y_0 + y_1i + y_2j + y_3k$ em $\mathbb{Q}t$, então:

$$A + B = (x_0 + x_1i + x_2j + x_3k) + (y_0 + y_1i + y_2j + y_3k)$$

$$A + B = (x_0 + y_0) + (x_1 + y_1)i + (x_2 + y_2)j + (x_3 + y_3)k.$$

2. $A.B = (x_0 + x_1i + x_2j + x_3k).(y_0 + y_1i + y_2j + y_3k)$

$$A.B = (x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3) + (x_0y_1 + x_1y_0 + x_2y_3 - x_3y_2)i + (x_0y_2 + x_2y_0 + x_3y_1 - x_1y_3)j + (x_0y_3 + x_3y_0 + x_1y_2 - x_2y_1)k.$$

Essa fórmula é obtida da multiplicação formal de dois destes símbolos e a reunião de dos termos usando a relação: $i^2 = j^2 = k^2 = ijk = -1$, $ij = -ji = k$, $jk = -kj = i$ e $ki = -ik = j$. Essa relação, denominada tábua de multiplicação das unidades dos quatérnios, pode ser representada pelo diagrama abaixo quando se percorre no sentido horário, por exemplo, $ij = k, jk = i$ e $ki = j$, sendo o sentido anti-horário negativo.

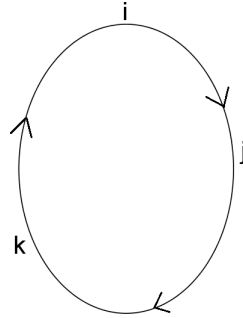


Figura 2.3: Diagrama: Anel dos Quatérnios

Em $\mathbb{Q}t$ temos que $0 = 0 + 0i + 0j + 0k$ e $1 = 1 + 0i + 0j + 0k$ são, respectivamente, o elemento neutro e a unidade e como $i.j \neq j.i$ temos que $\mathbb{Q}t$ é um exemplo de anel não comutativo com unidade, além do mais, prova-se que, se $A = x_0 + x_1i + x_2j + x_3k$ então existe um elemento $B = A^{-1} = \frac{x_0 - x_1i - x_2j - x_3k}{x_0^2 + x_1^2 + x_2^2 + x_3^2}$ em $\mathbb{Q}t$, tal que, $A.B = B.A = 1$. Logo $\mathbb{Q}t$ é um anel com divisão, mas não um corpo, uma vez que não satisfaz a comutatividade para a multiplicação.

O lema a seguir mostra o jogo de sinais para o produto, que normalmente são ensinados no Ensino Fundamental quando consideramos $R = \mathbb{Q}$, ou seja, o corpo $(\mathbb{Q}, +, \cdot)$.

Lema 2.2.11. *Seja R um anel, então para todo $a, b \in R$ temos:*

1. $a.0 = 0.a = 0$
2. $a.(-b) = (-a).b = -(a.b)$
3. $(-a).(-b) = a.b$

E ainda se R possui um elemento unidade 1, então

4. $(-1).a = -a$.
5. $(-1).(-1) = 1$.

Demonstração.

1. Se $a \in R$, então $a.0 = a.(0 + 0) = a.0 + a.0$, e como R é um grupo com relação à adição, então $a.0 = 0$, de forma similar, $0.a = (0 + 0).a = 0.a + 0.a$, que implica que $0.a = 0$.

2. Para mostrar que $a.(-b) = -(a.b)$, basta mostrarmos que $a.b + a.(-b) = 0$. Temos que, $a.b + a.(-b) = a.(b + (-b)) = a.0 = 0$. Analogamente, $(-a).b = -(a.b)$.
3. Na demonstração do terceiro item usamos o segundo, assim $(-a).(-b) = -(a.(-b)) = -(-(a.b)) = a.b$.
4. Vamos supor que R possua um elemento unidade 1, assim $a + (-1).a = 1.a + (-1).a = (1 + (-1)).a = 0.a = 0$. Logo, $(-1).a = -a$.
5. Em particular, se $a = -1$, então de $(-1).a = -a$, temos $(-1).(-1) = -(-1) = 1$.

□

2.2.2 Homomorfismo de Anéis

A definição de homomorfismo de anéis é similar à proposta em grupo. O que difere, é que nos anéis devemos analisar a aplicação para duas operações.

Definição 2.2.12. *Dados $a, b \in R$, dizemos que ϕ é um homomorfismo de um anel $(R, +, \cdot)$ em um anel $(R', +, \cdot)$ se:*

- i. $\phi(a + b) = \phi(a) + \phi(b)$ (i.é, ϕ é um homomorfismo de grupos);*
- ii. $\phi(a.b) = \phi(a).\phi(b)$.*

Se ϕ é um homomorfismo de R em R' , definimos o *núcleo de ϕ* como o conjunto de todos os elementos $a \in R$ tal que $\phi(a) = 0$ e chamamos esse núcleo de N_ϕ . Ou seja,

$$N_\phi = \{a \in R : \phi(a) = 0\}.$$

Lema 2.2.13. *Seja N_ϕ o núcleo de um homomorfismo de R em R' , então:*

- 1. Em relação à adição, N_ϕ é um subgrupo normal de R .*
- 2. Se $a \in N_\phi$ e $r \in R$, então $a.r \in N_\phi$ e $r.a \in N_\phi$.*

Demonstração.

1. Como ϕ é um homomorfismo de R em R' , como grupo aditivo, então pelo Teorema 2.1.28, temos que N_ϕ é um subgrupo normal de R .

2. Vamos supor que $a \in N_\phi$ e $r \in R$, então, pela definição de núcleo, temos que $\phi(a) = 0$. Temos também que $\phi(a.r) = \phi(a).\phi(r) = 0.\phi(r) = 0$. Analogamente, $\phi(r.a) = 0$. Assim, temos que $a.r$ e $r.a$ estão em N_ϕ .

□

Um homomorfismo de R em R' , onde ϕ é uma aplicação injetora, é dito *monomorfismo de anéis*, já se ϕ for uma aplicação sobrejetora, é dito *epimorfismo de anéis*. Se ϕ é bijetora, dizemos que ϕ é um *isomorfismo de anéis* e assim podemos afirmar que os anéis R e R' são isomorfos.

Exemplo 2.2.14. *Sejam R e R' dois anéis quaisquer tais que $\phi(a) = 0$, para todo $a \in R$. Temos que ϕ é um homomorfismo e que $N_\phi = R$. Nesse caso, ϕ é chamado de homomorfismo nulo.*

Definição 2.2.15. *Um conjunto não vazio I de R é chamado de **ideal** de R se:*

- (1) *I é um subgrupo de R em relação à adição;*
- (2) *Para todo $i \in I$ e $r \in R$ tivermos $i.r$ e $r.i \in I$.*

Seja R um ideal, então 0 e R são ideais de R denominados ideais triviais.

Lema 2.2.16. *Seja R um anel comutativo com elemento unidade onde os únicos ideais são os triviais. Então, R é um corpo.*

Demonstração. Para todo $a \neq 0 \in R$ queremos construir um elemento $b \neq 0 \in R$ tal que $ab = 1$.

Seja $a \neq 0 \in R$ e considere o conjunto $Ra = \{xa \mid x \in R\}$. Então, Ra é um ideal de R . De fato, se u e $v \in Ra$, então $u = r_1a$ e $v = r_2a$ para algum r_1 e $r_2 \in R$. Assim, $u+v = r_1a+r_2a = (r_1+r_2)a \in Ra$; $-u = -r_1a = (-r_1)a \in Ra$, o que mostra que Ra é um subgrupo aditivo de R . Temos também que, se $r \in R$, $ru = r(r_1a) = (rr_1)a \in Ra$, que complementa as condições para que Ra seja um ideal de R .

Temos, por hipótese, que $Ra = \{0\}$ ou $Ra = R$. Como $0 \neq a = 1a \in Ra$, então $Ra \neq \{0\}$, ou seja, $Ra = R$. Assim, todo elemento em R é múltiplo de a segundo algum elemento de R . Particularmente, $1 \in R$ e pode ser considerado um múltiplo de a , assim, existe um elemento $b \in R$ tal que $ba = 1$. □

Sejam U um ideal do anel R e R/U o conjunto de todas as classes laterais distintas de U em R , que obtemos quando consideramos U como um subgrupo de R com relação à adição. Em símbolos, temos $R/U = \{a + U \mid a \in R\}$.

Lema 2.2.17. *Se U é um ideal do anel R , então R/U é um anel e é uma imagem homomorfa de R .*

Demonstração. Definimos em R/U a operação de multiplicação $(a+U)(b+U) = ab+U$. Agora, para mostrar que R/U é um anel devemos verificar se os axiomas que definem um anel valem para R/U . Fazemos a demonstração para um dos axiomas, pois as demais demonstrações são bastante semelhantes. Temos que a propriedade distributiva à direita vale para R/U , pois se $X = a+U$, $Y = b+U$ e $Z = c+U$ são três elementos de R/U , onde $a, b, c \in R$, então $(X+Y)Z = ((a+U)+(b+U))(c+U) = ((a+b)+U)(c+U) = (a+b)c+U = ac+bc+U = (ac+U)+(bc+U) = (a+U)(c+U)+(b+U)(c+U)$. Portanto, R/U é um anel. Logo, se R é comutativo, então R/U também o é, se R possui um elemento unidade 1 , então R/U também possui um elemento unidade $1+U$. E ainda, existe um homomorfismo sobrejetor ϕ de R em R/U dado por $\phi(a) = a+U$, em que U é o núcleo. \square

Teorema 2.2.18. *Sejam R e R' anéis e ϕ um homomorfismo sobrejetor de R em R' com núcleo N_ϕ . Então:*

- i) R' é isomorfo a R/U , onde $U = N_\phi$ é o núcleo do homomorfismo;*
- ii) Existe uma correspondência bijetora entre o conjunto dos ideais de R' e o conjunto dos ideais de R que contêm N_ϕ .*

Omitimos a demonstração do teorema acima, uma vez que se trata de uma tradução literal da demonstração para grupos para a linguagem de anéis, veja Teorema do Isomorfismo 2.1.28 e o Teorema da Correspondência 2.1.29.

Definição 2.2.19. *Um ideal $M \neq R$ num anel R é chamado de **ideal maximal** de R se, sempre que U for um ideal de R , tal que $M \subset U \subset R$, então $U = M$ ou $U = R$. Ou seja, um ideal M é maximal se não for possível colocar um ideal entre ele e o anel todo.*

Teorema 2.2.20. *Sejam R um anel comutativo com elemento unidade e M um ideal de R . Então, M é maximal em R se, e somente se, R/M é um corpo.*

Demonstração. Vamos supor que M seja um ideal de R tal que R/M seja um corpo. Como R/M é um corpo então seus únicos ideais são $\{0\}$ e o próprio R/M . Mas, pelo Teorema 2.2.18, existe uma correspondência bijetora entre o conjunto dos ideais R/M e o conjunto de ideais de R que contêm M . Na correspondência em questão, o ideal M

de R corresponde ao ideal $\{0\}$ de R/M , e o ideal R de R corresponde ao ideal R/M de R/M . Ou seja, não existe nenhum ideal entre M e R além dos triviais, assim M é um ideal maximal. Se M é um ideal maximal de R , então pela correspondência citada, temos que R/M possui apenas $\{0\}$ e R/M como ideais. Como R/M é comutativo e possui um elemento unidade, R/M é um corpo. \square

2.3 O Corpo de Fração de um Anel de Integridade

Conforme a Definição 2.2.5, o anel dos inteiros é um exemplo de anel de integridade. E ele possui a característica necessária que podemos estendê-lo para o conjunto dos racionais, que é um corpo. Tal fato, pode ser percebido em qualquer anel de integridade.

Definição 2.3.1. *Dados os anéis R e R' dizemos que R pode ser imerso em R' se existir um monomorfismo de R em R' . O anel R' é denominado sobre-anel ou uma extensão de R .*

Se R e R' possuem 1 e $1'$, respectivamente, como elementos unidades, é necessário que esse monomorfismo leve 1 sobre $1'$.

Teorema 2.3.2. *Todo anel de integridade pode ser imerso em um corpo.*

Demonstração. Seja D um anel de integridade. Assim, o corpo que procuramos deve ser constituído de todas as frações $\frac{a}{b}$ onde $a, b \in D$ e $b \neq 0$, onde $\frac{a}{b}$ pertence ou não a D .

Seja M o conjunto de todos os pares ordenados (a, b) com $a, b \in D$ e $b \neq 0$. Em M definimos a seguinte relação de equivalência:

$$(a, b) \sim (c, d) \text{ se, e somente se, } ad = bc.$$

Para demonstrar a validade da relação acima, vamos verificar as três condições da definição de relação de equivalência.

- i) Se $(a, b) \in M$, então $(a, b) \sim (a, b)$, pois $ab = ba$.
- ii) Se $(a, b), (c, d) \in M$ e $(a, b) \sim (c, d)$, então $ad = bc$, e ainda $cb = da$. Logo, $(c, d) \sim (a, b)$.

iii) Se $(a, b), (c, d), (e, f) \in M$, $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$ então $ad = bc$ e $cf = de$. Assim, $bcf = bde$ e como $bc = ad$, então $adf = bde$. Uma vez que D é comutativo, temos que $afd = bed$, logo $af = be$, pois D é um anel de integridade e $d \neq 0$. Portanto, $(a, b) \sim (e, f)$.

Considere que $[a, b]$ a classe de equivalência em M de (a, b) e F o conjunto de todas essas classes de equivalência $[a, b]$, onde $a, b \in D$ e $b \neq 0$. Vamos mostrar que F é um corpo.

Para adição definimos,

$$[a, b] + [c, d] = [ad + bc, bd].$$

Temos que $b \neq 0$, $d \neq 0$, logo $bd \neq 0$, pois D é um anel de integridade, assim $[ad + bc, bd] \in F$.

Afim de verificarmos a definição temos que se $[a, b] = [a', b']$ e $[c, d] = [c', d']$, então

$$[a, b] + [c, d] = [a', b'] + [c', d'].$$

De fato, se $[a, b] = [a', b']$, então $ab' = ba'$ e se $[c, d] = [c', d']$, então $cd' = dc'$.

Temos que,

$$[a, b] + [c, d] = [ad + bc, bd]$$

$$[a', b'] + [c', d'] = [a'd' + b'c', b'd']$$

Queremos mostrar que $[ad + bc, bd] = [a'd' + b'c', b'd']$, mas isso ocorre se $(ad + bc)b'd' = (a'd' + b'c')bd$.

Mas, $(ad + bc)b'd' = adb'd' + bcb'd' = ab'dd' + bb'cd' = ba'dd' + bb'dc' = bd(a'd' + b'c')$.

Temos que F é um grupo abeliano em relação a esta adição e $[0, b]$ é o elemento neutro da adição e $[-a, b]$ é o oposto de $[a, b]$.

Para multiplicação definimos,

$$[a, b].[c, d] = [ac, bd]$$

Da mesma forma que na adição, com $b \neq 0$ e $d \neq 0$, temos que $bd \neq 0$ e se fizermos $[a, b] = [a', b']$ e $[c, d] = [c', d']$, obtemos que $[a, b].[c, d] = [a', b'].[c', d']$.

Temos ainda que,

1. Todos elementos $[a, b]$, com $b \neq 0$ formam um grupo abeliano com relação a multiplicação.
2. $[d, d]$ é o elemento unidade da multiplicação.

3. $[c, d]^{-1} = [d, c]$, pois $c \neq 0$ e $[d, c]$ está em F .
4. Vale a propriedade distributiva em F .

Portanto, F é um corpo.

Agora, seja $x, y \in D$, com $x \neq 0$ e $y \neq 0$, então $[ax, x] = [ay, y]$, pois $(ax)y = x(ay)$. Denotamos $[ax, x] = [a, 1]$. Definamos $\phi : D \rightarrow F$, por $\phi(a) = [a, 1]$. É fácil ver que ϕ é um monomorfismo de D em F , e que se 1 é o elemento unidade de D então $\phi(1) = [1, 1]$ é o elemento unidade de F . Portanto, F é um corpo de fração de D e D está imerso em F . \square

2.4 Anéis de Polinômios

Nos Ensinos Fundamental e Médio iniciamos o estudo de polinômios, desde operações com polinômios, fatorações, simplificações e até determinação de raízes de alguns deles. No Ensino Superior, já como funções, tivemos a preocupação em verificar suas continuidades, derivadas, integrais e máximos e mínimos. Nesse estudo, estamos interessados em incluir esses polinômios como elementos de um anel e estudar as propriedades algébricas em cada caso. O interesse principal decorre do fato deles nos fornecerem um anel euclidiano no qual as propriedades levam a uma discussão de corpos e de extensões de corpos.

Um anel de polinômios na indeterminada x é indicado de $F[x]$, onde F é um corpo. $F[x]$ é o conjunto de todos os símbolos da forma $a_0 + a_1x + \dots + a_mx^m$, onde m pode ser qualquer inteiro não negativo e os coeficientes a_0, a_1, \dots, a_m pertencem ao corpo F .

$$F[x] = \{a_0 + a_1x + \dots + a_nx^n \mid a_i \in F \text{ e } n \in \mathbb{Z}_+\}$$

Para que $F[x]$ seja um anel é necessário sabermos quando dois elementos dele são iguais, precisamos adicionar e multiplicar elementos de $F[x]$ tal que os axiomas que definem um anel valham em $F[x]$.

Definição 2.4.1. *Se $p(x) = a_0 + a_1x + \dots + a_nx^n$ e $q(x) = b_0 + b_1x + \dots + b_nx^n$ pertencem a $F[x]$, então $p(x) = q(x)$ se, e somente se, para todo inteiro $i \geq 0$, $a_i = b_i$.*

Em outras palavras, dizemos que dois polinômios são iguais se, e somente se, os coeficientes correspondentes forem iguais.

Definição 2.4.2. Se $p(x) = a_0 + a_1x + \dots + a_nx^n$ e $q(x) = b_0 + b_1x + \dots + b_mx^m$ estão ambos em $F[x]$, com $n \geq m$, então $p(x) + q(x) = c_0 + c_1x + \dots + c_kx^k + \dots + c_nx^n$, onde para cada i , $c_i = a_i + b_i$. Para $n > m$ teremos $b_n = 0$.

Assim, para somarmos dois polinômios quaisquer devemos somar seus coeficientes correspondentes e colecionar seus termos. Como exemplo, se somarmos os polinômios $7 + 3x + x^2$ e $10 - x$, onde podemos considerar $10 - x$ como $10 - x + 0x^2$, obtemos $(7 + 10) + (3 + (-1))x + (1 + 0)x^2$, que corresponde a $17 + 2x + x^2$.

Podemos observar que a expressão obtida para $p(x) + q(x)$ mostra que $p + q$ também é um polinômio em F . É possível mostrar que o par obtido do conjunto dos polinômios sobre F e a operação de adição definida é um grupo abeliano. O elemento neutro é a função identicamente nula, $0 + 0x + 0x^2 + \dots + 0x^m$, onde 0 indica o zero do anel F e que o simétrico aditivo de um polinômio $p(x) = a_0 + a_1x + \dots + a_mx^m$ é o polinômio $-p$ definido por $(-p)(x) = -a_0 + (-a_1)x + \dots + (-a_m)x^m$.

Definição 2.4.3. Se $p(x) = a_0 + a_1x + \dots + a_mx^m$ e $q(x) = b_0 + b_1x + \dots + b_nx^n$, então $p(x)q(x) = c_0 + c_1x + \dots + c_t x^t$, onde $c_i = a_i b_0 + a_{i-1} b_1 + a_{i-2} b_2 + \dots + a_0 b_i$.

Na multiplicação de polinômios, multiplicamos todos os seus termos formalmente e utilizamos a relação $x^a x^b = x^{a+b}$. Como exemplo, observe o produto abaixo:

$$p(x) = 5 - x + x^2, \quad q(x) = 2 + 3x - x^3.$$

Neste caso, $a_0 = 5, a_1 = -1, a_2 = 1$ e $a_3 = a_4 = \dots = 0$ e $b_0 = 2, b_1 = 3, b_2 = 0, b_3 = -1$ e $b_4 = b_5 = \dots = 0$. Assim,

$$c_0 = a_0 b_0 = 5 \cdot 2 = 10,$$

$$c_1 = a_1 b_0 + a_0 b_1 = (-1) \cdot 2 + 5 \cdot 3 = 13,$$

$$c_2 = a_2 b_0 + a_1 b_1 + a_0 b_2 = 1 \cdot 2 + (-1) \cdot 3 + 5 \cdot 0 = -1,$$

$$c_3 = a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3 = 0 \cdot 2 + 1 \cdot 3 + (-1) \cdot 0 + 5 \cdot (-1) = -2,$$

$$c_4 = a_4 b_0 + a_3 b_1 + a_2 b_2 + a_1 b_3 + a_0 b_4 = 0 \cdot 2 + 0 \cdot 3 + 1 \cdot 0 + (-1) \cdot (-1) + 5 \cdot 0 = 1,$$

$$c_5 = a_5 b_0 + a_4 b_1 + a_3 b_2 + a_2 b_3 + a_1 b_4 + a_0 b_5 = 0 \cdot 2 + 0 \cdot 3 + 0 \cdot 0 + 1 \cdot (-1) + (-1) \cdot 0 + 5 \cdot 0 = -1,$$

$$c_6 = a_6 b_0 + a_5 b_1 + a_4 b_2 + a_3 b_3 + a_2 b_4 + a_1 b_5 + a_0 b_6 = 0 \cdot 2 + 0 \cdot 3 + 0 \cdot 0 + 0 \cdot (-1) + (-1) \cdot 0 + 5 \cdot 0 = 0,$$

$$c_7 = c_8 = \dots = 0.$$

Portanto, segundo a definição o produto

$$(5 - x + x^2)(2 + 3x - x^3) = 10 + 13x - x^2 - 2x^3 + x^4 - x^5.$$

Temos ainda que na multiplicação de polinômios valem a associatividade e a comutatividade, onde o polinômio definido por $1 + 0x + 0x^2 + \dots + 0x^m$ é o elemento neutro dessa operação e que 0 e 1 indicam respectivamente o zero e a unidade de F .

