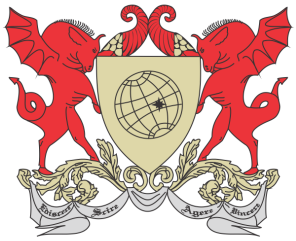
Universidade Federal de Viçosa

Dissertação de Mestrado



Cristiano Gonçalves Augusto

Equações Algébricas: soluções e aplicações

Florestal
Minas Gerais – Brasil
2019

Cristiano Gonçalves Augusto

EQUAÇÕES ALGÉBRICAS: SOLUÇÕES E APLICAÇÕES

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional, para obter o título *Magister Scientiae*.

Florestal
Minas Gerais – Brasil
2019

Ficha catalográfica preparada pela Biblioteca da Universidade Federal de Viçosa - Câmpus Florestal

T
A923e
2019

Augusto, Cristiano Gonçalves, 1981-
Equações Algébricas : soluções e aplicações / Cristiano Gonçalves Augusto. – Florestal, MG, 2019.
viii, 120 f. : il. (algumas color.) ; 29 cm.

Inclui apêndices.
Orientador: Danielle Franco Nicolau Lara.
Dissertação (mestrado) - Universidade Federal de Viçosa.
Referências bibliográficas: f.117.

1. Álgebra. 2. Matemática. 3. Teoria das equações. I. Universidade Federal de Viçosa. Departamento de Matemática. Mestrado Profissional em Matemática em Rede Nacional. II. Título.

512

CRISTIANO GONÇALVES AUGUSTO

EQUAÇÕES ALGÉBRICAS: SOLUÇÕES E APLICAÇÕES

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional, para obter o título *Magister Scientiae*.

APROVADA: 11 de abril de 2019.

Gerson Geraldo Chaves

Camila Ferreira de Souza

Justino Muniz Junior

Daniele Franco Nicolau Lara
(Orientadora)

Dedicatória

Ao meu irmão Ângelo Gonçalves Augusto, pelo convívio, apoio e amizade.

Agradecimentos

Agradeço a Deus, pela vida, pela saúde e, em especial, pela inspiração no decorrer deste trabalho.

Agradeço, carinhosamente, aos meus pais, Conceição Gonçalves Augusta e Ramiro Sérvulo Augusto, pelo amor incondicional, pelos ensinamentos e pelo apoio em todos os momentos de minha vida.

Agradeço ao minha orientadora, Danielle Franco Nicolau Lara, por ter me apoiado e acreditado que este trabalho era pertinente e possível de se realizar. Obrigado pela paciência e pelas anotações de grande valia. Tenho certeza de que não poderia ter percorrido este caminho em melhor companhia.

Lista de Figuras

Resumo

AUGUSTO, Cristiano Gonçalves, M.Sc., Universidade Federal de Viçosa, abril de 2019. **Equações Algébricas: soluções e aplicações**. Orientadora: Danielle Franco Nicolau Lara.

Neste trabalho discutiu-se a resolubilidade das equações algébricas com coeficientes reais de grau menor ou a igual a quatro, as relações existentes entre coeficientes e raízes das equações gerais, o Teorema Fundamental da Álgebra, e no caso de grau maior que quatro focaremos de forma elementar a Teoria de Galois. Introduziu-se aspectos elementares da teoria dos grupos, números complexos, a geometria do plano complexo, propriedades básicas dos polinômios e fatoração de polinômios para compreensão da resolubilidade de equações algébricas. Com isso, esclarecer conceitos teoria da algébrica para possibilitar uma prática mais adequada ao estudante do ensino médio. Então, enfatizou-se a resoluções de equações algébricas de grau menor ou igual a quatro e apresentou-se, para docentes da educação básica e superior, a Teoria de Galois para grau maior ou igual a cinco. Apresentou-se no final deste trabalho algumas aplicações em sala de aula sobre as soluções de equações algébricas de grau ≤ 4, e um estudo que envolva aproximações numéricas e o *software GeoGebra* para determinar a solução de uma equação do 5° grau. A aplicação foi direcionada aos alunos 3° ano do ensino médio, no intuito de contextualizar este trabalho e sugerir uma abordagem diferenciada na solução de equações algébricas. E ainda, motivar o docente a buscar novas metodologias de ensino sobre soluções de equações algébricas.