Portanto, temos que $F[x]$ é um anel com estas operações.

Definição 2.4.4. Se $f(x) = a_0 + a_1x + \dots + a_mx^m \neq 0$ e $a_m \neq 0$ e $a_j = 0 \forall j > m$, então o grau de $f(x)$, que é indicado por $gr[f(x)]$, é m .

Lema 2.4.5. Se $f(x)$ e $g(x)$ são dois elementos não nulos de $F[x]$, então $gr[f(x)g(x)] = gr[f(x)] + gr[g(x)]$.

Demonstração. Nesse caso suponhamos que $f(x) = a_0 + a_1x + \dots + a_mx^m$ e $g(x) = b_0 + b_1x + \dots + b_nx^n$, com $a_m \neq 0$ e $b_n \neq 0$, então $gr[f(x)] = m$ e $gr[g(x)] = n$. Como $f(x)g(x) = c_0 + c_1x + \dots + c_tx^t$, onde $c_i = a_ib_0 + a_{i-1}b_1 + a_{i-2}b_2 + \dots + a_0b_i$. Afirmamos que $c_{m+n} = a_mb_n \neq 0$ e $c_i = 0$ para $i > m+n$. Temos que $c_{m+n} = a_mb_n$ segue da definição, já que c_i é obtido pela soma dos termos da forma a_jb_{i-j} . Caso $i = j + (i-j) > m+n$, então $j > m$ ou $i-j > n$, o que implica que $a_j = 0$ ou $b_{i-j} = 0$, de modo que $a_j \cdot b_{i-j} = 0$, assim temos $c_i = 0$. Dessa maneira, o maior coeficiente não nulo de $f(x)g(x)$ é c_{m+n} , assim $gr[f(x)g(x)] = m+n = gr[f(x)] + gr[g(x)]$. \square

Corolário 2.4.6. Se $f(x)$ e $g(x)$ são elementos não nulos de $F[x]$, então $gr[f(x)] \leq gr[f(x)g(x)]$.

Demonstração. Como $gr[f(x)g(x)] = gr[f(x)] + gr[g(x)]$, e sabendo que $gr[g(x)] \geq 0$, temos que $gr[f(x)] = gr[f(x)g(x)] - gr[g(x)] \leq gr[f(x)g(x)]$. \square

Corolário 2.4.7. $F[x]$ é um anel de integridade.

Demonstração. Como $F[x]$ possui um elemento neutro para operação de multiplicação (no caso, $n(x) = 1$), é comutativo em relação a multiplicação, ou seja, $f(x) \cdot g(x) = g(x) \cdot f(x)$ e dados dois elementos $f(x)$ e $g(x)$ em $F[x]$, temos que se $f(x) \cdot g(x) = 0$ então $f(x) = 0$ ou $g(x) = 0$. Portanto, $F[x]$ é um anel de integridade. \square

Definição 2.4.8. Dizemos que $(p(x))$ é um ideal se $(p(x)) = \{q(x)p(x) : q(x) \in F[x]\}$.

Sabendo que $F[x]$ é um anel de integridade, podemos construir para ele seu corpo de frações, que consiste em todas as frações de polinômios e é denominado *corpo de funções racionais em x sobre F* . Denotamos por $F[x]/(p(x))$, onde $p(x)$ é um polinômio em $F[x]$.

Lema 2.4.9 (O Algoritmo da Divisão). *Dados dois polinômios $f(x)$ e $g(x) \neq 0$ em $F[x]$, então existem dois polinômios $q(x)$ e $r(x)$ em $F[x]$ tais que $f(x) = q(x)g(x) + r(x)$, onde $r(x) = 0$ ou $gr[r(x)] < gr[g(x)]$.*

Demonstração. Se o $gr[f(x)] < gr[g(x)]$, basta colocarmos $q(x) = 0$, $r(x) = f(x)$ e teremos $f(x) = 0 \cdot g(x) + f(x)$, onde $gr[f(x)] < gr[g(x)]$ ou $f(x) = 0$.

Agora, vamos analisar o caso em que $f(x) = a_0 + a_1x + \dots + a_mx^m$ e $g(x) = b_0 + b_1x + \dots + b_nx^n$, onde $a_m \neq 0$, $b_n \neq 0$ e $m \geq n$.

Seja $f_1(x) = f(x) - \left(\frac{a_m}{b_n}\right)x^{m-n}g(x)$, assim $gr[f_1(x)] \leq m - 1$, então por indução sobre o grau de $f(x)$ podemos admitir que $f_1(x) = q_1(x)g(x) + r(x)$, onde $r(x) = 0$ ou $gr[r(x)] < gr[g(x)]$. Mas então, $f(x) - \left(\frac{a_m}{b_n}\right)x^{m-n}g(x) = q_1(x)g(x) + r(x)$, assim, temos que $f(x) = \left(\frac{a_m}{b_n}x^{m-n} + q_1(x)\right)g(x) + r(x)$. Fazendo $q(x) = \frac{a_m}{b_n}x^{m-n} + q_1(x)$, obtemos $f(x) = q(x)g(x) + r(x)$, onde $q(x), r(x) \in F[x]$ e $r(x) = 0$ ou $gr[r(x)] < gr[g(x)]$. \square

Definição 2.4.10. *Dizemos que um polinômio $p(x)$ em $F[x]$ é irredutível em F , caso $p(x) = f(x)g(x)$, com $f(x), g(x) \in F[x]$, tivermos $gr[f(x)] = 0$ ou $gr[g(x)] = 0$, ou seja, $p(x) = f(x)g(x)$ é irredutível se $f(x)$ ou $g(x)$ for uma constante.*

A irredutibilidade de um polinômio depende do corpo F ao qual pertence. Por exemplo, o polinômio $x^2 + 4$ é irredutível no corpo dos reais, porém não é irredutível no corpo dos complexos, uma vez que $(x^2 + 4) = (x + 2i)(x - 2i)$, onde $i^2 = -1$.

Lema 2.4.11. *Qualquer polinômio $f(x)$ pode ser escrito de uma única maneira como produto de polinômios irredutíveis em $F[x]$.*

Demonstração. Seja $f(x) \in F[x]$ um polinômio de grau n maior ou igual a 1, vamos por indução sobre $gr(f(x))$.

O caso $gr(f(x)) = 1$ não há o que provar: pois $f(x)$ tendo grau 1 já está fatorado como produto de irredutíveis.

Caso contrário, podemos escrever $f(x) = f_1(x)f_2(x)$, onde $f_1(x)$ e $f_2(x)$ possuem grau menor que n . Se $f_1(x)$ e $f_2(x)$ forem irredutíveis, a fatoração está concluída. Caso contrário, devemos repetir o processo até obtermos uma fatoração de $f(x)$ como produto de irredutíveis. Suponha que $f(x)$ seja o produto de m polinômios irredutíveis, assim vamos mostrar a unicidade da fatoração. Suponhamos que

$$f(x) = f_1(x)f_2(x)\dots f_m(x) = g_1(x)g_2(x)\dots g_n(x)$$

sejam duas possíveis fatorações de $f(x)$ como produto de polinômios irredutíveis, onde $m \leq n$. Então, $f_1(x) \mid g_1(x)g_2(x)\dots g_n(x)$ donde, $f_1(x) \mid g_j(x)$ para alguma $j \in 1, 2, \dots, n$. Podemos assumir, sem perda de generalidade, que $j = 1$, então $f_1(x) \mid g_1(x)$. No entanto, $g_1(x)$ é irredutível, assim $g_1(x) = \alpha_1 f_1(x)$, com $\alpha_1 \in F$. Substituindo $g_1(x)$ na equação destacada anteriormente e cancelando, ficamos com

$$f_1(x)f_2(x)\dots f_m(x) = \alpha_1 f_1(x)g_2(x)\dots g_n(x)$$

$$f_2(x)\dots f_m(x) = \alpha_1 g_2(x)\dots g_n(x)$$

Repetindo o argumento, obtemos

$$1 = \alpha_1 \dots \alpha_m g_{m+1}(x) \dots g_n(x)$$

o que só é possível se $m = n$. Portanto, concluímos que os fatores irredutíveis $f_i(x)$ e $g_i(x)$ são os mesmos, a menos pela forma que se escrevem os fatores.

□

Lema 2.4.12. *O ideal $A = (p(x))$ em $F[x]$ é maximal se, e somente se, $p(x)$ é um polinômio irredutível em $F[x]$.*

Demonstração. Provamos que $p(x)$ é redutível se, e somente se, A não é maximal. Suponhamos que $p(x)$ é redutível. Então ou é invertível ou pode ser escrita como um produto de polinômios. No primeiro caso tem-se $1 = (p(x))^{-1}p(x) \in A$ onde $A = F[x]$ não é maximal. No segundo caso tem-se $p(x) = q_1(x)q_2(x)$ com $gr[q_1(x)] \geq 1$ e $gr[q_2(x)] \geq 1$. Então, $1 \leq gr[q_1(x)] < gr[p(x)]$, e pela Definição 2.4.8 de Ideal gerado por $q_1(x)$, segue que

$$(p(x)) \subset (q_1(x)) \subset F[x]$$

o que mostra que, também neste caso, A não é maximal.

Reciprocamente, suponhamos que A não é maximal, ou seja, que existe um ideal $B = (q(x))$ tal que $A \subset B \subset F[x]$. Então $p(x) = r(x)q(x)$ para algum $r(x) \in F[x]$. É claro que $gr[r(x)] \geq 1$ (pois se $r(x)$ for constante, $q(x)$ pertence a $(p(x))$ e teremos $B = A$). Por outro lado, também $gr[q(x)] \geq 1$ (caso contrário, $B = F[x]$). Assim, a fatoração $p(x) = r(x)q(x)$ mostra que $p(x)$ é redutível em $F[x]$. □

Exemplo 2.4.13. *Seja F o corpo dos números racionais e considere o polinômio $p(x) = x^3 - 2$ em $F[x]$. Temos que $p(x)$ é irredutível sobre F e que $F[x]/(x^3 - 2)$ é um corpo. Como são seus elementos?*

Seja $A = (x^3 - 2)$ o ideal em $F[x]$ gerado por $x^3 - 2$.

Todo elemento em $F[x]/(x^3 - 2)$ é uma classe lateral da forma $f(x) + A$ do ideal A , com $f(x)$ em $F[x]$. Mas, dado um polinômio qualquer $f(x)$ em $F[x]$, pelo algoritmo da divisão temos $f(x) = t(x)(x^3 - 2) + r(x)$, onde $r(x) = 0$ ou $\text{gr}[r(x)] < \text{gr}[(x^3 - 2)] = 3$. Assim, $r(x) = a_0 + a_1x + a_2x^2$, onde $a_0, a_1, a_2 \in F$, assim, $f(x) + A = a_0 + a_1x + a_2x^2 + t(x)(x^3 - 2) + A = a_0 + a_1x + a_2x^2 + A$, pois $t(x)(x^3 - 2) \in A$. Pela adição e multiplicação em $F[x]/(x^3 - 2)$, $f(x) + A = (a_0 + A) + a_1(x + A) + a_2(x + A)^2$. Fazendo $t = x + A$, temos que todo elemento de $F[x]/(x^3 - 2)$ é da forma $a_0 + a_1t + a_2t^2$, onde $a_0, a_1, a_2 \in F$. Perceba que $t^3 - 2 = (x + A)^3 - 2(1 + A) = (x + A)(x + A)(x + A) - 2(1 + A) = (x^2 + A)(x + A) - 2(1 + A) = x^3 + A - 2(1 + A) = x^3 - 2 + A = A = 0$, pois $x^3 - 2 \in A$ e A é o elemento zero de $F[x]/(x^3 - 2)$, assim $t^3 = 2$.

Se $a_0 + a_1t + a_2t^2 = b_0 + b_1t + b_2t^2$, então $(a_0 - b_0) + (a_1 - b_1)t + (a_2 - b_2)t^2 = 0$, onde $f(t) = 0$ então $f(x) + A = A$ o que implica que $f(x) \in A$, assim $(a_0 - b_0) + (a_1 - b_1)x + (a_2 - b_2)x^2 = 0$ está em $A = (x^3 - 2)$. Isso só pode ocorrer se $(a_0 - b_0) + (a_1 - b_1)x + (a_2 - b_2)x^2 = 0$, uma vez que todo elemento de A tem grau no mínimo igual a 3, assim $a_0 = b_0$, $a_1 = b_1$ e $a_2 = b_2$. Desta forma, percebemos que todo elemento em $F[x]/(x^3 - 2)$ tem apenas uma representação na forma $a_0 + a_1t + a_2t^2$, onde $a_0, a_1, a_2 \in F$. Pelo Teorema 2.2.20, $F[x]/(x^3 - 2)$ é um corpo. Para verificar, devemos demonstrar que $a_0 + a_1t + a_2t^2 \neq 0$, então ele possui um inverso multiplicativo, que representamos por $\alpha + \beta t + \gamma t^2$. Agora, precisamos resolver a relação $(a_0 + a_1t + a_2t^2)(\alpha + \beta t + \gamma t^2) = 1$, onde a_0, a_1 e a_2 não são todos nulos. Fazendo a multiplicação termo a termo e utilizando o fato de que $t^3 = 2$, temos $(a_0\alpha + 2a_2\beta + 2a_1\gamma) + (a_1\alpha + a_0\beta + 2a_2\gamma)t + (a_2\alpha + a_1\beta + a_0\gamma)t^2 = 1$, assim:

$$\begin{cases} a_0\alpha + 2a_2\beta + 2a_1\gamma = 1 \\ a_1\alpha + a_0\beta + 2a_2\gamma = 0 \\ a_2\alpha + a_1\beta + a_0\gamma = 0 \end{cases}$$

A solução desse sistema existe se, e somente se, $a_0^3 + 2a_1^3 + 4a_2^3 - 6a_0a_1a_2 \neq 0$. Portanto, para demonstrar que $F[x]/(x^3 - 2)$ é um corpo se reduz a demonstrar que a única solução de $a_0^3 + 2a_1^3 + 4a_2^3 = 6a_0a_1a_2$ é a solução trivial $a_0 = a_1 = a_2 = 0$. Se existir uma solução racional, simplificando os denominadores podemos mostrar que existe uma solução onde a_0, a_1 e a_2 são números inteiros. Assim, podemos admitir que a_0, a_1 e a_2 não possui divisores inteiros diferentes de 1, pois caso contrário, se $a_0 = b_0d, a_1 = b_1d$

e $a_2 = b_2d$, onde d é o máximo divisor comum de a_0, a_1 e a_2 , substituindo na equação $a_0^3 + 2a_1^3 + 4a_2^3 = 6a_0a_1a_2$ teríamos $(b_0d)^3 + 2(b_1d)^3 + 4(b_2d)^3 = 6(b_0d)(b_1d)(b_2d)$, ou seja, $d^3(b_0^3 + 2b_1^3 + 4b_2^3) = d^3(6b_0b_1b_2)$, e então $b_0^3 + 2b_1^3 + 4b_2^3 = 6b_0b_1b_2$, o problema fica assim reduzido à demonstração de que a equação não possui soluções inteiras que sejam relativamente primas. Mas, a equação implica que a_0^3 é par, de modo que a_0 é par. Substituindo $a_0 = 2\alpha_0$ temos que $4\alpha_0^3 + a_1^3 + 2a_2^3 = 6\alpha_0a_1a_2$. Assim, a_1^3 é par, de modo que a_1 é par. Fazendo $a_1 = 2\alpha_1$ temos $2\alpha_0^3 + 4\alpha_1^3 + a_2^3 = 6\alpha_0\alpha_1a_2$. Assim, a_2^3 é par, e portanto a_2 é par. Mas, então a_0, a_1, a_2 possuem 2 como fator comum, o que contradiz o fato de serem relativamente primos. Logo, a equação $a_0^3 + 2a_1^3 + 4a_2^3 = 6a_0a_1a_2$ não possui solução racional além de $a_0 = a_1 = a_2 = 0$. Portanto, podemos resolver para α, β e γ e demonstramos diretamente que $F[x]/(x^3 - 2)$ é um corpo.

2.5 Polinômios sobre o Corpo Racional

Em particular, estudamos o caso dos polinômios cujos coeficientes são números racionais. Porém, na maior parte dos casos os coeficientes será números inteiros, onde estamos atentos com sua irredutibilidade.

Definição 2.5.1. Dado o polinômio $f(x) = a_0 + a_1x + \dots + a_nx^n$, onde a_0, a_1, \dots, a_n são inteiros, chamamos f de primitivo se o $\text{mdc}(a_0, a_1, \dots, a_n) = 1$.

Lema 2.5.2. Se $f(x)$ e $g(x)$ são polinômios primitivos, então $f(x)g(x)$ é um polinômio primitivo.

Demonstração. Sejam $f(x) = a_0 + a_1x + \dots + a_nx^n$ e $g(x) = b_0 + b_1x + \dots + b_mx^m$ dois polinômios primitivos. Vamos supor que o lema fosse falso, ou seja, todos os elementos de $f(x)g(x)$ são divisíveis por algum inteiro maior que 1, ou melhor, por algum número primo p ($p \mid c_i$, para todo i inteiro maior que 1). Como $f(x)$ é primitivo, p não divide algum coeficiente a_i , analogamente, como $g(x)$ também é primitivo, p não divide algum coeficiente b_j . Sejam a_k e b_l os primeiros coeficientes de $f(x)$ e $g(x)$, respectivamente, não divisíveis por p . Em $f(x)g(x)$ o coeficiente de x^{k+l} , c_{k+l} , é

$$c_{k+l} = a_kb_l + (a_{k+1}b_{l-1} + a_{k+2}b_{l-2} + \dots + a_{k+l}b_0) + (a_{k-1}b_{l+1} + a_{k-2}b_{l+2} + \dots + a_0b_{k+l}).$$

Mas, com a escolha que fizemos de b_l , $p \mid b_{l-1}, b_{l-2}, \dots, b_0$ de modo que

$$p \mid a_{k+1}b_{l-1} + a_{k+2}b_{l-2} + \dots + a_{k+l}b_0.$$

Da mesma forma, pela nossa escolha de $a_k, p \mid a_{k-1}, a_{k-2}, \dots, a_0$ de modo que

$$p \mid a_{k-1}b_{l+1} + a_{k-2}b_{l+2} + \dots + a_0b_{l+k}.$$

Por hipótese, $p \mid c_{k+l}$, assim $p \mid a_k b_l$, o que é absurdo, pois $p \nmid a_k$ e $p \nmid b_l$. \square

Definição 2.5.3. Dado um polinômio $f(x) = a_0 + a_1x + \dots + a_nx^n$ de coeficientes inteiros, definimos como conteúdo o máximo divisor comum de a_0, a_1, \dots, a_n .

Teorema 2.5.4. Lema de Gauss - Se o polinômio primitivo $f(x)$ pode ser fatorado como o produto de dois polinômios com coeficientes racionais, então ele pode ser fatorado como o produto de dois polinômios com coeficientes inteiros.

Demonstração. Suponhamos que $f(x) = p(x)q(x)$, onde $p(x)$ e $q(x)$ são polinômios de coeficientes racionais. Reduzindo ao mesmo denominador e colocando em evidência os fatores comuns podemos escrever $f(x) = \frac{a}{b}u(x)v(x)$ onde a e b são números inteiros e $u(x)$ e $v(x)$ são primitivos e possuem coeficientes inteiros. Assim, $bf(x) = au(x)v(x)$. Temos que, o conteúdo do primeiro membro da igualdade anterior é b , pois $f(x)$ é primitivo, e como $u(x)$ e $v(x)$ são primitivos, temos pelo Lema 2.5.2 que $u(x)v(x)$ é primitivo, assim o conteúdo do segundo membro é a . Portanto, $a = b, \frac{a}{b} = 1$ e $f(x) = u(x)v(x)$, onde $u(x)$ e $v(x)$ possuem coeficientes inteiros. \square

Definição 2.5.5. Um polinômio do tipo $a_0x^n + a_1x^{n-1} + \dots + a_n$ é dito inteiro e unitário se a_0, a_1, \dots, a_n são inteiros e o coeficiente do termo de maior grau é 1, ou seja, $a_0 = 1$.

Teorema 2.5.6. O Critério de Eisenstein - Seja $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ um polinômio de coeficientes inteiros. Suponhamos que para algum número primo $p, p \nmid a_n, p \mid a_1, p \mid a_2, \dots, p \mid a_0, p^2 \nmid a_0$. Então, $f(x)$ é irredutível aos racionais.