Abstract

AUGUSTO, Cristiano Gonçalves, M.Sc., Universidade Federal de Viçosa, April, 2019. **Algebraic equations: solutions and applications**. Adviser: Danielle Franco Nicolau Lara.

At this work we will discuss the algebraic equations resolution with real coefficients of lesser or equal degree to four, the relations existent between coefficients and roots of the general equations, the Fundamental Theorem of Algebra, and in the case of a greater degree than four we will concentrate substantially or Galois Theory. We will introduce elementary of group theory aspects, complex numbers, geometry of the complex plane, basic polynomial properties, and polynomial factorization to be able us to understand the solubility of algebraic equations. In order to enable more adequate practice for the high school student, we will emphasize resolutions of algebraic equations of lesser or equal degree to four. And we will present the Theory of Galois to a greater or equal degree to five. At the end of this paper, we presented some applications in the classroom about solutions of degree ≤ 4 algebraic equations, and a study involving approximations and *GeoGebra* software to determine the solution of an equation of 5 degree. The application was directed to students of the 3rd grade of high school, in order to contextualize this work and suggest a differentiated approach in the solution of algebraic equations. And, motivate the teacher to seek new methodologies of teaching about solutions of algebraic equations.

Sumário

1

Introdução

Visto que a solução de equações algébricas é amplamente trabalhado na educação básica e superior, necessitou-se de um estudo sistemático sobre esse assunto sendo direcionado para professores da educação básica. Com o objetivo esclarecer e ampliar conceitos e propriedades da Álgebra no domínio da solubilidade de equações algébricas. Alguns pesquisadores brasileiros destacam-se neste campo de pesquisa, dentre eles, o professor Doutor Adilson Gonçalves.

Neste trabalho discutiu-se no Capítulo 2 a teoria de de anéis e corpos e ampliou-se o estudo dessa teoria no Capítulo 5. No Capítulo 3 abordamos sobre os polinômios com coeficientes em anéis e suas raízes e citamos o Teorema Fundamental da Álgebra. No Capítulo 4 introduzimos conceitos básicos de números complexos, trabalhamos a resolubilidade das equações algébricas com coeficientes reais de grau menor ou a igual a quatro, as relações existentes entre coeficientes e raízes da equação de quarto grau. Nos Capítulos 6 e 7 abordamos conceitos básicos da teoria de grupos e a Teoria de Galois elementar. E no Capítulo 8 apresentamos uma proposta de atividade sobre solubilidade de equações algébricas para alunos 3° ano do ensino médio.

Introduziu-se aspectos elementares de teoria dos grupos, números complexos, propriedades básicas dos polinômios e fatoração de polinômios para compreendermos a resolubilidade das equações algébricas.

A teoria de grupos permite um vasto desenvolvimento na teoria algébrica, e também há aplicação prática na sociedade contemporânea, como exemplo, na teoria dos códigos corretores de erros.

Há importantes propriedades nas seguintes relações de inclusão dos conjuntos $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, que possuem estrutura de anel, são munidos das operações de adição e de multiplicação, com propriedades específicas tratadas neste trabalho.

Nota-se a importância histórica da resolubilidade das equações algébricas que foi debatida por muitos matemáticos.

Hefez e Villela [10] (2012 p.170), apontam que

> *Passaram-se vários séculos até que se conseguisse resolver as equações de graus três e quatro, tarefa realizada pelos matemáticos de Bolonha, Itália, no século 16. O problema da resolubilidade das equações de grau maior ou igual do que cinco se constituiu, desde então, num dos problemas centrais*

> *da Matemática até ser totalmente elucidado pela Teoria de Galois, na primeira metade do Século 19. (HEFEZ E VILLELA, 2012, p. 170)*

Abordaremos demonstrações sistemáticas de diversos teoremas, proposições e corolários, com o objetivo de ratificar a teoria corpos e grupos e esclarecer de forma rigorosa as fórmulas de resolubilidade das equações algébricas.

O estudo do corpo dos números complexos leva-nos a ampliar a resolução das equações algébricas já que algumas equações em $\mathbb{R}$ não possuem solução. Por exemplo, a equação $x^2 = -1$, cuja solução é $i, -i \in \mathbb{C}$. Além de auxiliar na compreensão das soluções de equações algébricas de terceiro e quarto graus. Segundo Hefez [9] (p.173) "O corpo dos números reais foi criado com o objetivo de completar o corpo dos números racionais [...]".

O século XVII apresentou uma intensa atividade em torno da forma dos complexos. Os primeiros resultados podem ser encontrados, em 1747, na dissertação de d'Alembert sobre os ventos. No artigo, 79, ele afirma que uma quantidade qualquer, composta de tantos complexos quanto desejarmos, pode ser reduzida à forma $A + B\sqrt{-1}$ com A e B quantidades reais. Euler aborda esta temática em sua obra *Recherches sur les racines imaginaires des équations*, de 1749, com diversos teoremas e corolários, dos quais ressaltamos o teorema XII, que afirma que todo fração formada por adição, subtração, multiplicação ou por divisão envolvendo quantidades complexas quaisquer da forma $A + B\sqrt{-1}$, terá a mesma forma $A + B\sqrt{-1}$ em que A e B representam quantidades reais.

A partir do final do século XVIII e início do século XIX, começaram a ser sugeridas diferentes representações geométricas para os números negativos e complexos, tentando garantir a sua aceitação no universo dos números. Além do nome de Gauss, também são importantes os nomes dos matemáticos Caspar Wessel e Jean-Robert Argand.

Por séculos, matemáticos se empenharam em resolver equações algébricas. Fórmulas foram determinadas para soluções de equação de terceiro e quarto graus. Mas, para equações gerais de grau maior do que ou igual a 5 não há soluções por meio de radicais. Vidigal et al. [18] afirma que, tal como no caso das equações de terceiro e quarto graus, existem equações de grau maior do que ou igual a 5 que não são solúveis por radicais, isto é, não existe uma fórmula que expresse suas raízes em função de seus coeficientes, utilizando apenas as operações de adição, subtração, multiplicação, divisão e extração de raízes n-ésimas. Esse importante resultado foi provado no século XIX por Abel (1802 – 1829) e Galois (1811 – 1832).

Portanto, a teoria algébrica é um campo da matemática que está em constante desenvolvimento. Notam-se diversas publicações de artigos, dissertações e eventos nacionais e internacionais para debates sobre essa teoria. Destaca-se no Brasil o evento semestral de algebristas, conhecida como *A Escola de Álgebra*, que é uma reunião semestral de algebristas dedicado inteiramente à Álgebra e tópicos relacionados. Seu principal objetivo é proporcionar uma oportunidade para pesquisadores e estudantes, de comunicarem e discutirem resultados de pesquisas em todos os ramos da Álgebra.

2

Anéis e Corpos

Neste capítulo descreveremos os conceitos básicos de Anéis e Corpos necessários para a compreensão da teoria das equações polinomiais. A teoria deste capítulo está de acordo com [7], [8] e [9].

2.1 Definições e propriedade básicas de Anéis

Os conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ são exemplos de aneis. Quais são as condições que esses conjuntos possuem para que sejam assim definidos? A seguir veremos essas condições e outras características.

Como em [7], descrevemos um anel por satisfazer condições $A'is$, e introduziremos propriedades adicionais $B'is$ e $C'is$ para designarmos aneis especiais.

Definição 2.1: Sejam A um conjunto e $(+)$ e $(\cdot)$ duas operações em A, chamadas de adição e multiplicação. A terna $(A, +, \cdot)$ será chamada de *anel* se as operações gozarem das seis propriedades enunciadas a seguir.

A1) A adição é associativa. Quaisquer que sejam $a, b, c \in A$, tem-se que $(a+b)+c = a+(b+c)$.