Demonstração. Suponhamos que $f(x)$ seja primitivo, uma vez que colocando em evidência o máximo divisor comum de seus coeficientes não atrapalhamos a hipótese, pois $p \nmid a_n$. Se $f(x)$ é fatorável como um produto de dois polinômios racionais, então, pelo Lema de Gauss, f é fatorável como um produto de dois polinômios que tem coeficientes inteiros. No caso, se considerarmos que $f(x)$ seja redutível, temos

$$f(x) = (b_0 + b_1x + \dots + b_\alpha x^\alpha)(c_0 + c_1x + \dots + c_\beta x^\beta)$$

onde os b_α e c_β são inteiros e $\alpha > 0$ e $\beta > 0$. Igualando os coeficiente obtemos $a_0 = b_0c_0$ e, como $p \mid a_0$ então $p \mid b_0$ ou $p \mid c_0$. Mas $p^2 \nmid a_0$, portanto p não pode dividir b_0 e c_0 . Ao mesmo tempo vamos supor que $p \mid b_0$ e $p \nmid c_0$. Observe que nem todos os coeficientes $b_0, b_1, \dots, b_\alpha$ são divisíveis por p , pois senão todos os coeficientes de $f(x)$ seriam divisíveis

por p , o que não é possível uma vez que $p \nmid a_n$. Seja b_i o primeiro b que não é divisível por p , $i \leq \alpha < n$. Assim, $b \mid b_{i-1}$ e todos os b anteriores. Mas $a_i = b_i c_0 + b_{i-1} c_1 + \dots + b_0 c_i$ e $p \mid a_i$, $p \mid b_{i-1}, b_{i-2}, \dots, b_0$, de modo que $p \mid b_i c_0$. Contradição, pois $p \nmid c_0$ e $p \nmid b_i$. Portanto, não podemos fatorar $f(x)$, ou seja, f é irredutível sobre os racionais. \square

2.6 Extensões de Corpos

Quando estudamos anéis, definimos que um corpo é um anel comutativo, com elemento unidade, onde todo elemento não nulo possui um inverso multiplicativo. Nesse momento, estamos interessados em abordar a parte da teoria de corpos que engloba equações e problemas de raízes de polinômios. Mais adiante, introduzimos algumas ideias escritas pelo matemático francês Evariste Galois que nos auxiliam em tal tarefa. Nesta seção falamos um pouco sobre a relação entre dois corpos.

Definição 2.6.1. Extensão de Corpos - Sejam F e K corpos, então K é chamado extensão de F se K contém F . Da mesma forma, K é uma extensão de F se F é um subcorpo de K .

Como $K \supset F$, então K é um espaço vetorial sobre F , uma vez que as relações de definição de um corpo são justamente as relações de definição de um espaço vetorial se o escalar está em F .

Definição 2.6.2. O grau de K sobre F é a dimensão de K como espaço vetorial sobre F , que indicamos por $[K : F]$.

Teorema 2.6.3. Se E é uma extensão finita de K e se K é uma extensão finita de F , então E é uma extensão finita de F . Temos ainda que $[E : F] = [E : K][K : F]$.

Demonstração. Suponhamos que $[E : K] = m$ e que $[K : F] = n$. Seja v_1, v_2, \dots, v_m uma base de E sobre K e seja w_1, w_2, \dots, w_n uma base de K sobre F . Mostramos que $v_i w_j$, com $i = 1, 2, \dots, m$ e $j = 1, 2, \dots, n$ formam uma base de E sobre F . Para isso, mostramos que todo elemento em E é uma combinação linear deles com elementos em F , em seguida mostramos que os mn elementos são linearmente independentes em F .

Seja t um elemento qualquer de E . Como todo elemento de E é uma combinação linear de v_1, v_2, \dots, v_m com os coeficientes em K , ou seja, t é da forma $t = k_1 v_1 + k_2 v_2 + \dots + k_m v_m$, onde os elementos $k_1, k_2, \dots, k_m \in K$. Mas, todo elemento K é uma combinação linear de w_1, w_2, \dots, w_n com coeficientes de F , ou seja, $k_i = f_{i1} w_1 + f_{i2} w_2 + \dots + f_{in} w_n$, onde $f_{ij} \in F$.

Fazendo a substituição destas expressões k_1, k_2, \dots, k_m em t , temos

$$t = k_1v_1 + \dots + k_iv_i + \dots + k_mv_m = (f_{11}w_1 + f_{12}w_2 + \dots + f_{1n}w_n)v_1 + \dots + (f_{i1}w_1 + f_{i2}w_2 + \dots + f_{in}w_n)v_i + \dots + (f_{m1}w_1 + f_{m2}w_2 + \dots + f_{mn}w_n)v_m.$$

Fazendo os produtos utilizando as leis distributivas e associativas obtemos

$$t = f_{11}v_1w_1 + \dots + f_{1n}v_1w_n + \dots + f_{ij}v_iw_j + \dots + f_{mn}v_mw_n.$$

Como os f_{ij} estão em F , exibimos t como um combinação linear sobre F dos elementos v_iw_j .

Vamos mostrar agora que v_iw_j são linearmente independentes sobre F . Suponhamos que $f_{11}v_1w_1 + \dots + f_{1n}v_1w_n + \dots + f_{ij}v_iw_j + \dots + f_{mn}v_mw_n = (f_{11}w_1 + f_{12}w_2 + \dots + f_{1n}w_n)v_1 + \dots + (f_{i1}w_1 + f_{i2}w_2 + \dots + f_{in}w_n)v_i + \dots + (f_{m1}w_1 + f_{m2}w_2 + \dots + f_{mn}w_n)v_m = 0$, onde $f_{ij} \in F$. Queremos mostrar que $f_{ij} = 0$. Como w_i estão em K e como $K \supset F$, todos os elementos $k_i = f_{i1}w_1 + f_{i2}w_2 + \dots + f_{in}w_n$ estão em K . Assim, $k_1v_1 + \dots + k_iv_i + \dots + k_mv_m = 0$ com $k_1, k_2, \dots, k_m \in K$. Por hipótese, v_1, v_2, \dots, v_m formam uma base de E sobre K , assim temos $k_1 = k_2 = \dots = k_m = 0$, o que nos fornece que

$$f_{i1}w_1 + f_{i2}w_2 + \dots + f_{in}w_n = 0 \text{ para } i = 1, 2, 3, \dots, m.$$

Mas, como w_i são linearmente independentes sobre F , temos que cada $f_{ij} = 0$, assim v_iw_j são linearmente independentes sobre F .

Como v_iw_j geram pela combinação linear E sobre F e são linearmente independentes sobre F , temos que mn elementos v_iw_j formam uma base de E sobre F . Assim, $[E : F] = mn$, como $m = [E : K]$ e $n = [K : F]$ mostramos que $[E : F] = [E : K][K : F]$.

□

Corolário 2.6.4. *Se E é uma extensão finita de F e se K é um subcorpo de E que contém F , então $[K : F] \mid [E : F]$.*

Demonstração. Sejam E, K e F três corpos tais que $E \supset K \supset F$ e que $[E : F]$ seja finito. Temos que, qualquer elemento de F , linearmente dependente sobre K , também é linearmente dependente sobre F . Assim, a hipótese de que $[E : F]$ é finito, implica que $[E : K]$ também é finito. Além disso, como K é subespaço de E , $[K : F]$ é finito. Pelo Teorema 2.6.3, temos que $[E : F] = [E : K][K : F]$, logo $[K : F] \mid [E : F]$. □

Definição 2.6.5. Um elemento $a \in K$ é chamado de algébrico sobre F se existem elementos $\alpha_0, \alpha_1, \dots, \alpha_n$ em F , não todos nulos, tais que $\alpha_0 a^n + \alpha_1 a^{n-1} + \dots + \alpha_n = 0$.

Se o polinômio $q(x) \in F[x]$, tal que $q(x) = \beta_0 x^n + \beta_1 x^{n-1} + \dots + \beta_n$, então, para todo elemento $b \in K$, por $q(b)$ indicamos o elemento $\beta_0 b^n + \beta_1 b^{n-1} + \dots + \beta_n$ de K , onde $q(b)$ é o valor do polinômio $q(x)$ quando substituimos x por b . Diz-se que o elemento b satisfaz $q(x)$ se $q(b) = 0$. Assim, $a \in K$ é algébrico sobre F se existe um polinômio não nulo $p(x) \in F[x]$ que é satisfeito por a , ou seja, $p(a) = 0$.

Proposição 2.6.6. Seja K uma extensão de F , com $a \in K$ e seja M o conjunto de todos os subcorpos de K que contém F e a . O subcorpo obtido pela interseção de todos os subcorpos de K é o menor subcorpo de K que contém F e a .

Demonstração. Seja K uma extensão de F e seja $a \in K$. Considere M o conjunto de todos os subcorpos de K que contém F e a . Sabemos que M não é vazio, pois pelo menos K é um elemento de M . Temos ainda que a interseção de uma quantidade qualquer de subcorpos de K também é um subcorpo de K . Chamamos de $F(a)$ o subcorpo obtido pela interseção de todos os subcorpos de K . Temos que $F(a)$ contém F e a . Além disso, todo subcorpo de M contém $F(a)$ e, ao mesmo tempo, $F(a)$ está em M . Assim, $F(a)$ é o menor subcorpo de K que contém F e a .

Descrivemos $F(a)$ de uma forma um pouco mais construtiva. Assim, considere todos os elementos em K que podem ser escritos na forma $\beta_0 + \beta_1 a + \dots + \beta_r a^r$, com $\beta_i \in F$ e r um número inteiro não negativo. Temos que, dados quaisquer dois elementos em K , um elemento pode ser dividido pelo outro desde que o último seja diferente de zero. Seja U o conjunto de todas estas frações. Omitimos aqui, mas é possível demonstrar que U é um subcorpo de K .

Observe que, U contém F e a , ou seja, $U \supset F(a)$. Temos também que qualquer subcorpo de K que contém F e a necessariamente contém todos os elementos $\beta_0 + \beta_1 a + \dots + \beta_r a^r$, onde $\beta_i \in F$. Como $F(a)$ contém todos esses elementos e é um subcorpo de K , então $F(a)$ contém todas as frações de tais elementos, ou seja, $F(a) \supset U$. Portanto, $U = F(a)$. \square

Teorema 2.6.7. O elemento $a \in K$ é algébrico sobre F se, e somente se, $F(a)$ é uma extensão finita de F .

Demonstração. Suponhamos que $a \in K$ seja algébrico em F . Por hipótese, a satisfaz algum polinômio não nulo em $F[x]$. Seja $p(x)$ um polinômio de $F[x]$ de grau positivo

e mínimo tal que $p(a) = 0$. Temos que $p(x)$ é irredutível sobre F , caso contrário teríamos $p(x) = f(x)g(x)$, onde $f(x), g(x) \in F[x]$, mas $p(a) = f(a)g(a) = 0$ e como $f(a)$ e $g(a)$ são elementos do corpo K , temos $f(a) = 0$ ou $g(a) = 0$, mas como $p(x)$ é de grau positivo e mínimo e $p(a) = 0$, concluímos que $gr(f(x)) \geq gr(p(x))$ ou $gr(g(x)) \geq gr(p(x))$. Portanto, $p(x)$ é irredutível.

Na sequência definimos a aplicação ψ de $F[x]$ em $F(a)$ da seguinte maneira. Para todo $h(x) \in F[x]$, temos $(h(x))\psi = h(a)$. Temos que ψ é um homomorfismo de anel, do anel $F[x]$ no corpo $F(a)$. O núcleo V de ψ é dado por $V = \{h(x) \in F[x] \mid h(a) = 0\}$. Note que, V é múltiplo de $p(x)$ e como $p(x)$ é irredutível, pelo Lema 2.4.12 temos que V é um ideal maximal de $F[x]$. Pelos Teoremas 2.2.20 e 2.2.18 $F[x]/V$ é um corpo e é isomorfo à imagem de $F[x]$ através de ψ . A imagem de $F[x]$ através de ψ é um subcorpo de $F(a)$. Esta imagem contém $x\psi = a$ e, para todo $\alpha \in F$, $\alpha\psi = \alpha$. Portanto, a imagem de $F[x]$ através de ψ é um subcorpo de $F(a)$ que contém F e a . Assim, pela definição de $F(a)$, concluímos que a imagem de $F[x]$ através de ψ é $F(a)$, ou seja, $F[x]/V$ é isomorfo a $F(a)$.

Portanto, $V = (p(x))$, o ideal gerado por $p(x)$. Assim, dizemos que a dimensão de $F[x]/V$ é igual ao $gr(p(x))$. Pelo isomorfismo entre $F[x]/V$ e $F(a)$ temos que $[F(a) : F] = gr(p(x))$. Concluímos que $[F(a) : F]$ é finito, ou melhor, $[F(a) : F]$ é igual ao grau do polinômio de grau mínimo satisfeito por a sobre F .

Agora, vamos supor que $F(a)$ seja uma extensão finita de F e que $[F(a) : F] = m$. Considerando os elementos $1, a, a^2, \dots, a^m$, temos que todos estão em $F(a)$, no total são $m+1$ elementos e são linearmente dependentes sobre F . Portanto, existem elementos $\alpha_0, \alpha_1, \dots, \alpha_m$, em F , não todos nulos, tais que $\alpha_0 \cdot 1 + \alpha_1 \cdot a + \alpha_2 \cdot a^2 + \dots + \alpha_m \cdot a^m = 0$. Logo, a é algébrico sobre F e satisfaz o polinômio não $p(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \dots + \alpha_m x^m$ em $F[x]$ de grau no máximo $[F(a) : F] = m$.

□

Definição 2.6.8. *O elemento $a \in K$ é dito algébrico de grau n sobre F se ele satisfaz um polinômio de grau n , mas não satisfaz nenhum polinômio não nulo de grau menor do que n .*

Teorema 2.6.9. *Se $a \in K$ é algébrico de grau n , então $[F(a) : F] = n$.*

Demonstração. Pela Definição 2.6.8, como $a \in K$ é algébrico de grau n , então ele satisfaz um polinômio de grau n e não satisfaz nenhum polinômio não nulo de grau menor do que n . Como $[F(a) : F]$ é igual ao grau do polinômio de grau mínimo satisfeito por a sobre F , então $[F(a) : F] = n$.

□

Teorema 2.6.10. *Se a e b em K são algébricos sobre F , então $a \pm b$, ab e a/b (se $b \neq 0$) são todos algébricos sobre F .*

Demonstração. Suponhamos que a seja algébrico de grau m sobre F e que b seja algébrico de grau n sobre F . Pelo Teorema 2.6.7, temos que $F(a)$ e $F(b)$ em K são extensões finitas sobre F . O subcorpo $T = F(a)$ de K é de grau m sobre F e o subcorpo $W = F(b)$ de K é de grau n sobre F , mas como T contém F , então $F(b)$ também é de grau no máximo n sobre T . Pelo Teorema 2.6.3, temos que $[W : F] = [W : T][T : F]$, portanto, $[W : F] \leq mn$ e então W é uma extensão finita de F . Temos que, a e b estão em W , logo $a \pm b$, ab e a/b (se $b \neq 0$) estão em W . Pelo Teorema 2.6.7, como $[W : F]$ é finito, temos que os elementos a e b são algébricos em F . \square

Na demonstração do teorema anterior fizemos duas extensões do corpo F , uma chamamos de $T = F(a)$ e a outra de $W = F(b)$. Agora, temos $N = (F(a))(b) = F(a, b)$. De maneira análoga, temos $F(b, a)$. É possível demonstrar que $F(a, b) = F(b, a)$, indutivamente, e assim podemos definir $F(a_1, a_2, \dots, a_n)$ para elementos $a_1, a_2, \dots, a_n \in K$.

Definição 2.6.11. *A extensão K de F é denominada uma extensão algébrica de F se todo elemento de K é algébrico sobre F .*

Teorema 2.6.12. *Se A é uma extensão algébrica de B e se B é uma extensão algébrica de C , então A é uma extensão algébrica de C .*

Demonstração. Seja a um elemento qualquer de A , mostramos que a satisfaz algum polinômio não trivial com coeficientes em C . Sabemos que a satisfaz um polinômio $p(x) = x^n + \alpha_1 x^{n-1} + \dots + \alpha_n$, com $\alpha_i \in B$ para $i = 1, 2, \dots, n$. Como B é uma extensão algébrica sobre C , utilizando várias vezes o Teorema 2.6.9 concluímos que $D = C(\alpha_1, \alpha_2, \dots, \alpha_n)$ é uma extensão algébrica finita de C . Como a satisfaz $p(x) = x^n + \alpha_1 x^{n-1} + \dots + \alpha_n$ cujos coeficientes estão em D , então a é algébrico sobre D , o que implica que a é algébrico sobre C . \square

Um caso particular envolvendo o teoremas anteriores é quando C é o corpo dos racionais e B é o corpo dos complexos.

Definição 2.6.13. *Um número complexo é algébrico se ele é algébrico sobre o corpo dos racionais.*

A aplicação do Teorema 2.6.10 nos números algébricos demonstra que eles formam um corpo, ou seja, a soma, o produto e o quociente entre números algébricos são

algébricos. No caso de utilizarmos o Teorema 2.6.12 juntamente com o “Teorema Fundamental da Álgebra”, verifica-se que as raízes de um polinômio, cujos coeficientes são números algébricos, também são números algébricos.

Capítulo 3

Raízes de Polinômios e a Teoria de Galois

Neste Capítulo apresentamos alguns resultados importantes sobre raízes de polinômios, para posteriormente abordarmos os elementos da Teoria de Galois e exemplificá-la. Nele, F e K são considerados corpos. Para mais detalhes, veja [4].

3.1 Raízes de Polinômios

Dado um polinômio $p(x)$ em $F[x]$, desejamos encontrar um corpo K que seja uma extensão de F na qual $p(x)$ tenha uma raiz. Temos que construir o corpo K .

Definição 3.1.1. *Se $p(x) \in F[x]$, então um elemento a , pertencente a alguma extensão de F , é dito raiz de $p(x)$ se $p(a) = 0$.*

Lema 3.1.2. *Se $p(x)$ está em $F[x]$ e se K é uma extensão de F , então para todo elemento $a \in K$ temos que $p(x) = (x - a)q(x) + p(a)$, onde $q(x) \in K[x]$ e $gr(q(x)) = gr(p(x)) - 1$.*

Demonstração. Como $F \subset K$ então $F[x] \subset K[x]$, assim temos que $p(x) \in K[x]$. Pelo algoritmo da divisão para polinômios em $K[x]$ (Teorema 2.4.9), temos que $p(x) = (x - a)q(x) + r(x)$, onde $q(x) \in K[x]$ e $r(x) = 0$ ou $gr(r(x)) < gr(x - a) = 1$, assim temos $r(x) = 0$ ou $gr(r(x)) = 0$, em ambos os casos temos $r(x) \in K$ e podemos

escrever $r(x) = r$. Assim $p(x) = (x - a)q(x) + r$ e $p(a) = (a - a)q(a) + r = r$. Logo, $p(x) = (x - a)q(x) + p(a)$. Sabendo que $p(a) = r$, então $p(a) = 0$ ou $gr(p(a)) = 0$, e observando que $gr(x - a) = 1$, pela regra do produto entre polinômios, temos que $gr(q(x)) = gr(p(x)) - 1$. \square

Corolário 3.1.3. *Seja K uma extensão de F , se $a \in K$ é uma raiz de $p(x)$ que está em $F[x]$, então em $K[x]$ temos que $(x - a) \mid p(x)$.*

Demonstração. Pelo Lema 3.1.2, temos que $p(x) = (x - a)q(x) + p(a)$ em $K[x]$. Como a é uma raiz de $p(x)$, então $p(a) = 0$, logo $p(x) = (x - a)q(x)$. Donde concluímos que $(x - a) \mid p(x)$ em $K[x]$. \square

Definição 3.1.4. *Seja $p(x) \in F[x]$, dizemos que o elemento $a \in K$ é uma raiz de $p(x)$ com multiplicidade m se $(x - a)^m \mid p(x)$, mas $(x - a)^{m+1} \nmid p(x)$.*

Lema 3.1.5. *Um polinômio de grau n sobre um corpo pode ter no máximo n raízes sobre qualquer extensão deste corpo.*

Demonstração. Seja $p(x)$ um polinômio de grau n no corpo F . Provamos o lema por indução sobre n . Inicialmente, se $p(x)$ for de grau 1, então ele é da forma $ax + b$, onde $a, b \in F$ e $a \neq 0$. Todo a' tal que $p(a') = 0$ resulta em $aa' + b = 0$, ou seja, $a' = -\frac{b}{a}$. Portanto, para $p(x)$ de grau 1, temos que a única raiz é $-\frac{b}{a}$.

Vamos supor que o Lema seja verdadeiro em qualquer corpo e para todos os polinômios com grau menor que n , agora mostramos que para $p(x)$ de grau n o número de raízes é menor ou igual a n . Seja K uma extensão de F . Se $p(x)$ não possui raízes, não há mais o que demonstrar, pois 0 é menor ou igual a n . Portanto, suponhamos que $p(x)$ possua pelo menos uma raiz a e que essa raiz seja de multiplicidade m . Pela Definição 3.1.4, $(x - a)^m \mid p(x)$, assim temos $m \leq n$. Como $p(x) = (x - a)^m q(x)$, onde $q(x) \in K[x]$ temos que $gr(q(x)) = n - m$. E ainda, como $(x - a)^{m+1} \nmid p(x)$ concluímos que $(x - a) \nmid q(x)$, portanto a não é raiz de $q(x)$. Se $b \neq a$ é raiz de $p(x)$ em K , então $0 = (b - a)^m q(b)$, como $b - a \neq 0$, então $q(b) = 0$, ou seja, qualquer raiz de $p(x)$, em K , diferente de a é uma raiz de $q(x)$. Como $q(x)$ possui grau $n - m < n$, então $q(x)$ tem no máximo $n - m$ raízes em K , que junto com a raiz a contada m vezes, resulta que $p(x)$ possui no máximo $n - m + m = n$ raízes em K . \square

Agora determinamos extensões convenientes de F onde os polinômios possuem raízes, para assim analisar tais extensões e chegarmos a alguns resultados interessantes.