A2) A adição é comutativa. Quaisquer que seja $a, b \in A$, tem-se que $a + b = b + a$.

A3) Existe um elemento neutro para a adição. Existe $\alpha \in A$ tal que $\alpha + a = a$, para todo $a \in A$.

A4) Todo elemento de A possui um simétrico. Para todo $a \in A$, existe $a' \in A$ tal que $a + a' = \alpha$.

A5) A multiplicação é associativa. Quaisquer que sejam a, b, c em A, tem-se que $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

A6) A multiplicação é distributiva com relação à adição. Quaisquer que sejam $a, b, c \in A$, tem-se que $a \cdot (b + c) = a \cdot b + a \cdot c$.

Se um anel A satisfaz a propriedade:

B7) Quaisquer que sejam $a, b \in A$, tem-se que $a \cdot b = b \cdot a$. Dizemos que é um *anel comutativo*.

E se satisfaz a propriedade:

B8) Existe um elemento neutro para a multiplicação. Existe $e \in A$, com $e \neq \alpha$, tal que $a \cdot e = a$, para todo $a \in A$. Dizemos neste caso que A é um *anel com unidade*.

Usaremos o símbolo 0 para denotar o elemento neutro da adição (único), que será chamado de elemento zero, ou de elemento nulo. O símbolo 1 para denotar o elemento neutro da multiplicação (único), que será chamado de unidade do anel, ou apenas unidade. O simétrico de um elemento denotado a será simbolizado por $-a$.

Os exemplos iniciais de aneis são os conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Esses conjuntos tem características importantes, que nos auxiliam na resolução de equações. Por exemplo, encontrar $x \in \mathbb{R}$, tal que $x^2 - 4 = 0$ é uma tarefa simples, uma vez que $x^2 - 4 = (x+2)(x-2)$ e daí $(x+2)(x-2) = 0$ nos dá $x + 2 = 0$ e $x - 2 = 0$, ou seja, $x = 2$ e $x = -2$. Mas essa conclusão não é válida para quaisquer aneis, somente para aqueles que são ditos domínios de integridade, o que definiremos adiante.

Temos ainda a propriedade de um anel A sem divisores de zero.

Definição 2.2: Um *divisor de zero* em um anel A é um elemento $a \in A$, não nulo tal que $\exists\ b \in A$, com $b \neq 0$ e $a \cdot b = 0$.

Definição 2.3: Se A é um anel comutativo, com unidade e sem divisores de zero, dizemos que $(A, +, \cdot)$ é um *domínio de integridade*, ou simplesmente um *domínio*.

Assim, em um domínio A, temos: $a, b \in A$ tais que: $a \cdot b = 0$, então $a = 0$ ou $b = 0$. Vale, também, uma importante propriedade, a lei do cancelamento:

Teorema 2.1: Sejam a, b e c pertencente a um domínio de integridade. Se $a \neq 0$ e $ab = ac$ então $b = c$. Reciprocamente se A é um anel comutativo com unidade, satisfazendo a propriedade de cancelamento então K não possui divisores de zeros e portanto A é um domínio de integridade.

Demonstração. De $ab = ac$ temos $a(b - c) = 0$ e como $a \neq 0$ e estamos em um domínio temos $b = c$. Reciprocamente, suponha que A satisfaz a lei do cancelamento e $ab = 0$. Então $ab = a \cdot 0$ como $a \neq 0$ pela lei do cancelamento $b = 0$. Mostrando que A não possui divisores de zero. □

Vejamos alguns exemplos

Exemplo 2.1.1: O anel $\mathbb{Z}_n$ é comutativo com unidade sendo a unidade a classe $\bar{1}$ e é um domínio.

Segue a definição de $\mathbb{Z}_n$.

Seja n um inteiro positivo, para $a, b \in \mathbb{Z}$, definimos a relação

$$a \equiv b \mod n \Leftrightarrow n|(b - a).$$

Lê-se: a é congruente à b módulo n se, e somente se, n divide $b-a$.
Essa relação possui as propriedades

1 Reflexiva ($a \equiv a \ \forall \ a \in \mathbb{Z}$)

De fato, $a - a = 0$ e $n \mid 0 \ \forall \ n \in \mathbb{Z}$.

2 Simétrica (Para quaisquer $a, b \in \mathbb{Z}, a \equiv b \mod n \Rightarrow b \equiv a \mod n$).

Se $a \equiv b \mod n$ temos $n \mid a - b$, logo $a - b = kn$ para algum $k \in \mathbb{Z}$. Note que $b - a = -kn$ com $-k \in \mathbb{Z}$, assim $n \mid b - a$ e $b \equiv a \mod n$.

3 Transitiva (Para quaisquer $a, b, c \in \mathbb{Z}$), $a \equiv b \mod n$ e $b \equiv c \mod n \Rightarrow a \equiv c \mod n$)

Se $a \equiv b \mod n$ e $b \equiv c \mod n$ temos.

$$n \mid a - b \Rightarrow a - b = k_1 n, \ k_1 \in \mathbb{Z}$$
$$n \mid b - c \Rightarrow b - c = k_2 n, \ k_2 \in \mathbb{Z}.$$

Assim $a - b + b - c = k_1 n + k_2 n$ o que nos dá

$$a - c = (k_1 + k_2)n \text{ com } k_1 + k_2 \in \mathbb{Z}$$

Logo $a \equiv c \mod n$.
Assim essa relação é de equivalência e é chamada de congruência. Como toda relação e equivalência, a congruência particiona $\mathbb{Z}$ em subconjuntos disjuntos ditos classes de congruência, $\bar{a}$

$$\bar{a} = \{a \equiv b \mod n\}$$

As classes de congruência em $\mathbb{Z} \mod n$, serão as classes dos restos da divisão por n. Com efeito, dado a em $\mathbb{Z}$, pelo algorítmo de Euclides temos $a = qn + r$ com $0 \leq r < n$. Isto mostra que $a \equiv r \mod n$ e reciprocamente, se $a \equiv b \mod n$, então $n|(b-a) \Rightarrow b - a = kn$ e $b = nq_1 + r_1, \ a = nq_2 + r_2$ pela divisão euclidiana, com $0 \leq r_1 < n$ e $0 \leq r_2 < n$.
Assim,

$$kn = b - a = (q_1 - q_2)n + (r_1 - r_2),$$

como $r_1 - r_2 < n$ temos $r_1 = r_2$.
Denotaremos por $\mathbb{Z}_n$ o conjunto das classes de congruência de $\mathbb{Z}$ módulo n. Assim,

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$$

A este conjunto atribuímos duas operações. Seja $\bar{a}$ e $\bar{b}$ classes em $\mathbb{Z}_n$. Definimos,

$$\bar{a} + \bar{b} = \overline{a+b} = \text{(soma de classes)}$$
$$\bar{a} \cdot \bar{b} = \overline{a \cdot b} = \text{(produto de classes)}$$

Note que as operações acima descritas estão bem definidas. O conjunto $\mathbb{Z}_n$, munido da soma e da multiplicação de classes será denotado por $(\mathbb{Z}_n+,\cdot)$ e tem caraterística de anel já que a soma e o produto satisfazem as propriedades da Definição 2.1. Na verdade $\mathbb{Z}_n$ é um anel comutativo com unidade, além disso, se $\bar{a} \cdot \bar{b} = 0$, temos $\overline{a \cdot b} = 0$ e $ab \equiv 0 \mod n \Rightarrow n \mid ab$. Agora $n \mid ab$ implica $n \mid a$ ou $n \mid b$ ocorre se, e somente se, n é primo. Assim $\mathbb{Z}_n$ é domínio se, e só se, n é primo.

Exemplo 2.1.2: Os anéis $\mathbb{Z}, \mathbb{Q}, \mathbb{C}, \mathbb{R}$ são domínios. Já que $\mathbb{Z}_6$ não é um domínio pois $\bar{2} \cdot \bar{3} = \bar{0}$ e $\bar{2}, \bar{3} \neq \bar{0}$

Exemplo 2.1.3: $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ é domínio.