Teorema 3.1.6. *Se $p(x)$ é um polinômio irredutível em $F[x]$ e de grau $n \geq 1$, então existe uma extensão E de F , onde $[E : F] = n$ e $p(x)$ possui uma raiz.*

Demonstração. Seja $F[x]$ o anel dos polinômios em x sobre F e $V = (p(x))$ o ideal de $F[x]$ gerado por $p(x)$. Pelo Lema 2.2.19, V é o ideal maximal de $F[x]$ gerado por $p(x)$ e pelo Teorema 2.2.20, $F[x]/V$ é um corpo.

Tomemos \bar{F} a imagem de F em E , ou seja, $\bar{F} = \{\alpha + V, \text{ onde } \alpha \in F\}$ que é um corpo isomorfo a F , pois se ψ é a aplicação de $F[x]$ em $F[x]/V = E$ definida por $(f(x))\psi = f(x) + V$, então a restrição de ψ a F induz a um isomorfismo de F em \bar{F} . Logo, $F \cong \bar{F}$ e podemos admitir E como uma extensão de F .

Observe que E é uma extensão finita de F de grau $n = gr(p(x))$, pois $1 + V, x + V, (x + V)^2 = x^2 + V, \dots, (x + V)^i = x^i + V, \dots, (x + V)^{n-1} = x^{n-1} + V$ formam uma base de E sobre F . Tomemos, no corpo E , $a = (x)\psi + V$. Dado $f(x) \in F[x]$, com $f(x) = \beta_0 + \beta_1 x + \dots + \beta_k x^k$, temos que $(f(x))\psi = (\beta_0)\psi + (\beta_1)\psi(x\psi) + \dots + (\beta_k)\psi((x)\psi)^k$ e substituindo $\beta_i\psi$ simplesmente por β_i obtemos $f(x)\psi = \beta_0 + \beta_1(a) + \dots + \beta_k(a)^k = f(a)$. Em particular, como $p(x) \in V$, $p(x) = 0$, mas $p(x) = p(a)$. Logo, concluímos que o elemento $a = (x)\psi$ em E é uma raiz de $p(x)$. \square

Corolário 3.1.7. *Se $f(x) \in F[x]$, então existe uma extensão finita E de F onde $f(x)$ tem uma raiz e ainda $[E : F] \leq gr(f(x))$.*

Demonstração. Seja $p(x)$ um fator irredutível de $f(x)$, assim toda raiz de $p(x)$ também é raiz de $f(x)$. Pelo Teorema 3.1.6, existe uma extensão E de F onde $[E : F] = gr(p(x)) \leq gr(f(x))$ onde $p(x)$ possui uma raiz e, conseqüentemente, $f(x)$ também possui uma raiz. \square

Teorema 3.1.8. *Seja $f(x) \in F[x]$ de grau $n \geq 1$. Existe uma extensão E de F , de grau no máximo $n!$, onde $f(x)$ possui n raízes.*

Demonstração. Pelo Corolário 3.1.7, existe uma extensão E_0 de F tal que $[E_0 : F] \leq gr(f(x)) = n$, onde $f(x)$ possui uma raiz x_0 . Assim, em $E_0[x]$, $f(x)$ pode ser fatorado na forma $f(x) = (x - x_0)g(x)$, onde $g(x)$ possui grau $n - 1$. Por indução, existe uma extensão E de E_0 , de grau no máximo $(n - 1)!$, onde $g(x)$ possui $n - 1$ raízes. Como as raízes de $f(x)$ ou é x_0 ou é uma raiz de $g(x)$, temos em E todas as raízes de $f(x)$. Assim, $[E : F] = [E : E_0][E_0 : F] \leq (n - 1)!n = n!$. \square

O Teorema 3.1.8 nos mostra que dado um polinômio $f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n$, com $a_0 \neq 0$, existe uma extensão finita E de F , onde $f(x)$ possui n raízes. Se as n

raízes em E são x_1, x_2, \dots, x_n , o polinômio $f(x)$ pode ser fatorado da seguinte forma: $f(x) = a_0(x - x_1)(x - x_2)\dots(x - x_n)$. Portanto, $f(x)$ decompõe-se completamente sobre E como um produto de fatores lineares.

Se E for uma extensão de F com grau mínimo, dizemos que E é o **corpo de raízes** sobre F para $f(x)$, onde $f(x)$ pode ser fatorado em produtos de fatores lineares sobre E . No entanto, não goza da mesma propriedade em nenhum subcorpo próprio de E .

Dados dois corpos de raízes E_1 e E_2 do mesmo polinômio $f(x)$ em $F[x]$, existe alguma relação entre eles? Nosso objetivo é mostrar que eles são isomorfos por um isomorfismo que deixa todo elemento de F fixo.

Sejam F e F' dois corpos e τ^* uma aplicação de F em F' , tal que a imagem de qualquer $\alpha \in F$ é α' , ou seja, $\alpha\tau^* = \alpha'$.

Utilizamos τ^* para estabelecer um isomorfismo entre $F[x]$ e $F'[x]$, assim $f(x) = a_0 + a_1x^1 + \dots + a_nx^n \in F[x]$ definimos τ^* por $f(x)\tau^* = (a_0 + a_1x^1 + \dots + a_nx^n)\tau^* = a'_0 + a'_1x^1 + \dots + a'_nx^n$.

Observe que se $f(x) = f_1(x) \cdot f_2(x) \dots f_k(x)$ onde $f_j(x) \in F[x]$ são irredutíveis sobre F com $j = 1, 2, \dots, k$, então $f(x)\tau^* = f_1(x)\tau^* \cdot f_2(x)\tau^* \dots f_k(x)\tau^*$ onde $f_j(x)\tau^* \in F'[x]$ são irredutíveis sobre F' , com $j = 1, 2, \dots, k$.

Em particular, se todas as raízes de $f(x)$ estão em K temos que cada $f_j(x)$ possui grau 1 e portanto $f_j(x)\tau^*$ também possui grau 1, daí segue que todas as raízes de $f_j(x)\tau^*$ estão em F' .

Lema 3.1.9. *A aplicação τ^* define um isomorfismo de $F[x]$ em $F'[t]$ tal que $\alpha\tau^* = \alpha'$ para todo $\alpha \in F$.*

Demonstração. Seja $f(x)$ um polinômio irredutível sobre F . Se α é uma raiz de $f(x) \in F[x]$, β é uma raiz de $f(t)\tau^* \in F'[t]$ e $gr(f(x)) = gr(f(t)\tau^*) = r$ segue que:

- (1) $F[\alpha] = \{a_0 + a_1\alpha^1 + \dots + a_{r-1}\alpha^{r-1} : a_i \in F\}$ e $1, \alpha, \alpha^2, \dots, \alpha^{r-1}$ é uma base vetorial $F[\alpha]$ sobre F .
- (2) $F'[\beta] = \{a'_0 + a'_1\beta^1 + \dots + a'_{r-1}\beta^{r-1} : a'_i \in F'\}$ e $1, \beta, \beta^2, \dots, \beta^{r-1}$ é uma base vetorial $F'[\beta]$ sobre F' .

Agora é fácil ver que $\tau^* : F[\alpha] \rightarrow F'[\beta]$ definido por $\tau(a_0 + a_1\alpha^1 + \dots + a_{r-1}\alpha^{r-1}) = \tau(a_0) + \tau(a_1)\beta + \dots + \tau(a_{r-1})\beta^{r-1}$ é um isomorfismo do corpo $F[x]$ sobre o corpo $F'[t]$. \square

Indicamos $f(x)\tau^* = f'(t)$. O Lema 3.1.9 implica que a fatoração de $f(x)$ em $F[x]$ resulta em fatorações iguais de $f'(t)$ em $F'[t]$ e vice versa.

Lema 3.1.10. *Existe um isomorfismo τ^{**} de $F[x]/(f(x))$ em $F'[t]/(f'(t))$ com a propriedade de que $\alpha\tau^{**} = \alpha'$ para todo $\alpha \in F$.*

Demonstração. Inicialmente, deixamos claro a última parte do enunciado do Lema. Podemos considerar F como imerso em $F[x]/(f(x))$ identificando o elemento $\alpha \in F$ como a classe lateral $\alpha + (f(x))$ em $F[x]/(f(x))$. Da mesma forma, podemos considerar F' em $F'[t]/(f'(t))$. O isomorfismo τ^{**} é então suposto satisfazer $[\alpha + (f(x))]\tau^{**} = \alpha' + (f'(t))$.

Procuramos um isomorfismo τ^{**} de $F[x]/(f(x))$ em $F'[t]/(f'(t))$. O mais simples e natural é supor que τ^{**} seja definido por $[g(x) + (f(x))]\tau^{**} = g'(t) + (f'(t))$ para cada $g(x) \in F[x]$. Não prolongamos nos detalhes necessários para demonstrar que τ^{**} está assim bem definido e é um isomorfismo de $F[x]/(f(x))$ em $F'[t]/(f'(t))$ e possui as propriedades necessárias para cumprir a declaração do Lema. \square

O nosso objetivo nesse momento é mostrar a unicidade de corpos de raízes e os Lemas 3.1.9 e 3.1.10 são fundamentais nessa tarefa, uma vez que eles auxiliam na demonstração do teorema a seguir.

Teorema 3.1.11. *Se $p(x)$ é irredutível em $F[x]$ e se u é uma raiz de $p(x)$ então $F(u)$ é isomorfo a $F'(v)$ onde v é uma raiz de $p'(t)$. E ainda, o isomorfismo pode ser escolhido de modo que:*

(1) $u\sigma = v$.

(2) $\alpha\sigma = \alpha'$, para todo $\alpha \in F$.

Demonstração. Seja u uma raiz do polinômio $p(x)$ em alguma extensão K de F . Seja $M = \{f(x) \in F[x]/f(u) = 0\}$. Temos que M é um ideal de $F[x]$ e $M \neq f(x)$. Como $p(x) \in M$ e é irredutível, então $M = (p(x))$. Agora, levemos $F[x]$ em $F(u) \subset K$ pela aplicação ψ definida por $q(x)\psi = q(u)$ para todo $q(x) \in F[x]$. O núcleo de ψ é $M = (p(x))$. Pelo teorema fundamental do homomorfismo para anéis, existe um isomorfismo ψ^* de $F[x]/(f(x))$ em $F(u)$. Observe que $\alpha\psi^* = \alpha$ para todo $\alpha \in F$. Assim, ψ^* é um isomorfismo de $F[x]/(p(x))$ em $F(u)$ que deixa todo elemento de F fixo e onde $u = [x + (p(x))]\psi^*$.

Como $p(x)$ é irredutível em $F[x]$ e $p'(t)$ é irredutível em $F'[t]$ então, pelo Lema 3.1.9, existe um isomorfismo θ^* de $F'[t]/(p'(t))$ em $F'(v)$ onde v é uma raiz de $p'(t)$, θ^* deixa todo elemento de F' fixo e $v = [t + p'(t)]\theta^*$.

Pelo Lema 3.1.10, existe um isomorfismo τ^{**} de $F[x]/(p(x))$ em $F'[t]/(p'(t))$ que equivale a τ sobre F e que leva $x + (p(x))$ em $t + (p'(t))$. Considere a aplicação $\sigma = (\psi^*)^{-1}\tau^{**}\theta^*$ de $F(u)$ sobre $F'(v)$:

$$F(u) \xrightarrow{(\psi^*)^{-1}} \frac{F[x]}{(p(x))} \xrightarrow{(\tau^{**})} \frac{F'[t]}{(p'(t))} \xrightarrow{(\theta^*)} F'(v)$$

Ela é um isomorfismo pois as aplicações ψ^* , τ^{**} e θ^* são isomorfismos.

$$u = [x + (p(x))]\psi^*$$

$$u\sigma = (u(\psi^*)^{-1})\tau^{**}\theta^* = [(x + (p(x))\psi^*)(\psi^*)^{-1}]\tau^{**}\theta^* = (x + p(x))\tau^{**}\theta^* = (t + (p'(t))\theta^* = v.$$

Para todo $\alpha \in F$, temos

$$\alpha\sigma = (\alpha(\psi^*)^{-1})\tau^{**}\theta^* = \alpha\tau^{**}\theta^* = \alpha'\theta^* = \alpha'.$$

Portanto, ψ é um isomorfismo que satisfaz todos os requisitos do teorema. □

A seguir enunciamos um dos principais teoremas para a Teoria de Galois.

Teorema 3.1.12. *Quaisquer corpos de raízes E e E' dos polinômios $f(x) \in F[x]$ e $f'(t) \in F'[t]$, respectivamente, são isomorfos por ϕ com a propriedade $\alpha\phi = \alpha'$ para todo $\alpha \in F$.*

Demonstração. Provamos por indução. Seja $[E : F] = 1$, então $E = F$, logo $f(x)$ decompõe-se num produto de fatores lineares sobre o próprio F . Pelo Lema 3.1.9, $f'(t)$ decompõe-se sobre F' num produto de fatores lineares, assim $E' \cong F'$. Portanto, $\phi = \tau$ é um isomorfismo de E em E' coincidente com τ sobre F .

Considere que o resultado seja válido para todo corpo F_0 e todo polinômio $f(x) \in F[x]$ desde que o grau seja menor que n , ou seja, $[E_0 : F_0] < n$.

Suponhamos que $[E : F] = n > 1$, onde E é um corpo de raízes de $f(x)$ sobre F . Como $n > 1$, temos que $f(x)$ possui um fator irredutível $p(x)$ de grau $r \geq 1$. Seja $p'(t)$ um fator irredutível de $p(t)$. Como E decompõe $f(x)$, um complemento de raízes de $f(x)$ e de raízes de $p(x)$ estão em E . Portanto, existe $u \in E$ tal que $p(u) = 0$. Pelo Teorema 2.6.9, $[F(u) : F] = r$. Da mesma forma, existe $v \in E'$ tal que $p'(v) = 0$. Assim, conforme o Teorema 3.1.11, existe um isomorfismo σ de $F(u)$ em $F'(v)$ com a propriedade $\alpha\sigma = \alpha'$, para todo $\alpha \in F$.

Com $[E : F(u)] = r > 1$, temos

$$[E : F(u)] = \frac{[E : F]}{[F(u) : F]} = \frac{n}{r} < n.$$

Afirmamos que E é um corpo de raízes de $f(x)$ considerado como um polinômio sobre $F_0 = F(u)$, pois como consideramos que E era um corpo de raízes de $f(x)$ em F , nenhum subcorpo de E , que contenha F_0 e portanto F , pode decompor $f(x)$. Analogamente, E' é um corpo de raízes de $f'(t)$ sobre $F'_0 = F'(v)$. Assim, pela hipótese de indução, existe um isomorfismo ϕ de E em E' , tal que $a\phi = a'$ para todo $a \in F_0$. Mas, para todo $\alpha \in F$, $\alpha\sigma = \alpha'$, logo $\alpha \in F \subset F_0$, assim $\alpha\phi = \alpha\sigma = \alpha'$.

Agora, seja $F = F'$ e seja τ a aplicação idêntica $\alpha\tau = \alpha$ para todo $\alpha \in F$. Suponhamos que E_1 e E_2 sejam dois corpos de raízes de $f(x)$ em $F[x]$. Considerando $E_1 = E \supset F$ e $E_2 = E' \supset F' = F$ e aplicando o teorema, resulta que E_1 e E_2 são isomorfos por um isomorfismo que deixa todo elemento de F fixo. □

Na sequência falamos um pouco mais sobre raízes de polinômios.

Definição 3.1.13. *Seja F um corpo qualquer e $F[x]$ o anel de polinômio em x sobre F , se $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in F[x]$, definimos a derivada de um polinômio $f(x)$, e indicamos por $f'(x)$, como sendo*

$$f'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + \dots + a_{n-1} \in F[x].$$

Note que se F é de característica $p \neq 0$, é possível que a derivada de x^p seja nula, ou seja, $px^{p-1} = 0$, o que mostra que, diferentemente do que estudamos em cálculo, a derivada de um polinômio pode ser zero mesmo que ele não seja uma constante. Mas, se F é de característica $p = 0$ e $f'(x) = 0$, então $f(x) = \alpha \in F$.

Se $f(x), g(x) \in F[x]$ e $k \in F$, segue imediatamente as seguintes regras:

- 1) $(f(x) + g(x))' = f'(x) + g'(x)$;
- 2) $(kf(x))' = kf'(x)$;
- 3) $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

Lema 3.1.14. *O polinômio $f(x) \in F[x]$ tem um raiz múltipla se, e só se, $f(x)$ e $f'(x)$ possuem um fator comum não trivial (de grau positivo).*

Demonstração. Inicialmente, observe que se $f(x)$ e $g(x) \in F[x]$ tem um fator comum não trivial em $K[x]$, onde K é uma extensão de F , então eles tem um fator comum não trivial em $F[x]$. Isso ocorre, pois, caso eles fossem primos entre si como elementos

de $F[x]$, encontramos dois polinômios $m(x)$ e $n(x)$ tais que $m(x)f(x) + n(x)g(x) = 1$, relação que também vale para aqueles elementos em $K[x]$, assim eles também são primos entre si em $K[x]$.

Desse modo, podemos admitir, sem perda de generalidade, que as raízes de $f(x)$ estão todas em F , caso contrário, estendemos F a K obtendo o corpo de raízes de $f(x)$. Se $f(x)$ possui raízes múltipla α , então $f(x) = (x - \alpha)^m g(x)$, onde $m > 1$. Nesse caso, $f'(x) = m(x - \alpha)^{m-1}g(x) + (x - \alpha)^m g'(x)$, ou seja, $f'(x) = (x - \alpha)r(x)$, pois $m > 1$, o que indica que $f(x)$ e $f'(x)$ possuem o fator comum $x - \alpha$.

Por outro lado, se $f(x)$ não possui raiz múltipla, então $f(x) = (x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n)$, onde x_i são todos distintos. Desta forma

$$f'(x) = \sum_{i=1}^n (x - \alpha_1)\dots \underline{(x - \alpha_i)} \dots (x - \alpha_n)$$

onde o termo sublinhado é omitido em cada termo da somatória. Assim, é notório que nenhuma raiz de $f(x)$ é raiz de $f'(x)$, para

$$f'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j) \neq 0$$

uma vez que as raízes são todas distintas. No entanto, se $f(x)$ e $f'(x)$ possuem um fator comum não trivial, eles possuem uma raiz comum, que é a raiz desse fator comum. Assim, temos que $f(x)$ e $f'(x)$ não possuem nenhum fator comum não trivial. \square

Definição 3.1.15. *A extensão K de F é uma extensão simples de F se, para algum $\alpha \in K$, tivermos $K = F(\alpha)$.*

Teorema 3.1.16. *Se F é de característica 0 e a e b são algébricos sobre F , então existe $c \in F(a, b)$ tal que $F(a, b) = F(c)$.*

Demonstração. Seja $f(x)$ um polinômio de grau m satisfeito por a e seja $g(x)$ um polinômio de grau n satisfeito por b , ambos irreduzíveis sobre F . Tomemos a extensão K de F onde $f(x)$ e $g(x)$ podem ser fatorados completamente. O fato de F ter característica 0 implica que todas as raízes são distintas, tanto as de $f(x)$ quanto as de $g(x)$. Considere $a = a_1, a_2, \dots, a_m$ as raízes de $f(x)$ e $b = b_1, b_2, \dots, b_n$ as de $g(x)$.

Dado $j \neq 1$, então $b_j \neq b_1 = b$, assim a equação $a_i + \lambda b_j = a_1 + \lambda b_1 = a + \lambda b$, possui uma única solução em K , que é

$$\lambda = \frac{a_i - a}{b - b_j}.$$

Como F é de característica 0 então ele possui um número infinito de elementos. Portanto, podemos encontrar um elemento $\gamma \in F$ tal que $a_i + \gamma b_j$ contenha $a + \gamma b$ para todo i e para todo $j \neq 1$. Seja $c = a + \gamma b$, afirmamos que $F(c) = F(a, b)$. Como $c \in F(a, b)$ então $F(c) \subset F(a, b)$. Queremos mostrar agora que $F(a, b) \subset F(c)$.

Por hipótese, temos que b satisfaz o polinômio $g(x)$ sobre F , portanto satisfaz $g(x)$ considerando como um polinômio sobre $K = F(c)$. Observe que, se $h(x) = f(c - \gamma x)$ então $h(x) \in K[x]$ e $h(b) = f(c - \gamma b) = f(a) = 0$, pois $a = c - \gamma b$. Assim, em alguma extensão de K , $f(x)$ e $g(x)$ possuem $x - b$ como fator comum. E mais, apesar de omitirmos aqui, é possível mostrar que $x - b$ é na verdade o máximo divisor comum desses polinômios (ver na demonstração em [4]). Assim $x - b \in K[x]$, logo $b \in K$ e como $K = F(c)$, temos que $b \in F(c)$. Tendo $a = c - \gamma b$, $b, c \in F(c)$ e $\gamma \in F \subset F(c)$, logo $a \in F(c)$ e $F(a, b) \subset F(c)$. Concluimos assim que $F(a, b) = F(c)$. \square

Corolário 3.1.17. *Toda extensão finita de um corpo de característica 0 é uma extensão simples.*

Utilizando a indução é possível estender o resultado sobre 2 elementos para qualquer número finito, ou seja, se $\alpha_1, \alpha_2, \dots, \alpha_n$ são algébricos sobre F , então existe um elemento $c \in F(\alpha_1, \alpha_2, \dots, \alpha_n)$ tal que $F(c) = F(\alpha_1, \alpha_2, \dots, \alpha_n)$.