Note que o zero do anel é $0 = 0 + 0\sqrt{2}$ e a unidade $1 = 1 + 0\sqrt{2}$. Além disso, se $x, y \in \mathbb{Z}[\sqrt{2}]$, $x = a + b\sqrt{2}$ e $y = c + d\sqrt{2}$ são tais que $xy = 0$, temos

$$xy = (ac + 2bd) + (ad + bc)\sqrt{2} = 0 \Leftrightarrow (ac + 2bd) = 0 \text{ e } (ad + bc) = 0$$

O sistema formado por essas equações somente possui as soluções triviais em $\mathbb{Z}[\sqrt{2}]$. Então,

$$x = 0 \text{ ou } \ y = 0.$$

Exemplo 2.1.4: Considere o conjunto $\mathbb{Z}_n[i] = \{a + bi \mid a, b \in \mathbb{Z}_n \text{ e } i = \sqrt{-1}\}$. Aqui, para facilitar a escrita, escreveremos a classe $\bar{a} \in \mathbb{Z}_n$ simplesmente por a. Com as operações,

$$\text{Soma } : \ (a + bi) + (c + di) = (a + c) + (b + d)i$$
$$\text{Multiplicação } : \ (a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i, \mathbb{Z}_n[i] \text{é anel.}$$

$\mathbb{Z}_n[i]$ é um anel.

Para finalizarmos os conceitos básicos de anel, chamaremos de anel ordenado, o anel A no qual existe uma relação de ordem $(\leq)$ em A, que possui as seguintes propriedades adicionais:

C9) Compatibilidade com a adição. Para todos a, b, c em A, se $a \leq b$, então $a + c \leq b + c$.

C10) Compatibilidade com a multiplicação. Para todos a, b, c em A, se $a \leq b$ e $0 \leq c$, então $a \cdot c \leq b \cdot c$

Exemplo 2.1.5: $\mathbb{R}$ é um anel ordenado já que a relação $\leq$ (menor ou igual que) é uma relação de ordem em $\mathbb{R}$.

Há subconjuntos de aneis mais importantes que outros, que no estudo desta teoria traz muitas informações sobre o anel estudado. Um desses subconjuntos são os chamados subaneis.

Definição 2.4: Um subconjunto não vazio S de um anel A é dito ser um *subanel de* A se, com as operações induzidas pelas operações de A (restrições), S é um anel.

O teorema é abaixo é conhecido com *Teste para Subanel*.

Teorema 2.2: Um subconjunto $S \neq \varnothing$, de um anel A é um subanel de A se, e somente se valem as seguinte afirmações:

1. Para todo $a, b \in S \Rightarrow a - b = a + (-b) \in S$
2. Para todo $a, b \in S \Rightarrow ab \in S$

Demonstração. Como as propriedades comutativa, associativa, distributiva são válidas para A, então são para S. Verificaremos se as operações são fechadas, se o elemento neutro aditivo está em S e se o inverso aditivo de cada elemento de S está em S. S é fechada para o produto pela propriedade 2 da hipótese.

Como $S \neq \varnothing$, tome m em S. Por hipótese $m - m = 0 \in S$. Então elemento neutro aditivo está em S.

Se $a \in S$, por hipótese, $0 - a = -a \in S$ para todo $a \in S$. Logo, o inverso aditivo de cada elemento de S está em S.

Sejam se a e $b \in S$, então $a + b = a - (-b) \in S$ e $ab \in S$ por hipótese.

E o teste está provado. □

Exemplo 2.1.6: $\mathbb{Z}$ é subanel de $\mathbb{Q}$ e $\mathbb{Q}$ é subanel de $\mathbb{R}$.

Exemplo 2.1.7: O conjunto $D_7 = \left\{ \frac{a}{7^k}; a \text{ é inteiro e } k \in \{1,2,3\ldots\} \right\}$ é um subanel de $(\mathbb{Q}, +, \cdot)$.

Tomando $a = 0 \Rightarrow 0 \in D_7$. Logo $D_7 \neq \varnothing$.