3.2 Os Elementos da Teoria de Galois

Dado $p(x) \in F[x]$, associamos $p(x)$ a um grupo que é denominado grupo de Galois de $p(x)$, que é um grupo de permutações das raízes do polinômio $p(x)$.

Teorema 3.2.1. *Se K é um corpo e se $\sigma_1, \dots, \sigma_n$ são automorfismos distintos em K , então não existem elementos a_1, a_2, \dots, a_n , não todos nulos em K , tais que $a_1\sigma_1(u) + a_2\sigma_2(u) + \dots + a_n\sigma_n(u) = 0$ para todo $u \in K$.*

Demonstração. Suponhamos que fosse possível encontrar elementos $a_1, a_2, \dots, a_n \in K$, não todos nulos tais que $a_1\sigma_1(u) + a_2\sigma_2(u) + \dots + a_n\sigma_n(u) = 0$ para todo $u \in K$. Então, é possível encontrar uma relação desta para um número mínimo de elementos não nulos. Sendo m essa relação mínima, temos

$$a_1\sigma_1(u) + a_2\sigma_2(u) + \dots + a_m\sigma_m(u) = 0 \tag{3.1}$$

onde a_1, a_2, \dots, a_m são todos não nulos.

Se $m = 1$, então $a_1\sigma_1 = 0$ para todo $u \in K$, portanto $a_1 = 0$, o que contradiz a hipótese. Portanto, seja $m > 1$. Como os automorfismos são distintos, existe um elemento $b \in K$ tal que $\sigma_1(b) \neq \sigma_m(b)$. Como $bu \in K$, temos que a relação (3.1) também vale para bu , ou seja,

$$a_1\sigma_1(bu) + a_2\sigma_2(bu) + \dots + a_m\sigma_m(bu) = 0 \text{ para todo } u \in K.$$

Ou ainda,

$$a_1\sigma_1(b)\sigma_1(u) + a_2\sigma_2(b)\sigma_2(u) + \dots + a_m\sigma_m(b)\sigma_m(u) = 0 \text{ para todo } u \in K. \quad (3.2)$$

Multiplicando a relação (3.1) por $\sigma_1(b)$ e subtraindo da relação (3.2) obtemos

$$a_2(\sigma_2(b) - \sigma_1(b))\sigma_2(u) + \dots + a_m(\sigma_m(b) - \sigma_1(b))\sigma_m(u) = 0. \quad (3.3)$$

Na relação (3.3), fazemos $c_i = a_i(\sigma_i(b) - \sigma_1(b))$ para $i = 1, 2, \dots, m$, temos

$$c_2\sigma_2(u) + \dots + c_m\sigma_m(u) = 0.$$

Mas, $c_m = a_m(\sigma_m(b) - \sigma_1(b)) \neq 0$, pois $a_m \neq 0$ e, como $\sigma_1(b) \neq \sigma_m(b)$, então $\sigma_m(b) - \sigma_1(b) \neq 0$. Portanto, isso produz uma relação menor que contraria a escolha feita inicialmente, demonstrando assim o teorema. \square

Definição 3.2.2. Corpo fixo - Se G é um grupo de automorfismo de K , então o corpo fixo de G é o conjunto de todos os elementos $x \in K$, tais que $\sigma(x) = x$ para todo $\sigma \in G$, é denotado por K_G .

Lema 3.2.3. O corpo fixo de G é um subcorpo de K .

Demonstração. Considere a e b no corpo fixo de G , logo para todo $\sigma \in G$ temos $\sigma(a) = a$, $\sigma(b) = b$, $\sigma(a \pm b) = \sigma(a) \pm \sigma(b) = a \pm b$ e $\sigma(ab) = \sigma(a)\sigma(b) = ab$. Portanto, $a \pm b$ e ab estão no corpo fixo de G . Se $b \neq 0$, temos $\sigma(b^{-1}) = \sigma(b)^{-1} = b^{-1}$, o que mostra que b^{-1} também está no corpo fixo de G . Logo, verificamos que G é um subcorpo de K . \square

Definição 3.2.4. Seja K um corpo e F um subcorpo de K , então $G(K, F)$ representa o grupo dos automorfismos de K relativos a F , que é o conjunto de todos os automorfismos de K que deixam fixos todo elemento de F . Assim, o automorfismo $\sigma \in K$ está em $G(K, F)$ se, e somente se, $\sigma(a) = a$ para todo $a \in F$.

Lema 3.2.5. $G(K, F)$ é um subgrupo do grupo dos automorfismos de K , $\text{Aut}(K)$.

Demonstração. É claro que o conjunto dos automorfismos de K é um grupo. Se σ e τ são automorfismos de K que fixam F , então $\sigma\tau$ e σ^{-1} são o mesmo em F , o que mostra que $G(K, F)$ é um subgrupo. \square

Exemplo 3.2.6. Sejam K o corpo dos complexos e F o corpo dos números reais, vamos calcular $G(K, F)$.

Solução. Se σ é um automorfismo qualquer de K , então como $i^2 = -1$ temos que $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$, onde $\sigma(i) = \pm i$. E ainda, dado que σ deixa todo número real fixo, então para todo $a + bi$, como a e b números reais, temos que $\sigma(a + bi) = \sigma(a) + \sigma(b)\sigma(i) = a \pm bi$. Então, temos duas possibilidades, a aplicação $\sigma_1(a + bi) = a + bi$, que é um automorfismo idêntico e $\sigma_2(a + bi) = a - bi$, onde σ_2 é a conjugação complexa. Logo, $G(K, F)$ é um grupo de ordem 2.

Observe que se $a + bi$ está no corpo fixo de $G(K, F)$, então $a + bi = \sigma_2(a + bi) = a - bi$, logo $b = 0$ e $a = a - bi \in F$. Portanto, o corpo fixo de $G(K, F)$ é o próprio F .

Exemplo 3.2.7. Seja F_0 o corpo dos racionais e seja $K = F_0(\sqrt[3]{2})$, na qual $\sqrt[3]{2}$ é a raiz cúbica de 2. Vamos calcular $G(K, F)$.

Solução Temos que todo elemento em K é da forma $\alpha_0 + \alpha_1(\sqrt[3]{2}) + \alpha_2(\sqrt[3]{2})^2$, onde α_0 , α_1 e α_2 são números racionais.

Se σ é um automorfismo em K , então $(\sigma(\sqrt[3]{2}))^3 = \sigma(\sqrt[3]{2}^3) = \sigma(2) = 2$, onde $\sigma(\sqrt[3]{2})$ também é uma raiz cúbica de 2 que está em K . Mas, existe apenas uma raiz cúbica real de 2, e como K é um subcorpo do corpo real, então $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Logo, $\sigma(\alpha_0 + \alpha_1\sqrt[3]{2} + \alpha_2(\sqrt[3]{2})^2) = \alpha_0 + \alpha_1\sqrt[3]{2} + \alpha_2(\sqrt[3]{2})^2$, o que mostra que σ é um automorfismo identidade de K . Portanto, o corpo fixo de $G(K, F)$ não é F_0 e sim todo K .

Teorema 3.2.8. Se K é uma extensão finita de F , então $G(K, F)$ é um grupo finito e sua ordem $|G(K, F)|$ é tal que $|G(K, F)| \leq [K : F]$.

Demonstração. Se $[K : F] = n$ e suponhamos que a_1, a_2, \dots, a_n seja uma base de K sobre F . Suponhamos ainda que seja possível encontrar $n + 1$ automorfismos $\sigma_1, \sigma_2, \dots, \sigma_{n+1}$ diferentes em $G(K, F)$. Temos que, o sistema de n equações lineares homogêneas nas $n + 1$ incógnitas x_1, x_2, \dots, x_{n+1} , possui uma solução não trivial $x_1 = s_1, x_2 = s_2, \dots, x_{n+1} = s_{n+1}$, ambos não nulos em K . Temos o sistema

$$\left\{ \begin{array}{l} \sigma_1(a_1)x_1 + \sigma_2(a_1)x_2 + \dots + \sigma_{n+1}(a_1)x_{n+1} = 0 \\ \vdots \\ \sigma_1(a_i)x_1 + \sigma_2(a_i)x_2 + \dots + \sigma_{n+1}(a_i)x_{n+1} = 0 \\ \vdots \\ \sigma_1(a_n)x_1 + \sigma_2(a_n)x_2 + \dots + \sigma_{n+1}(a_n)x_{n+1} = 0 \end{array} \right.$$

Que resulta em

$$s_1\sigma_1(a_i) + s_2\sigma_2(a_i) + \dots + s_{n+1}\sigma_{n+1}(a_i) = 0, \text{ para } i = 1, 2, \dots, n. \quad (3.4)$$

Como todo elemento em F é deixado fixo em relação a cada σ_i e como um elemento qualquer t em K é da forma $t = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n$, onde $\alpha_1, \alpha_2, \dots, \alpha_n \in F$, então em (3.4) obtemos $s_1\sigma_1(t) + s_2\sigma_2(t) + \dots + s_{n+1}\sigma_{n+1}(t) = 0$ para todo $t \in F$, o que contradiz o Teorema 3.2.1. Portanto, podemos concluir que $|G(K, F)| \leq [K : F]$. \square

No Teorema 3.2.8 obtemos uma cota superior para a ordem de $G(K, F)$ e temos que $|G(K, F)| \leq n!$. Essa cota superior é boa, pois existem exemplos de K e F tais que $|G(K, F)| = n!$, conforme [4].

Seja S_n o grupo simétrico de grau n considerado como operando o conjunto $[1, 2, \dots, n]$. Dado $\sigma \in S_n$ e i um inteiro onde $1 \leq i \leq n$, seja $\sigma(i)$ a imagem de i . Podemos fazer S_n operar sobre $F(x_1, \dots, x_n)$ da seguinte forma: dado $\sigma \in S_n$ e $r(x_1, \dots, x_n) \in F(x_1, \dots, x_n)$ definimos a aplicação que leva $r(x_1, \dots, x_n)$ em $r(x_{\sigma(1)}, \dots, x_{\sigma(n)})$, que será a aplicação de $F(x_1, \dots, x_n)$ em si mesmo por σ . Estas aplicações definem um automorfismo de $F(x_1, \dots, x_n)$. O corpo fixo de $F(x_1, \dots, x_n)$ com respeito a S_n , consiste de todas as funções racionais $r(x_1, \dots, x_n)$ tais que $r(x_1, \dots, x_n) = r(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ para todo $\sigma \in S_n$. Mas estes são os elementos em $F(x_1, \dots, x_n)$ que são conhecidos como *funções racionais simétricas*. Sendo o corpo fixo de S_n elas formam um subcorpo de $F(x_1, \dots, x_n)$, denominado *corpo das funções racionais simétricas*, que indicaremos por S .

Em S podemos construir certas funções a partir de x_1, \dots, x_n conhecidas como funções simétricas elementares, que são definidas da seguinte maneira:

$$a_1 = x_1 + x_2 + \dots + x_n = \sum_i^n x_i$$

$$a_2 = \sum_{i < j} x_i x_j$$

$$a_3 = \sum_{i < j < k} x_i x_j x_k$$

⋮

$$a_n = x_1 x_2 \dots x_n$$

É possível verificar que essas funções são simétricas. Para $n = 2, 3$ e 4 temos:

- $n = 2$

$$a_1 = x_1 + x_2$$

$$a_2 = x_1 x_2$$

- $n = 3$

$$a_1 = x_1 + x_2 + x_3$$

$$a_2 = x_1 x_2 + x_1 x_3 + x_2 x_3$$

$$a_3 = x_1 x_2 x_3$$

- $n = 4$

$$a_1 = x_1 + x_2 + x_3 + x_4$$

$$a_2 = x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4$$

$$a_3 = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_3 x_4 + x_2 x_3 x_4$$

$$a_4 = x_1 x_2 x_3 x_4$$

Observe que:

Para $n = 2$, x_1 e x_2 são as raízes do polinômio $t^2 - a_1 t + a_2$;

Para $n = 3$, x_1, x_2 e x_3 são as raízes de $t^3 - a_1 t^2 + a_2 t - a_3$;

Para $n = 4$, x_1, x_2, x_3 e x_4 são as raízes de $t^4 - a_1 t^3 + a_2 t^2 - a_3 t + a_4$.

Como $a_1, \dots, a_n \in S$ o corpo $F(a_1, \dots, a_n)$ obtido pela união de a_1, \dots, a_n a F claramente está contido em S .

Teorema 3.2.9. *Seja F um corpo e $F(x_1, x_2, \dots, x_n)$ o corpo das funções racionais em x_1, x_2, \dots, x_n sobre F . Se S é o corpo das funções racionais simétricas, temos:*

- 1) $[F(x_1, \dots, x_n) : S] = n!$
- 2) $G(F(x_1, \dots, x_n), S) = S_n$, o grupo simétrico de grau n .
- 3) Se a_1, \dots, a_n são as funções simétricas elementares em x_1, x_2, \dots, x_n então $S = F(a_1, \dots, a_n)$.
- 4) $F(x_1, \dots, x_n)$ é o corpo das raízes sobre $[F(a_1, \dots, a_n) = S]$ do polinômio $t^n - a_1 t^{n-1} + a_2 t^{n-2} + \dots + (-1)^n a_n$.

Demonstração. Como S_n é um grupo de automorfismos de $F(x_1, \dots, x_n)$ que deixa S fixo, temos que $S_n \subset G(F(x_1, \dots, x_n), S)$. Assim, pelo Teorema 3.2.8, $[F(x_1, \dots, x_n) : S] \geq |G(F(x_1, \dots, x_n), S)| > |S_n| = n!$. Observe que o polinômio $p(t) = t^n - a_1 t^{n-1} + a_2 t^{n-2} + \dots + (-1)^n a_n$ que tem coeficientes em $[F(a_1, \dots, a_n)]$ é escrito na forma fatorada sobre $[F(a_1, \dots, a_n) = S]$ como $p(t) = (t-x_1)(t-x_2)\dots(t-x_n)$, logo $p(t)$ que possui grau n , fatora-se como um produto de fatores lineares sobre $F(x_1, \dots, x_n)$. No entanto, não é possível fatorar $p(t)$ sobre um subcorpo de $F(x_1, \dots, x_n)$ que contém $F(a_1, \dots, a_n)$, pois caso contrário esse subcorpo teria de conter F e todas as raízes de $p(t)$, que são x_1, \dots, x_n . Assim, esse subcorpo seria o próprio $F(x_1, \dots, x_n)$. Portanto, temos que $F(x_1, \dots, x_n)$ é o corpo de raízes de $p(t) = t^n - a_1 t^{n-1} + a_2 t^{n-2} + \dots + (-1)^n a_n$ sobre F . Como $p(t)$ é de grau n , pelo Teorema 3.1.8 temos $[F(x_1, \dots, x_n) : S] \leq n!$. Assim, concluímos que $[F(x_1, \dots, x_n) : S] = n!$. \square

Definição 3.2.10. *Dizemos que K é uma **extensão normal** de F se K é uma extensão finita de F tal que F seja o corpo fixo de $G(K, F)$.*

O Exemplo 3.2.6 é um caso de extensão normal. A hipótese de normalidade permite calcular o tamanho do corpo fixo de qualquer subgrupo de $G(K, F)$, melhorando assim o Teorema 3.2.8 de uma desigualdade para uma igualdade.

Teorema 3.2.11. *Seja K uma extensão normal de F e seja H um subgrupo de $G(K, F)$. Tomando como corpo fixo $K_H = \{x \in K \mid \sigma(x) = x \text{ para todo } \sigma \in H\}$, temos:*

$$(1) [K : K_H] = |H|$$

$$(2) \quad H = G(K, K_H)$$

Em particular, para $H = G(K, F)$, $[K : F] = |G(K, F)|$.

Demonstração. Uma vez que todo elemento de H deixa todo elemento K_H fixo, então $H \subset G(K, K_H)$. Pelo Teorema 3.2.8 temos $[K : K_H] \geq |G(K, K_H)|$, mas como $|G(K, K_H)| \geq |H|$ obtemos a desigualdade $[K : K_H] \geq |G(K, K_H)| \geq |H|$. Mostramos que $[K : K_H] = |H|$, conseqüentemente, temos que $|H| = |G(K, K_H)|$ e como um subgrupo de $G(K, K_H)$ tendo a mesma ordem de $|G(K, K_H)|$, obtemos $H = G(K, K_H)$.

Segundo o Teorema 3.1.16, existe $a \in K$ tal que $K = K_H(a)$, onde a satisfaz um polinômio irredutível em K_H de grau $n = [K : K_H]$ e não satisfaz qualquer polinômio não trivial de grau menor.

Sejam $\sigma_1, \sigma_2, \dots, \sigma_h$ os elementos de H , onde σ_1 é o elemento unidade de $G(K, K_H)$ e $h = |H|$. Considere $a = \sigma_1(a), \sigma_2(a), \dots, \sigma_h(a)$, que são:

$$\begin{aligned} \alpha_1 &= \sigma_1(a) + \sigma_2(a) + \dots + \sigma_h(a) = \sum_i^h \sigma_i(a); \\ \alpha_2 &= \sum_{i < j} \sigma_i \sigma_j; \\ &\vdots \\ \alpha_h &= \sigma_1(a) \sigma_2(a) \dots \sigma_h(a). \end{aligned}$$

É possível mostrar que α_i é constante em relação a todo $\sigma \in H$. Logo, pela definição de K_H , $\sigma_1, \sigma_2, \dots, \sigma_h \in K_H$. Mas, $a, \sigma_2(a), \dots, \sigma_h(a)$, são raízes do polinômio $p(x) = (x - \sigma_1(a))(x - \sigma_2(a)) \dots (x - \sigma_h(a)) = x^h - \alpha_1 x^{h-1} + \alpha_2 x^{h-2} + \dots + (-1)^h \alpha_h$, onde os coeficientes estão em K_H . Pela natureza de a , temos $h \geq n = [K : K_H]$ e, portanto, $|H| \geq [K : K_H]$. Mas, já sabemos que $|H| \leq [K : K_H]$. Assim, chegamos a conclusão que $|H| = [K : K_H]$.

Se $H = G(K, F)$, pela normalidade de K em F , temos $K_H = F$ e, conseqüentemente, obtemos $[K : F] = |G(K, F)|$. □

Lema 3.2.12. *Seja K o corpo de raízes de $f(x)$ em $F[x]$ e seja $p(x)$ um fator irredutível de $f(x)$ em $F[x]$. Se as raízes de $p(x)$ são a_1, a_2, \dots, a_r , então para cada i existe um automorfismo σ_i em $G(K, F)$ tal que $\sigma_i(a_1) = a_i$.*

Demonstração. Como toda raiz de $p(x)$ é uma raiz de $f(x)$ então tal raiz está em K . Seja, a_1 e a_i duas raízes quaisquer de $p(x)$. Pelo Teorema 3.1.11, existe um isomorfismo

τ de $F_1 = F(a_1)$ em $F'_1 = F(a_i)$ que leva a_1 em a_i e deixa todo elemento de F fixo. Mas, K é o corpo de raízes de $f(x)$ considerado como um polinômio sobre F_1 e também considerado sobre F'_1 . Pelo Teorema 3.1.12, existe um isomorfismo σ_i de K em K (automorfismo) que coincide com τ sobre F_1 . Portanto, $\sigma_i(a_1) = \tau(a_i)$ e σ_i deixa todo elemento de F fixo. \square

Teorema 3.2.13. *K é uma extensão normal sobre F se, e somente se, K é o corpo de raízes de algum polinômio sobre F .*

Demonstração. Suponhamos que K seja uma extensão normal sobre F . Pelo Teorema 3.1.16, temos que $K = f(a)$. Considerando o polinômio $p(x) = (x - \sigma_1(a))(x - \sigma_2(a)) \dots (x - \sigma_n(a))$ sobre K , onde $\sigma_1, \sigma_2, \dots, \sigma_n \in G(K, F)$, quando desenvolvemos $p(x)$ obtemos $p(x) = x^n - \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \dots + (-1)^n \alpha_n$, onde $\alpha_1, \dots, \alpha_n$ são funções simétricas elementares em $a = \sigma_1(a), \sigma_2(a), \dots, \sigma_n(a)$. Portanto, os elementos $\alpha_1, \alpha_2, \dots, \alpha_n$, são constantes em relação a cada $\sigma \in G(K, F)$, onde pela normalidade em K sobre F , estão todos em F . Logo, temos que K decompõe o polinômio $p(x) \in F[x]$ num produto de fatores lineares. Uma vez que a é uma raiz de $p(x)$ e gera K sobre F , então a não pode estar em nenhum subcorpo próprio de K que contém F . Portanto, K é o corpo de raízes de $p(x)$ sobre F .

Reciprocamente, admita que K seja o corpo de raízes de $f(x)$ sobre F . Devemos provar que K é normal sobre F , para isso façamos indução sobre $[K : F]$, admitindo que para todo par de corpos K_1, F_1 de grau menor que $[K : F]$, sempre que K_1 for o corpo de raízes de F_1 de um polinômio $F_1[x]$, então K_1 é normal sobre F_1 .

Se $f(x) \in F[x]$ decompõe-se como um produto de fatores lineares sobre F , então $K = F$, que é uma extensão normal de F . Assim, considere que $f(x)$ possua um fator irreduzível $p(x) \in F[x]$ de grau $r > 1$. Todas as r raízes distintas $\alpha_1, \alpha_2, \dots, \alpha_r$ de $p(x)$ estão em K , que é o corpo de raízes de $f(x)$ considerado como um polinômio sobre $F(\alpha_1)$. Já que

$$[K : F(\alpha_1)] = \frac{[K : F]}{[F(\alpha_1) : F]} = \frac{n}{r} < n.$$

Então, pela hipótese de indução, K é uma extensão normal de $F[\alpha_1]$.

Seja $\delta \in K$ conservado fixo por todo automorfismo $\sigma \in G(K, F)$. Devemos mostrar que δ está em F . Como todo automorfismo em $G(K, F(\alpha_1))$ deixa F fixo, também deixa δ fixo e pela normalidade de K sobre $F(\alpha_1)$ temos que δ está fixo em $F(\alpha_1)$. Logo,

$$\delta = \lambda_0 + \lambda_1\alpha_1 + \lambda_2\alpha_1^2 + \dots + \lambda_{r-1}\alpha_1^{r-1}, \text{ onde } \lambda_0, \dots, \lambda_{r-1} \in F. \quad (3.5)$$

Pelo Lema 3.2.12, existe um automorfismo $\sigma_i \in G(K : F)$ tal que $\sigma_i(\alpha_1) = \alpha_i$. Aplicando esse lema em (3.5), obtemos

$$\delta = \lambda_0 + \lambda_1\alpha_i + \lambda_2\alpha_i^2 + \dots + \lambda_{r-1}\alpha_i^{r-1}, \text{ onde } i = 1, 2, \dots, r.$$

Assim o polinômio $q(x) = \lambda_{r-1}x^{r-1} + \lambda_{r-2}x^{r-2} + \dots + \lambda_1x + (\lambda_0 - \delta)$, em $K[x]$, com grau máximo igual a $r - 1$, contém as r raízes distintas $\alpha_1, \dots, \alpha_r$. No entanto, isto somente acontece se todos seus coeficientes são nulos, em especial $\lambda_0 - \delta = 0$, ou seja, $\lambda_0 = \delta$ e, portanto, δ está em F . \square

Definição 3.2.14. Grupo de Galois - Sejam $f(x)$ um polinômio em $F[x]$ e K o corpo de raízes sobre F . O Grupo de Galois de $f(x)$ é o grupo $G(K, F)$ de todas os automorfismos de K que deixam todo elemento de F fixo.

O Grupo de Galois de $f(x)$ pode ser considerado como um grupo de permutações de suas raízes, uma vez que se α é uma raiz de $f(x)$ e se $\sigma \in G(K, F)$, então $\sigma(\alpha)$ também é uma raiz de $f(x)$.

Definição 3.2.15. Corpo Intermediário - Dizemos que L é um corpo intermediário se $K \subseteq L \subseteq F$. Para cada corpo intermediário é associado um subgrupo $G(L, F)$, que contém todos os automorfismos do Grupo de Galois que fixam todos os elementos de L , ou seja, $G(L, F) = \{\sigma \in G \mid \sigma(x) = x, \text{ para todo } x \in L\}$.

A seguir apresentamos o Teorema Fundamental da teoria de Galois. Nele é estabelecido uma correspondência bijetora entre subcorpos de raízes de $f(x)$ e os subgrupos de seu Grupo de Galois. Ele nos fornece um critério para analisar se um subcorpo de uma extensão é também uma extensão normal de F e é uma ferramenta essencial para obtermos condições na resolução por radicais das raízes de um polinômio.

Teorema 3.2.16. Teorema Fundamental de Galois - Sejam $f(x)$ um polinômio em $F[x]$, K o corpo de raízes sobre F e $G(K, F)$ o Grupo de Galois. Para todo subcorpo L de K , com $F \subseteq L$, seja $G(K, L) = \{\sigma \in G(K, F) \mid \sigma(t) = t, \forall t \in L\}$ e para todo subgrupo H de $G(K, F)$ seja $K_H = \{x \in K \mid \sigma(x) = x, \forall \sigma \in H\}$. Assim, a associação de L com $G(K, L)$ estabelece uma correspondência bijetora do conjunto dos subcorpos de K que contêm F com o conjunto dos subgrupos de $G(K, F)$ de tal forma que:

- (1) $L = K_{G(K,L)}$;
- (2) $H = G(K, K_H)$;
- (3) $[K : L] = |G(K, L)|$, onde $[L : F]$ é o índice de $G(K, L)$ em $G(K, F)$;
- (4) L é uma extensão normal de F se, e somente se, $G(K, L)$ é um subgrupo normal de $G(K, F)$;
- (5) Quando L é uma extensão normal de F , $G(L, F)$ é isomorfo a $G(K, F)/G(K, L)$.

Demonstração. (1) Como K é o corpo de raízes de $f(x)$ sobre F , então ele também é o corpo de raízes de $f(x)$ sobre qualquer subcorpo de L que contém F , assim, pelo Teorema 3.2.13, K é uma extensão normal de L . Logo, pela definição de normalidade L é o corpo fixo de $G(K, L)$, ou seja, $L = K_{G(K,L)}$.

- (2) Pelo Teorema 3.2.11, como K é uma extensão normal de F , dado um subgrupo H de $G(K, F)$, temos $H = G(K, K_H)$.
- (3) A asserção (1) mostra que todo subgrupo de $G(K, F)$ aparece na forma $G(K, L)$, assim a associação de L com $G(K, L)$ leva o conjunto de todos os subcorpos K que contém F no conjunto de todos subgrupos de $G(K, F)$. Essa aplicação é injetora, pois, se $G(K, L_1) = G(K, L_2)$ então, por (1), $L_1 = K_{G(K,L_1)} = K_{G(K,L_2)} = L_2$. Portanto, pelo Teorema 3.2.11, temos que $[K : L] = |G(K, L)|$. Logo, $|G(K, F)| = [K : F] = [K : L][L : F] = |G(K, L)||L : F|$ e

$$[L : F] = \frac{|G(K, F)|}{|G(K, L)|}.$$

- (4) Observe que L é uma extensão normal de F se, e somente se, para todo $\sigma \in G(K, L)$ tivermos $\sigma(L) \subset L$. De fato, pelo Teorema 3.1.16, sabemos que $L = F(a)$, logo se $\sigma(L) \subset L$, então $\sigma(a) \in L$ para todo $\sigma \in G(K, F)$, o que implica, pelo Teorema 3.2.13, que L é o corpo de raízes de $p(x) = \prod_{\sigma \in G(K,F)} (x - \sigma(a))$, que tem coeficientes em F .

Ainda pelo Teorema 3.2.13, como L é o corpo de raízes de $p(x)$, então L é uma extensão normal de F . Reciprocamente, se L é uma extensão normal de F , então $L = F(a)$, onde o polinômio minimal $p(x)$ de a sobre F possui todas suas raízes em L . Mas, para todo $\sigma \in G(K, F)$ temos que $\sigma(a)$ também é uma raiz de $p(x)$,

o que implica que $\sigma(a)$ também está em L . Como L é gerado por a sobre F , temos que $\sigma(L) \subset L$ para todo $\sigma \in G(K, F)$.

Portanto, L é uma extensão normal de F se, e somente se, para todo $\sigma \in G(K, F)$, $\tau \in G(K, L)$ e $l \in L$, tivermos $\sigma(l) \in L$ e então $\tau(\sigma(l)) = \sigma(l)$, ou seja, se, e somente se, $\sigma^{-1}\tau\sigma(l) = l$. Logo L é normal sobre F se, e somente se, $\sigma^{-1}G(K, L)\sigma \subset G(K, L)$ para todo $\sigma \in G(K, F)$, sendo esta última condição que define $G(K, L)$ como um subgrupo normal de $G(K, F)$.

- (5) Se L é normal sobre F , dado $\sigma \in G(K, F)$, como $\sigma(L) \subset L$, então σ leva a um automorfismo σ_* de L , definido por $\sigma_*(l) = \sigma(l)$ para todo $l \in L$. E ainda, para todo $\sigma, \psi \in G(K, F)$, temos $(\sigma\psi)_* = \sigma_*\psi_*$, portanto a aplicação de $G(K, F)$ em $G(L, F)$ definida por $\sigma \rightarrow \sigma_*$ é um homomorfismo de $G(K, F)$ em $G(L, F)$. O núcleo desse homomorfismo constitui-se de todos os elementos σ em $G(K, F)$ tais que σ_* seja uma aplicação idêntica sobre L , ou seja, o núcleo é dado pelo conjunto de todos $\sigma \in G(K, F)$ tais que $l = \sigma_*(l) = \sigma(l)$, que por definição é o próprio $G(K, L)$. Pelo Teorema 2.1.28, a imagem de $G(K, F)$ em $G(L, F)$ é isomorfa a $G(K, F)/G(K, L)$, que possui ordem $|G(K, F)|/|G(K, L)| = [L : F]$, onde pela parte (3) corresponde a $|G(L, F)|$. Portanto, a imagem de $G(K, F)$ em $G(L, F)$ coincide com $G(L, F)$, logo $G(L, F)$ é isomorfo a $G(K, F)/G(K, L)$.

□

3.3 Exemplos Utilizando a Teoria de Galois

O Teorema Fundamental da Teoria de Galois é utilizado nos dois exemplos que seguem. Em cada caso, estamos interessados em obter o corpo de raízes sobre \mathbb{Q} , o grupo de Galois G , bem como o corpo fixo por H , para todo subgrupo de G .

Exemplo 3.3.1. *Façamos o estudo da função $p(x) = x^3 - 2$, sobre \mathbb{Q} .*

Solução. *Seja \mathbb{Q} o corpo dos números racionais e seja $p(x) = x^3 - 2$. Temos que $a = \sqrt[3]{2}$ é uma raiz de $p(x)$, no entanto $a \notin \mathbb{Q}$. Assim, tome $L = \mathbb{Q}(a)$ como a extensão de \mathbb{Q} que contém a raiz a . Logo, $[L : \mathbb{Q}] = 3$ e também $\mathbb{Q}(a) = \{\alpha_0 + \alpha_1 a + \alpha_2 a^2 : \alpha_i \in \mathbb{Q}\}$. Portanto, $p(x)$ pode ser fatorado em $\mathbb{Q}(a)$ como $p(x) = (x - a)q(x)$, onde $q(x)$ é um polinômio de raízes complexas.*

Afim de determinarmos tais raízes, recordamos que a raiz n -ésima da unidade é obtida através da fórmula,

$$\omega = \cos \frac{2\pi}{n} + i \operatorname{sen} \frac{2\pi}{n}$$

Em nosso caso, $n = 3$. Portanto, temos que

$$\omega = \cos \frac{2\pi}{3} + i \operatorname{sen} \frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i.$$

Como $\omega \notin \mathbb{Q}(a) = L$, temos uma nova extensão $K = L(i\sqrt{3})$, uma vez que em $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, temos que $-\frac{1}{2}$ e $\frac{1}{2} \in \mathbb{Q}$ e apenas $\sqrt{3}i \notin \mathbb{Q}$. Mas, o polinômio de menor grau para essa nova extensão é dado por $x^2 + 3$, assim $[K : \mathbb{Q}] = 2$. Portanto, pelo Teorema 2.6.3 temos que $[K : \mathbb{Q}] = [K : L][L : \mathbb{Q}] = 2 \cdot 3 = 6$.

As raízes de $p(x)$ são da forma $a, a\omega$ e $a\omega^2$. Agora, todas estão em K . O corpo de raízes de $p(x)$ tem a forma $\{\alpha + \beta i\sqrt{3} : \alpha, \beta \in L\}$. Tome,

$$\alpha = \alpha_0 + \alpha_1 a + \alpha_2 a^2 \text{ e } \beta = \beta_0 + \beta_1 a + \beta_2 a^2, \text{ onde } \alpha_i, \beta_i \in \mathbb{Q}.$$

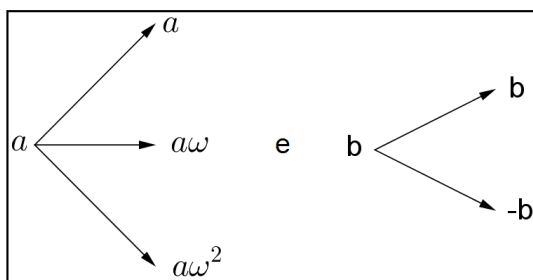
Logo, os elementos do corpo de raízes de $p(x)$ são representados por $x = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + (\beta_0 + \beta_1 a + \beta_2 a^2)i\sqrt{3}$, ou seja,

$$x = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \beta_0 \sqrt{3}i + \beta_1 a \sqrt{3}i + \beta_2 a^2 \sqrt{3}i.$$

Portanto, temos que $\{1, a, a^2, \sqrt{3}i, a\sqrt{3}i, a^2\sqrt{3}i\}$ é a base de K sobre \mathbb{Q} , onde $a = \sqrt[3]{2}$.

Vamos agora determinar o Grupo de Galois G de $p(x)$. Para isso, temos que $G(K, \mathbb{Q}) = \{\sigma \in \operatorname{Aut}(K) / \sigma(\alpha) = \alpha \text{ para todo } \alpha \in \mathbb{Q}\}$.

Observe o diagrama a seguir que representa os automorfismos de $G(K, \mathbb{Q})$,



Segundo o Teorema 3.2.11, temos $|G(K, \mathbb{Q})| = [K : \mathbb{Q}] = 6$. Portanto, vamos estudar os 6 automorfismos em G .

σ_1 :

$$a \longrightarrow a$$

$$b \longrightarrow b$$

Temos que para todo $\alpha \in \mathbb{Q}$, $\alpha \longrightarrow \alpha$. Logo, $\sigma_1 = id$.

σ_2 :

$$a \longrightarrow a\omega$$

$$b \longrightarrow b$$

Logo,

$$a \longrightarrow a\omega \longrightarrow a\omega^2 \longrightarrow a$$

$$b \longrightarrow b \longrightarrow b \longrightarrow b$$

Portanto, fazendo $\sigma_2 = \sigma$, temos que $\sigma^3 = id$.

σ_3 :

$$a \longrightarrow a$$

$$b \longrightarrow -b$$

Logo,

$$a \longrightarrow a \longrightarrow a$$

$$b \longrightarrow -b \longrightarrow b$$

Portanto, fazendo $\sigma_3 = \tau$, temos que $\tau^2 = id$.

σ_4 :

$$a \longrightarrow a\omega^2$$

$$b \longrightarrow b$$

Logo,

$$a \longrightarrow a\omega^2 \longrightarrow a\omega \longrightarrow a$$

$$b \longrightarrow b \longrightarrow b \longrightarrow b$$

Portanto, observe que $\sigma_4 = \sigma^2$, assim $(\sigma^2)^3 = id$.

σ_5 :

$$a \longrightarrow a\omega$$

$$b \longrightarrow -b$$

Inicialmente observe que,

$$a \xrightarrow{\tau} a \xrightarrow{\sigma} a\omega$$

$$b \xrightarrow{\tau} -b \xrightarrow{\sigma} -b$$

logo, $\sigma_5 = \sigma\tau$, assim

$$a \longrightarrow a\omega \longrightarrow a$$

$$b \longrightarrow b \longrightarrow b$$

Portanto, temos que $(\sigma\tau)^2 = id$.

σ_6 :

$$a \longrightarrow a\omega^2$$

$$b \longrightarrow -b$$

Inicialmente observe que,

$$a \xrightarrow{\tau} a \xrightarrow{\sigma^2} a\omega^2$$

$$b \xrightarrow{\tau} -b \xrightarrow{\sigma^2} -b$$

logo, $\sigma_6 = \sigma^2\tau$, assim

$$a \longrightarrow a\omega^2 \longrightarrow a$$

$$b \longrightarrow -b \longrightarrow b$$

Portanto, temos que $(\sigma^2\tau)^2 = id$.

Observe ainda que $\sigma\tau \neq \tau\sigma$, pois

$\tau\sigma$:

$$a \longrightarrow a\omega \longrightarrow a\omega^2$$

$$b \longrightarrow b \longrightarrow -b$$

Uma vez que $\sigma\tau \neq \tau\sigma$, concluímos que G não é abeliano.

Observando os automorfismos obtidos, verificamos que G é isomorfo ao grupo simétrico S_3 , pois $G = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1, \tau\sigma = \sigma^2\tau \rangle$, estrutura análoga a do grupo S_3 dada na seção 2.1.9.

Vamos descrever os subgrupos de G e depois determinar os corpos fixos para cada subgrupo H de G . Portanto, os subgrupos de G são:

Ordem 6: $G \cong S_3$

Ordem 3: $A = \{1, \sigma, \sigma^2\} = \langle \sigma \rangle$

$$B = \{1, \tau\} = \langle \tau \rangle$$

Ordem 2: $C = \{1, \sigma\tau\} = \langle \sigma\tau \rangle$

$$D = \{1, \sigma^2\tau\} = \langle \sigma^2\tau \rangle$$

Ordem 1: $I = \{1\} = \langle Id \rangle$ ou $\langle 1 \rangle$

Observe o diagrama a seguir, ele no fornece o reticulado¹ de subgrupos

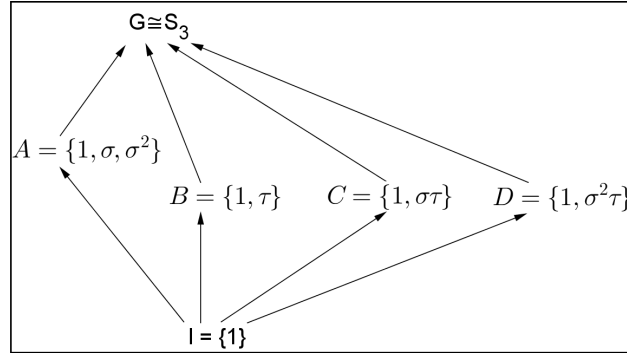


Figura 3.1: Reticulado de Subgrupos

A seguir, iremos determinar o corpo fixo para todo subgrupo de G . Lembre que, qualquer elemento de K pode ser expresso por $x = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \beta_0 b + \beta_1 ab + \beta_2 a^2 b$, onde $a = \sqrt[3]{2}$, $b = \sqrt{3}i$ e $\alpha_i, \beta_i \in \mathbb{Q}$. Assim, temos

$$1^\circ) H_1 = \langle 1 \rangle = \{1\}$$

$$K_{H_1} = K = \mathbb{Q}(a, \omega)$$

$$2^\circ) H_2 = \langle \sigma^2 \tau \rangle = \{1, \sigma^2 \tau\}$$

Dado $x \in K$, temos

$$\sigma^2 \tau(x) = \sigma^2 \tau(\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \beta_0 b + \beta_1 ab + \beta_2 a^2 b)$$

$$\sigma^2 \tau(x) = \sigma^2 \tau(\alpha_0) + \sigma^2 \tau(\alpha_1 a) + \sigma^2 \tau(\alpha_2 a^2) + \sigma^2 \tau(\beta_0 b) + \sigma^2 \tau(\beta_1 ab) + \sigma^2 \tau(\beta_2 a^2 b)$$

$$\sigma^2 \tau(x) = \alpha_0 + \alpha_1 a \omega^2 + \alpha_2 a^2 \omega - \beta_0 b - \beta_1 a \omega^2 b - \beta_2 a^2 \omega b$$

$$\sigma^2 \tau(x) = \alpha_0 + \alpha_1 a \left(-\frac{1}{2} - \frac{b}{2}\right) + \alpha_2 a^2 \left(-\frac{1}{2} + \frac{b}{2}\right) - \beta_0 b - \beta_1 ab \left(-\frac{1}{2} - \frac{b}{2}\right) - \beta_2 a^2 b \left(-\frac{1}{2} + \frac{b}{2}\right)$$

$$\sigma^2 \tau(x) = \alpha_0 - \frac{\alpha_1 a}{2} - \frac{\alpha_1 ab}{2} - \frac{\alpha_2 a^2}{2} + \frac{\alpha_2 a^2 b}{2} - \beta_0 b + \frac{\beta_1 ab}{2} - \frac{3\beta_1 a}{2} + \frac{\beta_2 a^2 b}{2} + \frac{3\beta_2 a^2}{2}$$

$$\sigma^2 \tau(x) = \alpha_0 + \left(-\frac{\alpha_1}{2} - \frac{3\beta_1}{2}\right)a + \left(-\frac{\alpha_2}{2} + \frac{3\beta_2}{2}\right)a^2 - \beta_0 b + \left(-\frac{\alpha_1}{2} + \frac{\beta_1}{2}\right)ab + \left(\frac{\alpha_2}{2} + \frac{\beta_2}{2}\right)a^2 b$$

Logo,

$$i) \alpha_0 \in \mathbb{Q} \text{ e } \beta_0 = 0$$

¹Um sistema parcialmente ordenado será dito um reticulado se nele existirem o supremo e o ínfimo de qualquer par de seus elementos

$$ii) -\frac{\alpha_1}{2} - \frac{3\beta_1}{2} = \alpha_1 \Rightarrow \alpha_1 = -\beta_1$$

$$-\frac{\alpha_1}{2} + \frac{\beta_1}{2} = \beta_1 \Rightarrow \alpha_1 = -\beta_1$$

$$iii) -\frac{\alpha_2}{2} + \frac{3\beta_2}{2} = \alpha_2 \Rightarrow \alpha_2 = \beta_2$$

$$\frac{\alpha_2}{2} + \frac{\beta_2}{2} = \beta_2 \Rightarrow \alpha_2 = \beta_2$$

Portanto, $x = \alpha_0 + \alpha_1 a + \alpha_2 a^2 - \alpha_1 ab + \alpha_2 a^2 b$

$$x = \alpha_0 + \alpha_1 a(1 - b) + \alpha_2 a^2(1 + b)$$

$$x = \alpha_0 + \alpha_1 a(-2)\left(-\frac{1}{2} + \frac{b}{2}\right) + \alpha_2 a^2(-2)\left(-\frac{1}{2} - \frac{b}{2}\right)$$

$$x = \alpha_0 + \alpha'_1 a\omega + \alpha'_2 (a\omega)^2, \text{ onde } \alpha'_1 = (-2)\alpha_1 \text{ e } \alpha'_2 = (-2)\alpha_2.$$

$$K_{H_2} = \mathbb{Q}(a\omega)$$

$$3^\circ) H_3 = \langle \sigma\tau \rangle = \{1, \sigma\tau\}$$

Dado $x \in K$, temos

$$\sigma\tau(x) = \sigma\tau(\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \beta_0 b + \beta_1 ab + \beta_2 a^2 b)$$

$$\sigma\tau(x) = \sigma\tau(\alpha_0) + \sigma\tau(\alpha_1 a) + \sigma\tau(\alpha_2 a^2) + \sigma\tau(\beta_0 b) + \sigma\tau(\beta_1 ab) + \sigma\tau(\beta_2 a^2 b)$$

$$\sigma\tau(x) = \alpha_0 + \alpha_1 a\omega + \alpha_2 a^2 \omega^2 - \beta_0 b - \beta_1 a\omega b - \beta_2 \omega^2 a^2 b$$

$$\sigma\tau(x) = \alpha_0 + \alpha_1 a\left(-\frac{1}{2} + \frac{b}{2}\right) + \alpha_2 a^2\left(-\frac{1}{2} - \frac{b}{2}\right) - \beta_0 b - \beta_1 ab\left(-\frac{1}{2} + \frac{b}{2}\right) - \beta_2 a^2 b\left(-\frac{1}{2} - \frac{b}{2}\right)$$

$$\sigma\tau(x) = \alpha_0 - \frac{\alpha_1 a}{2} + \frac{\alpha_1 ab}{2} - \frac{\alpha_2 a^2}{2} - \frac{\alpha_2 a^2 b}{2} - \beta_0 b + \frac{\beta_1 ab}{2} + \frac{3\beta_1 a}{2} + \frac{\beta_2 a^2 b}{2} - \frac{3\beta_2 a^2}{2}$$

$$\sigma\tau(x) = \alpha_0 + \left(-\frac{\alpha_1}{2} + \frac{3\beta_1}{2}\right)a + \left(-\frac{\alpha_2}{2} - \frac{3\beta_2}{2}\right)a^2 - \beta_0 b + \left(\frac{\alpha_1}{2} + \frac{\beta_1}{2}\right)ab + \left(-\frac{\alpha_2}{2} + \frac{\beta_2}{2}\right)$$

Logo,

$$i) \alpha_0 \in \mathbb{Q} \text{ e } \beta_0 = 0$$

$$ii) -\frac{\alpha_1}{2} + \frac{3\beta_1}{2} = \alpha_1 \Rightarrow \alpha_1 = \beta_1$$

$$\frac{\alpha_1}{2} + \frac{\beta_1}{2} = \beta_1 \Rightarrow \alpha_1 = \beta_1$$

$$iii) -\frac{\alpha_2}{2} - \frac{3\beta_2}{2} = \alpha_2 \Rightarrow \alpha_2 = -\beta_2$$

$$-\frac{\alpha_2}{2} + \frac{\beta_2}{2} = \beta_2 \Rightarrow \alpha_2 = -\beta_2$$

Portanto, $x = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \alpha_1 ab - \alpha_2 a^2 b$

$$x = \alpha_0 + \alpha_1 a(1 + b) + \alpha_2 a^2(1 - b)$$

$$x = \alpha_0 + \alpha_1 a(-2)\left(-\frac{1}{2} - \frac{b}{2}\right) + \alpha_2 a^2(-2)\left(-\frac{1}{2} + \frac{b}{2}\right)$$

$$x = \alpha_0 + \alpha'_1 a\omega^2 + \alpha'_2 (a\omega^2)^2, \text{ onde } \alpha'_1 = (-2)\alpha_1 \text{ e } \alpha'_2 = (-2)\alpha_2.$$

$$K_{H_3} = \mathbb{Q}(a\omega^2)$$

4°) $H_4 = \langle \tau \rangle = \{1, \tau\}$

Dado $x \in K$, temos

$$\tau(x) = \tau(\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \beta_0 b + \beta_1 ab + \beta_2 a^2 b)$$

$$\tau(x) = \tau(\alpha_0) + \tau(\alpha_1 a) + \tau(\alpha_2 a^2) + \tau(\beta_0 b) + \tau(\beta_1 ab) + \tau(\beta_2 a^2 b)$$

$$\tau(x) = \alpha_0 + \alpha_1 a + \alpha_2 a^2 - \beta_0 b - \beta_1 ab - \beta_2 a^2 b$$

Logo, $\alpha_0, \alpha_1, \alpha_2 \in \mathbb{Q}$, $\beta_0 = \beta_1 = \beta_2 = 0$.

Portanto, $x = \alpha_0 + \alpha_1 a + \alpha_2 a^2 \in \mathbb{Q}(a)$

$$K_{H_4} = \mathbb{Q}(a)$$

5°) $H_5 = \langle \sigma \rangle = \{1, \sigma, \sigma^2\}$

Dado $x \in K$, temos

$$\sigma(x) = \sigma(\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \beta_0 b + \beta_1 ab + \beta_2 a^2 b)$$

$$\sigma(x) = \sigma(\alpha_0) + \sigma(\alpha_1 a) + \sigma(\alpha_2 a^2) + \sigma(\beta_0 b) + \sigma(\beta_1 ab) + \sigma(\beta_2 a^2 b)$$

$$\sigma(x) = \alpha_0 + \alpha_1 a\omega + \alpha_2 a^2 \omega^2 + \beta_0 b + \beta_1 a\omega b - \beta_2 a^2 \omega^2 b$$

Logo, $\alpha_0, \beta_0 \in \mathbb{Q}$, $\alpha_1 = \alpha_2 = \beta_1 = \beta_2 = 0$.

Portanto, $x = \alpha_0 + \beta_0 b \in \mathbb{Q}(\omega)$

6°) $H_6 = G$

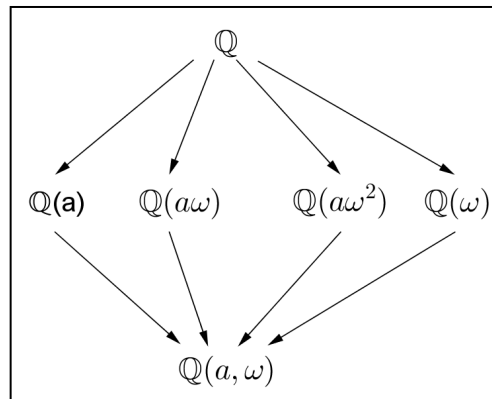


Figura 3.2: Reticulado de Corpos Intermediários

Exemplo 3.3.2. *Façamos um estudo, análogo ao exemplo anterior, agora da função $p(x) = x^4 - 2$, identificando o corpo de raízes de p sobre \mathbb{Q} , o Grupo de Galois G e para todo subgrupo de G determinar o corpo fixo.*

Solução. Seja $p(x) = x^4 - 2 = (x^2 + \sqrt{2})(x^2 - \sqrt{2}) = (x^2 + \sqrt{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2}) = (x + \sqrt[4]{2}i)(x - \sqrt[4]{2}i)(x + \sqrt[4]{2})(x - \sqrt[4]{2})$ sobre \mathbb{Q} .

Tomando $a = \sqrt[4]{2}$, temos que a é uma raiz positiva de $p(x)$. Como $a \notin \mathbb{Q}$, tome $L = \mathbb{Q}(a)$ como a extensão de \mathbb{Q} que contém a raiz a . Observe que, $[\mathbb{Q}(a) : \mathbb{Q}] = [L : \mathbb{Q}] = 4$ e ainda

$$\mathbb{Q}(a) = \{\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \alpha_3 a^3 / \alpha_i \in \mathbb{Q}\}.$$

Na expressão fatorada de $p(x)$ observamos que a função também possui raízes complexas. Nesse caso, vamos utilizar a fórmula $\omega = \cos \frac{2\pi}{n} + \text{sen} \frac{2\pi}{n} i$, onde $n = 4$ e obtemos

$$\omega = \cos \frac{\pi}{2} + \text{sen} \frac{\pi}{2} i = i$$

O polinômio minimal de i sobre $\mathbb{Q}(a)$ é $x^2 + 1$, cujas raízes são $\pm i$. Como $i \notin \mathbb{Q}(a) \subseteq \mathbb{R}$, temos uma nova extensão $K = L(i) = \mathbb{Q}(a, i)$, onde $[K : L] = 2$. Assim, pelo Teorema 2.6.3,

$$[K : \mathbb{Q}] = [K : L][L : \mathbb{Q}] = 2 \cdot 4 = 8.$$

As raízes de $p(x)$ são da forma $a, a\omega, a\omega^2$ e $a\omega^3$, com todas contidas em K .

O corpo de raízes de $p(x)$ é da forma $\{\alpha + \beta i : \alpha, \beta \in L\}$.

$$\text{Tomando } \begin{cases} \alpha = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \alpha_3 a^3 \\ \beta = \beta_0 + \beta_1 a + \beta_2 a^2 + \beta_3 a^3 \end{cases}, \text{ com } \alpha_i, \beta_i \in \mathbb{Q},$$

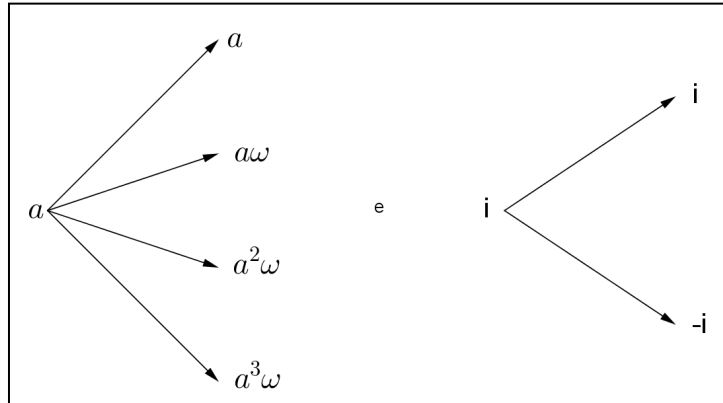
o corpo de raízes de $p(x) = x^4 - 2$, é representado pela expressão $(\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \alpha_3 a^3) + (\beta_0 + \beta_1 a + \beta_2 a^2 + \beta_3 a^3)i = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \alpha_3 a^3 + \beta_0 i + \beta_1 a i + \beta_2 a^2 i + \beta_3 a^3 i$.

Portanto, temos $\{1, a, a^2, a^3, i, ai, a^2 i, a^3 i\}$ como a base de K sobre \mathbb{Q} , onde $a = \sqrt[4]{2}$.

Temos que $G(K, \mathbb{Q}) = \{\sigma \in \text{Aut}(K) / \sigma(\alpha) = \alpha, \text{ para todo } \alpha \in \mathbb{Q}\}$. Como $a^4 = 2$, observe que $\sigma(a^4) = \sigma(2) = 2$, ao mesmo tempo que, $\sigma(a^4) = \sigma(a)\sigma(a)\sigma(a)\sigma(a) = \sigma(a)^4 = 2$, o que implica que $\sigma(a)$ também é uma raiz de $p(x) = x^4 - 2$.

Na extensão $K = L(i) = \mathbb{Q}(a, i)$, se $b = i$ então $b^2 = -1$, assim $\sigma(b^2) = \sigma(-1) = -1$, mas, $\sigma(b^2) = \sigma(b)\sigma(b) = \sigma(b)^2 = -1$. Logo, $\sigma(b) = \sigma(i)$ é uma raiz de $x^2 + 1$ e as raízes de $x^2 + 1$ são i e $-i$.

Assim temos,



Temos, pelo Teorema 3.2.11, que $|G(E, \mathbb{Q})| = [E : \mathbb{Q}] = 8$, assim vamos determinar os 8 automorfismos existentes, que denominamos de $\sigma_1, \sigma_2, \dots, \sigma_8$.

σ_1 :

$$a \longrightarrow a$$

$$i \longrightarrow i$$

Logo, $\sigma_1 = 1$.

σ_2 :

$$a \longrightarrow ai$$

$$i \longrightarrow i$$

Logo,

$$a \longrightarrow ai \longrightarrow -a \longrightarrow -ai \longrightarrow a$$

$$i \longrightarrow i \longrightarrow i \longrightarrow i \longrightarrow i$$

Assim, fazendo $\sigma_2 = \tau$, temos que $(\tau)^4 = 1$

σ_3 :

$$a \longrightarrow -a$$

$$i \longrightarrow i$$

Logo,

$$a \longrightarrow -a \longrightarrow a$$

$$i \longrightarrow i \longrightarrow i$$

Assim, temos que $\sigma_3 = \tau^2$ e $(\tau^2)^2 = 1$

σ_4 :

$$a \longrightarrow a$$

$$i \longrightarrow -i$$

Logo,

$$a \longrightarrow a \longrightarrow a$$

$$i \longrightarrow -i \longrightarrow i$$

Assim, fazendo $\sigma_4 = \sigma$, temos que $(\sigma)^2 = 1$

σ_5 :

$$a \longrightarrow -a$$

$$i \longrightarrow -i$$

Logo, $\sigma_5 = \tau^2\sigma$ e

$$a \longrightarrow -a \longrightarrow a$$

$$i \longrightarrow -i \longrightarrow i$$

Assim, temos que $(\tau^2\sigma)^2 = 1$

σ_6 :

$$a \longrightarrow ai$$

$$i \longrightarrow -i$$

Logo, $\sigma_6 = \tau\sigma$ e

$$a \longrightarrow ai \longrightarrow a$$

$$i \longrightarrow -i \longrightarrow i$$

Assim, temos que $(\tau\sigma)^2 = 1$

σ_7 :

$$a \longrightarrow -ai$$

$$i \longrightarrow i$$

Logo, $\sigma_7 = \tau^3$ e

$$a \longrightarrow -ai \longrightarrow -a \longrightarrow ai \longrightarrow a$$

$$i \longrightarrow i \longrightarrow i \longrightarrow i \longrightarrow i$$

Assim, temos que $(\tau^3)^4 = 1$

σ_8 :

$$a \longrightarrow -ai$$

$$i \longrightarrow -i$$

Logo, $\sigma_8 = \tau^3\sigma$ e

$$a \longrightarrow -ai \longrightarrow a$$

$$i \longrightarrow -i \longrightarrow i$$

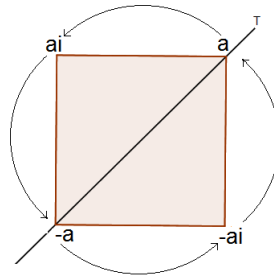
Assim, temos que $(\tau^3\sigma)^2 = 1$

Logo, $\sigma_1, \sigma_2, \dots, \sigma_8$ são os \mathbb{Q} automorfismos de K .

A estrutura abstrata do Grupo de Galois pode ser encontrada. Para isso, observe que

$$G = \langle \sigma, \tau : \sigma^2 = \tau^4 = 1, \tau\sigma = \sigma\tau^3 \rangle.$$

Conforme vimos na Seção 2.1.10, G é o grupo diedral de ordem 4, que escrevemos como D_4 , ou seja, $G = D_4$. Lembre-se que D_4 é definido como o grupo de todas as simetrias do quadrado. Assim, podemos classificar os quatro vértices do quadrado como zeros de $x^4 - 2$ de forma que as simetrias geométricas sejam as permutações que ocorrem no Grupo de Galois.



Temos os seguintes subgrupos de G :

Ordem 8: G ;

$$\begin{array}{l} \text{Ordem 4:} \\ \text{Ordem 2:} \end{array} \left\{ \begin{array}{l} H_8 : \{1, \sigma, \tau^2, \tau^2\sigma\} \\ H_7 : \{1, \tau, \tau^2, \tau^3\} \\ H_6 : \{1, \tau^2, \tau\sigma, \tau^3\sigma\} \\ H_5 : \{1, \tau^2\sigma\} \\ H_4 : \{1, \sigma\} \\ H_3 : \{1, \tau^2\} \\ H_2 : \{1, \tau\sigma\} \\ H_1 : \{1, \tau^3\sigma\} \end{array} \right.$$

Ordem 1: $\{1\}$;

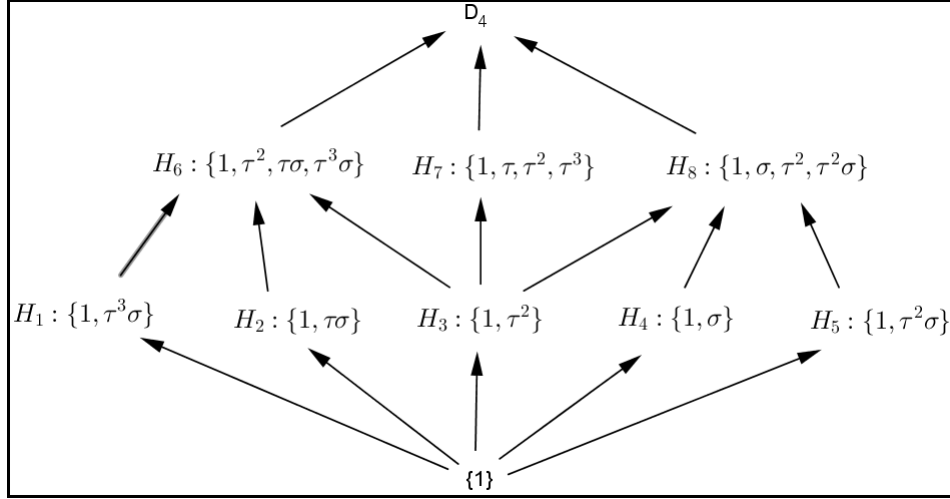


Figura 3.3: Reticulado de Subgrupos D_4

Existem três subcorpos triviais de K de grau 2 sobre $\mathbb{Q}(\sqrt{2}i)$, $\mathbb{Q}(i)$ e $\mathbb{Q}(\sqrt{2})$, que são corpos fixos por H_6 , H_7 e H_8 , respectivamente. Desejamos, para todo subgrupo de G , determinar o corpo fixo. Note que qualquer elemento $x \in K$ pode ser escrito da forma $x = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \alpha_3 a^3 + \beta_0 i + \beta_1 a i + \beta_2 a^2 i + \beta_3 a^3 i$.

Assim, temos

1. Temos que $\tau^2 : a \rightarrow -a$ e $i \rightarrow i$. Logo,

$$\tau^2(x) = \alpha_0 + \alpha_1(-a) + \alpha_2(-a)^2 + \alpha_3(-a)^3 + \beta_0 i + \beta_1(-a)i + \beta_2(-a)^2 i + \beta_3(-a)^3 i$$

$$\tau^2(x) = \alpha_0 - \alpha_1 a + \alpha_2 a^2 - \alpha_3 a^3 + \beta_0 i - \beta_1 a i + \beta_2 a^2 i - \beta_3 a^3 i$$

O elemento x é fixado por τ^2 se, e somente se, $\alpha_0 = \alpha_0$, $-\alpha_1 = \alpha_1$, $\alpha_2 = \alpha_2$, $-\alpha_3 = \alpha_3$, $\beta_0 = \beta_0$, $-\beta_1 = \beta_1$, $\beta_2 = \beta_2$ e $-\beta_3 = \beta_3$.

A partir das igualdades acima, temos α_0 , α_2 , β_0 e β_2 arbitrários, enquanto $\alpha_1 = \alpha_3 = \beta_1 = \beta_3 = 0$.

Nesse caso, $x = \alpha_0 + \alpha_2 a^2 + \beta_0 i + \beta_2 a^2 i$. Como $a = \sqrt[4]{2}$, temos $a^2 = \sqrt{2}$. Assim, $x = \alpha_0 + \alpha_2 \sqrt{2} + \beta_0 i + \beta_2 \sqrt{2} i \in \mathbb{Q}(\sqrt{2}, i)$. Portanto, o corpo fixo por τ^2 é $\mathbb{Q}(\sqrt{2}, i)$.

2. Temos que $\sigma : a \rightarrow a$ e $i \rightarrow -i$. Logo,

$$\sigma(x) = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \alpha_3 a^3 + \beta_0(-i) + \beta_1 a(-i) + \beta_2 a^2(-i) + \beta_3 a^3(-i)$$

$$\sigma(x) = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \alpha_3 a^3 - \beta_0 i - \beta_1 a i - \beta_2 a^2 i - \beta_3 a^3 i$$

O elemento x é fixado por σ se, e somente se, $\alpha_0 = \alpha_0$, $\alpha_1 = \alpha_1$, $\alpha_2 = \alpha_2$, $\alpha_3 = \alpha_3$, $-\beta_0 = \beta_0$, $-\beta_1 = \beta_1$, $-\beta_2 = \beta_2$ e $-\beta_3 = \beta_3$.

A partir das igualdades acima, temos α_0 , α_1 , α_2 e α_3 arbitrários, enquanto $\beta_0 = \beta_1 = \beta_2 = \beta_3 = 0$.

Nesse caso, $x = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \alpha_3 a^3 \in \mathbb{Q}(a) = \mathbb{Q}(\sqrt[4]{2})$. Portanto, o corpo fixo por σ é $\mathbb{Q}(\sqrt[4]{2})$.

3. $\tau\sigma : a \longrightarrow ai$ e $i \longrightarrow -i$. Logo,

$$\tau\sigma(x) = \alpha_0 + \alpha_1(ai) + \alpha_2(ai)^2 + \alpha_3(ai)^3 + \beta_0(-i) + \beta_1(ai)(-i) + \beta_2(ai)^2(-i) + \beta_3(ai)^3(-i)$$

$$\tau\sigma(x) = \alpha_0 + \alpha_1 ai - \alpha_2 a^2 - \alpha_3 a^3 i - \beta_0 i + \beta_1 a + \beta_2 a^2 i - \beta_3 a^3$$

O elemento x é fixado por $\tau\sigma$ se, e somente se, $\alpha_0 = \alpha_0$, $\alpha_1 = \beta_1$, $-\alpha_2 = \alpha_2$, $-\alpha_3 = \beta_3$, $-\beta_0 = \beta_0$, $\beta_1 = \alpha_1$, $\beta_2 = \beta_2$ e $-\beta_3 = \alpha_3$.

A partir das igualdades acima, temos α_0 e β_2 arbitrários, enquanto $\alpha_1 = \beta_1$, $\alpha_3 = -\beta_3$ e $\alpha_2 = \beta_0 = 0$.

Nesse caso,

$$x = \alpha_0 + \alpha_1 ai - \alpha_3 a^3 i + \beta_1 a + \beta_2 a^2 i - \beta_3 a^3$$

$$x = \alpha_0 + \alpha_1 ai - \alpha_3 a^3 i + \alpha_1 a + \beta_2 a^2 i + \alpha_3 a^3$$

$$x = \alpha_0 + \alpha_1 a(1+i) + \beta_2 a^2 i + \alpha_3 a^3(1-i)$$

$$x = \alpha_0 + \alpha_1 a(1+i) + \beta_2 \frac{[a(1+i)]^2}{2} - \alpha_3 \frac{[a(1+i)]^3}{2}$$

Portanto, o corpo fixo por $\tau\sigma$ é $\mathbb{Q}(\sqrt[4]{2}(1+i))$.

4. Temos que $\tau^2\sigma : a \longrightarrow -a$ e $i \longrightarrow -i$. Logo,

$$\tau^2\sigma(x) = \alpha_0 + \alpha_1(-a) + \alpha_2(-a)^2 + \alpha_3(-a)^3 + \beta_0(-i) + \beta_1(-a)(-i) + \beta_2(-a)^2(-i) + \beta_3(-a)^3(-i)$$

$$\tau^2\sigma(x) = \alpha_0 - \alpha_1 a + \alpha_2 a^2 - \alpha_3 a^3 - \beta_0 i + \beta_1 ai - \beta_2 a^2 i + \beta_3 a^3 i$$

O elemento x é fixado por $\tau^2\sigma$ se, e somente se, $\alpha_0 = \alpha_0$, $-\alpha_1 = \alpha_1$, $\alpha_2 = \alpha_2$, $-\alpha_3 = \alpha_3$, $-\beta_0 = \beta_0$, $\beta_1 = \beta_1$, $-\beta_2 = \beta_2$ e $\beta_3 = \beta_3$.

A partir das igualdades acima, temos α_0 , α_2 , β_1 e β_3 arbitrários, enquanto $\alpha_1 = \alpha_3 = \beta_0 = \beta_2 = 0$.

Nesse caso, $x = \alpha_0 + \alpha_2 a^2 + \beta_1 a i + \beta_3 a^2 i \in \mathbb{Q}(ai) = \mathbb{Q}(\sqrt[4]{2}i)$. Portanto, o corpo fixo por $\tau^2\sigma$ é $\mathbb{Q}(\sqrt[4]{2}i)$.

5. $\tau^3\sigma : a \rightarrow -ai$ e $i \rightarrow -i$. Logo,

$$\tau^3\sigma(x) = \alpha_0 + \alpha_1(-ai) + \alpha_2(-ai)^2 + \alpha_3(-ai)^3 + \beta_0(-i) + \beta_1(-ai)(-i) + \beta_2(-ai)^2(-i) + \beta_3(-ai)^3(-i)$$

$$\tau^3\sigma(x) = \alpha_0 - \alpha_1 ai - \alpha_2 a^2 + \alpha_3 a^3 i - \beta_0 i - \beta_1 a + \beta_2 a^2 i + \beta_3 a^3$$

O elemento x é fixado por $\tau^3\sigma$ se, e somente se, $\alpha_0 = \alpha_0$, $-\alpha_1 = \beta_1$, $-\alpha_2 = \alpha_2$, $\alpha_3 = \beta_3$, $-\beta_0 = \beta_0$, $-\beta_1 = \alpha_1$, $\beta_2 = \beta_2$ e $\beta_3 = \alpha_3$.

A partir das igualdades acima, temos α_0 e β_2 arbitrários, enquanto $-\alpha_1 = \beta_1$, $\alpha_3 = \beta_3$ e $\alpha_2 = \beta_0 = 0$.

Nesse caso,

$$x = \alpha_0 - \alpha_1 ai + \alpha_3 a^3 i - \beta_1 a + \beta_2 a^2 i + \beta_3 a^3$$

$$x = \alpha_0 - \alpha_1 ai + \alpha_3 a^3 i + \alpha_1 a + \beta_2 a^2 i + \alpha_3 a^3$$

$$x = \alpha_0 + \alpha_1 a(1 - i) + \beta_2 a^2 i + \alpha_3 a^3(1 + i)$$

$$x = \alpha_0 + \alpha_1 a(1 - i) - \beta_2 \frac{[a(1 - i)]^2}{2} - \alpha_3 \frac{[a(1 - i)]^3}{2}$$

Portanto, o corpo fixo por $\tau^3\sigma$ é $\mathbb{Q}(\sqrt[4]{2}(1 - i))$.

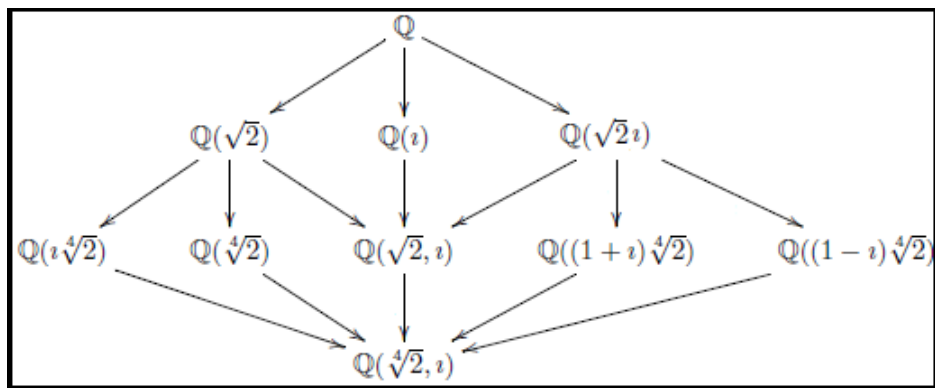


Figura 3.4: Reticulado de Corpos Intermediários D_4

3.4 Resolução por Radicais

Dado um corpo F e um polinômio $f(x) \in F[x]$, dizemos que $f(x)$ é solúvel por radicais sobre F , se for possível encontrar uma sequência finita de corpos $F_1 = F(\omega_1)$, $F_2 = F_1(\omega_2)$, ..., $F_k = F_{k-1}(\omega_k)$, onde $\omega_1^{r_1} \in F$, $\omega_2^{r_2} \in F_1$, ..., $\omega_k^{r_k} \in F_{k-1}$ e todas as raízes de $f(x)$ estejam em F_k .

Definição 3.4.1. Dizemos que um grupo G é solúvel se for possível determinar uma cadeia finita de subgrupos $G = N_0 \supset N_1 \supset N_2 \supset \dots \supset N_k = (e)$, onde N_i é um subgrupo normal de N_{i-1} e todo subgrupo quociente N_i/N_{i-1} seja abeliano.

Segue outra forma de descrever a solubilidade. Para isso, utilizamos a ideia de comutadores.

Dado G e os elementos $a, b \in G$, então o comutador de a e b é o elemento $aba^{-1}b^{-1}$. O subgrupo comutador G' de G é o subgrupo de G gerado por todos os comutadores em G . É possível mostrar que G' é um subgrupo normal de G e que G/G' é abeliano.

Definimos os subgrupos comutadores superiores $G^{(m)} = (G^{(m-1)})'$.

Lema 3.4.2. Um grupo G é solúvel se, e somente se, $G^{(K)} = (e)$, para algum inteiro K .

Demonstração. Se $G^{(K)} = (e)$, tome $N_0 = G$, $N_1 = G'$, $N_2 = G^{(2)}$, ..., $N_k = G^{(k)} = (e)$. Temos $N_0 \supset N_1 \supset N_2 \supset \dots \supset N_k = (e)$, e se cada N_i é normal em G , seguramente é normal em N_{i-1} . Enfim,

$$\frac{N_{i-1}}{N_i} = \frac{G^{(i-1)}}{G^{(i)}} = \frac{G^{(i-1)}}{(G^{(i-1)})'}$$

logo é abeliano. Assim, pela definição de solubilidade, G é um grupo solúvel.

Reciprocamente, se G é um grupo solúvel, segundo a Definição 3.4.1 existe $G = N_0 \supset N_1 \supset N_2 \supset \dots \supset N_k = (e)$, onde N_i é um subgrupo normal de N_{i-1} e todo N_i/N_{i-1} é abeliano. Logo, o subgrupo comutador $N'_{i-1} \subset N_i$. Portanto, $N_1 \supset N'_0 = G'$, $N_2 \supset N'_1 \supset (G')' = G^{(2)}$, $N_3 \supset N'_2 \supset (G^{(2)})' = G^{(3)}$, ..., $N_i \supset G^{(i)}$, $(e) = N_k \supset G^{(k)}$. Assim, chegamos que $G^{(k)} = (e)$. \square

Lema 3.4.3. Seja $G = S_n$, onde $n \geq 5$, então $G^{(k)}$, para $k = 1, 2, 3, \dots$ contém todo 3-ciclo de S_n .

Demonstração. Observe inicialmente que para um grupo qualquer G , se N é subgrupo normal em G , então N' também é um subgrupo normal de G .

Temos que se N é um subgrupo normal de $G = S_n$, com $n \geq 5$, que contém todo 3-ciclo em S_n , então S_n também contém todo 3-ciclo, pois supondo que $a = (1, 2, 3)$, $b = (1, 4, 5)$ estejam em N então $aba^{-1}b^{-1} = (1, 2, 3)(1, 4, 5)(3, 2, 1)(5, 4, 1) = (1, 4, 2)$ como um comutador de elementos de N está necessariamente em N' . Já que N' é um subgrupo normal de G , para todo $p \in S_n$ temos que $p(1, 4, 2)p^{-1}$ também está em N' . Tome um p em S_n tal que $p(1) = i_1$, $p(4) = i_2$ e $p(2) = i_3$, onde i_1, i_2 e i_3 são três inteiros distintos quaisquer variando de 1 até n . Portanto, $p(1, 4, 2)p^{-1} = (i_1, i_2, i_3)$ está em N' e N' contém todos os 3-ciclos. Fazendo $N = G$, que sem dúvida é normal em G e contém todos os 3-ciclos, obtemos que G' contém todos os 3-ciclos, continuando, como G' é normal em G , então $G^{(2)}$ contém todos os 3-ciclos, sucessivamente temos que $G^{(k)}$ contém todos os 3-ciclos para um k qualquer. \square

Lema 3.4.4. *Suponhamos que todas as raízes n -ésimas da unidade estejam em F e que $a \notin F$ também esteja em F . Seja $x^n - a \in F[x]$ e seja K seu corpo de raízes de F . Então:*

1. $K = F(t)$, onde t é qualquer raiz de $x^n - a$.
2. O Grupo de Galois de $x^n - a$ sobre F é abeliano.

Demonstração. Uma vez que F contém todas as n -ésimas raízes de unidade, contém $\omega = e^{\frac{2\pi i}{n}}$. Observe que $\omega^n = 1$, mas $\omega^m \neq 1$ para $0 < m < n$.

Se $u \in K$ é qualquer raiz de $x^n - a$, então $u, \omega u, \omega^2 u, \dots, \omega^{n-1} u$ são todas as raízes de $x^n - a$. É evidente que são raízes, vamos verificar agora se são distintas. Suponhamos que $\omega^i u = \omega^j u$, com $0 \leq i < j < n$. Então seja $u \neq 0$ e $(\omega^i - \omega^j)u = 0$, nesse caso teremos $\omega^i = \omega^j$, o que é impossível pois chegaremos que $\omega^{i-j} = 1$, com $0 < j - i < n$. Com $\omega \in F$, todos os $u, \omega u, \dots, \omega^{n-1} u$ estão em $F(u)$, assim $F(u)$ decompõe $x^n - a$, uma vez que nenhum subcorpo próprio de $F(u)$ que contém F também contém u , nenhum subcorpo apropriado de $F(u)$ pode decompor $x^n - a$. Assim, $F(u)$ é o corpo de raízes de $x^n - a$, e provamos que $K = F(u)$.

Se σ, τ são dois elementos quaisquer no grupo Galois de $x^n - a$, ou seja, se σ e τ são automorfismos de $K = F(u)$ deixando cada elemento de F fixo, então uma vez que $\sigma(u)$ e $\tau(u)$ são raízes de $x^n - a$, $\sigma(u) = \omega^i u$ e $\tau(u) = \omega^j u$, para alguns i e j . Assim, $\tau\sigma(u) = \sigma(\omega^j u) = \omega^j \sigma(u) = \omega^j \omega^i u = \omega^{i+j} u$; Similarmente, $\sigma\tau(u) = \omega^{i+j} u$. Portanto, $\sigma\tau$ e $\tau\sigma$ coincidem em u e em F . Logo, em todos os $K = F(u)$. Portanto, $\sigma\tau = \tau\sigma$ donde concluímos que o Grupo de Galois é abeliano. \square

Teorema 3.4.5. S_n não é solúvel para $n \geq 5$.

Demonstração. Se $G = S_n$, pelo Lema 3.4.3, $G^{(K)}$ inclui todos os 3-ciclos em S_n , para todo k , assim $G^{(k)} \neq (e)$ e pelo Lema 3.4.2, G não pode ser solúvel. \square

Teorema 3.4.6. Se $f(x) \in F[x]$ é solúvel por radicais sobre F , então o Grupo de Galois sobre F de $f(x)$ é um grupo solúvel.

Demonstração. Sejam K o corpo de raízes e $G(K, F)$ o Grupo de Galois de $f(x)$ sobre F . Como $f(x)$ é solúvel por radicais, existe uma sequência de corpos $F \subset F_1 = F(\omega_1)$, $F_2 = F_1(\omega_2)$, ..., $F_k = F_{k-1}(\omega_k)$, onde $\omega_1^{r_1} \in F$, $\omega_2^{r_2} \in F_1$, ..., $\omega_k^{r_k} \in F_{k-1}$ e onde $K \subset F_k$. Podemos admitir, sem perda de generalidade, que F_k é uma extensão normal de F e, assim sendo, F_k é uma extensão normal de qualquer corpo intermediário de F , ou seja, F_k é uma extensão normal de F_i .

Temos que F_i é uma extensão normal de F_{i-1} e como F_k é normal sobre F_{i-1} , pelo Teorema Fundamental de Galois (Teorema 3.2.16), $G(F_k, F_i)$ é um subgrupo normal em $G(F_k, F_{i-1})$. Observe a cadeia:

$$G(F_k, F) \supset G(F_k, F_1) \supset G(F_k, F_2) \supset \dots \supset G(F_k, F_{k-1}) \supset (e). \quad (3.6)$$

Temos que cada grupo nessa cadeia é um subgrupo normal no grupo anterior. Como F_i é uma extensão normal de F_{i-1} , pelo Teorema 3.2.16, o grupo F_i sobre F_{i-1} é isomorfo a $G(F_k, F_{i-1})/G(F_k, F_i)$. Mas, segundo o Lema 3.4.4, $G(F_i, F_{i-1})$ é abelino. Logo, todo grupo quociente $G(F_k, F_{i-1})/G(F_k, F_i)$ da cadeia (3.6) é abeliano.

Dado que $K \subset F_k$ é uma extensão normal de F , pelo Teorema 3.2.16, o grupo $G(F_k, K)$ é um subgrupo normal de $G(F_k, F)$ e $G(K, F)$ é isomorfo a $G(F_k, F)/G(F_k, K)$. Assim, $G(K, F)$ é uma imagem homomorfa de $G(F_k, F)$ que é solúvel. Portanto, o próprio $G(K, F)$ é um grupo solúvel. \square

3.4.1 A Insolubilidade do Polinômio Geral de Grau $n \geq 5$

Vimos pelo Teorema 3.2.9 que se $F(a_1, a_2, \dots, a_n)$ é o corpo das funções nas n variáveis a_1, a_2, \dots, a_n . Então o Grupo de Galois do polinômio $f(x) = x^n + a_1x^{n-1} + \dots + a_n$ sobre $F(a_1, a_2, \dots, a_n)$ é S_n , o grupo simétrico de grau n . Mas, pelo Teorema 3.4.5, temos que S_n não é um grupo solúvel para $n \geq 5$. Assim, pelo Teorema 3.4.6, $f(x)$ não é solúvel por radicais sobre $F(a_1, a_2, \dots, a_n)$ para $n \geq 5$.

Portanto, diferentemente dos casos dos polinômios de grau menor do que 5, não é possível determinar uma fórmula resolutive por meio de radicais para polinômios gerais de grau maior ou igual a 5.

Considerações Finais

Ao ler este trabalho é esperado que o leitor tenha ampliado seu conhecimento acerca de Equações Polinomiais, incluindo os aspectos históricos que as relacionam e compreendido as deduções das fórmulas resolutivas envolvendo equações de 3º e 4º grau que, diferentemente das de 1º e 2º grau, são pouco trabalhadas no Ensino Médio. É esperado também que entenda os assuntos envolvendo grupos, subgrupos, anéis, corpos e, principalmente, a Teoria de Galois, afim de perceber que polinômios gerais de grau maior ou igual a 5 não possuem um fórmula resolutiva e que polinômios de grau maior ou igual a 5, que não são da forma geral, só serão solúveis por meio de radicais caso pertençam ao grupo denominado Grupo de Galois.

No trabalho, apresentamos dois exemplos sobre equações polinomiais do tipo $x^n - a$, sendo uma de grau 3 e outra de grau 4 e generalizamos através do Lema 3.4.4. Para fazer o estudo de equações polinomiais “maiores” utilizando a Teoria de Galois, seriam necessários alguns cálculos a mais, no entanto, a solução em cada caso é obtida de modo análogo ao apresentado neste trabalho.

Apesar da importância da Teoria de Galois, os estudos envolvendo a determinação de raízes de equações polinomiais não tiveram fim com a descoberta de Galois, até porque métodos numéricos e algébricos continuaram sendo desenvolvidos. Além disso, com o advento das tecnologias, contamos atualmente com softwares matemáticos que também nos auxiliam nessa tarefa.

Referências Bibliográficas

- [1] A ORIGEM DAS EQUAÇÕES DO 1º GRAU. *Disponível em:* <http://www.matematiques.com.br/conteudo.php?id=582>. Acesso em 10 março 2017.
- [2] EVARISTE GALOIS, O GÊNIO AZARADO. *Disponível em:* <http://super.abril.com.br/cultura/evariste-galois-o-genio-azarado/>, Da Redação. Acesso em 08 março 2017.
- [3] GONÇALVES, ADILSON, *Introdução à Álgebra*, IMPA - Projeto Euclides, Rio de Janeiro, (1979).
- [4] HERSTEIN, I.N., *Tópicos de Álgebra*, Editora da Universidade de São Paulo, Editora Polígono, São Paulo, (1970), 408 p. ilustr.
- [5] HYGINO, H. DOMINGUES; IEZZI, GELSON, *Álgebra Moderna*, Volume único - 4ª Ed. reform. - São Paulo; Atual, 2003.
- [6] IEZZI, GELSON, *Fundamentos de Matemática Elementar*, 7ª Edição - São Paulo; Atual, 1939.
- [7] SANTOS, CARLOS PEREIRA; NETO, JOÃO PEDRO; SILVA, JORGE NUNO, *Galois: A Teoria de Grupos + o Puzzle do 15*, [Lisboa] : Público-Visão, imp. 2007. (Jogos com história). - ISBN 978-989-6122-70-6.
- [8] SILVA, MARCOS NOÉ PEDRO DA. *"O Surgimento da Equação do 2º Grau"; Brasil Escola. Disponível em* <http://brasilecola.uol.com.br/matematica/o-surgimento-equacao-2-o-grau.htm>. Acesso em 10 de março de 2017.

- [9] VILLELA, MARIA LÚCIA TORRES. *GRUPOS*. Disponível em: <http://www.professores.uff.br/marco/algebraII-2014/grupos-mod1.pdf>. Acesso em 08 abril 2017.