Sejam $x = \frac{a_1}{7_1^k}$ e $y = \frac{a_2}{7_2^k} \in D_7$. Suponhamos, sem perda de generalidade, que $k_1 \leq K_2$. Então,

$$x - y = \frac{a_1}{7^{k_1}} - \frac{a_2}{7^{k_2}} = \frac{a_1 7^{k_2 - k_1 - a_2}}{7^{k_2}} \in D_7$$
$$x \cdot y = \frac{a_1}{7^{k_1}} \cdot \frac{a_2}{7^{k_2}} = \frac{a_1 a_2}{7^{k_1 + k_2}} \in D_7.$$

Portanto, D_7 é um subanel de $\mathbb{Q}$.

Outra propriedade importante de um anel A é o que chamamos de característica. Note que para todo $x \in \mathbb{Z}_{11}[i] = \{a + bi | a, b \in \mathbb{Z}_{11} \text{ e } i = \sqrt{-1}\}$, $x = a + bi$, então,

$$11x = 11a + 11bi = 0 + 0i = 0.$$

Do mesmo modo para o anel $B = \{0, 4, 8, 12\}$ contido em $\mathbb{Z}_{20}$, encontramos, para todo $y \in B$, $5y = \bar{0}$. Estes exemplos motiva a seguinte definição.

Definição 2.5: A *característica de um anel* A é o menor inteiro positivo n tal que $nx = 0$ para todo $x \in A$. Se tal elemento n não existe nós dizemos que A tem a característica 0. Usaremos a notação $car(A)$.

Exemplo 2.1.8: $\mathbb{Z}$ tem a característica zero e $\mathbb{Z}_n$ tem característica n. O anel $\mathbb{Z}_7[x]$, denotamos por $\mathbb{Z}_7[x]$ o conjunto de todos os polinômios com coeficientes em $\mathbb{Z}_7$, tem característica 7.

Teorema 2.3: Seja A um anel com unidade 1. Se e n é o menor inteiro positivo tal que $n \cdot 1 = 0$ então a característica de A é n. Se não existe n inteiro positivo tal que $n \cdot 1 = 0$ então a característica de A é 0.

Demonstração. Se n é o menor inteiro positivo tal que $n \cdot 1 = 0$ temos que $nx = n(1x) = (n \cdot 1)x = 0$ para todo x em A. Suponhamos que não existe n inteiro positivo tal que $n \cdot 1 = 0$. Então, pela definição de característica de A, $car(A) = 0$. □

Finalizaremos esta subseção com o seguinte teorema.

Teorema 2.4: A característica de um domínio é 0 ou um número primo.

Esse teorema é muito interessante, sua demonstração utiliza elementos algébricos mais abstratos e pode ser verificado em [7].

2.1.1 Ideais e anéis quocientes

Certos subaneis de um anel A são mais importantes por serem usados para definirmos outros aneis quocientes. Esses subaneis são ditos ideais.

Definição 2.6: Um subanel I de um anel A é chamado um *ideal de* A se para todo $a \in A$ e todo $x \in I$, temos, $xa \in I$ e $ax \in I$.

Dado um anel A, então A e $\{0\}$ são sempre ideais de A, que chamaremos de ideais triviais. E ao ideal $I \neq A$, chamaremos de ideal próprio.

Existe um teste para sabermos se um subconjunto do anel A é um ideal de A. Note a semelhança com o teste para saber se um subconjunto é um subanel. A demonstração encontra-se na bibliografia indicada neste capítulo. Segue abaixo este teste.

Teorema 2.5: Um subconjunto não vazio de um anel I é um ideal de A se:

1. $a - b \in I$, para todo $a, b \in I$
2. xa e ax estão em I quando $a \in A$ e $x \in I$.

Exemplo 2.1.9: Para qualquer inteiro positivo n, $nZ = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$ é um ideal de $\mathbb{Z}$. Como os únicos subanéis de $\mathbb{Z}$ são os da forma nZ, estes também são os únicos ideais de $\mathbb{Z}$

Definição 2.7: Um anel com unidade 1 será chamado de *simples* se A e 0 são os únicos ideais de A.

A proposição abaixo explica um modo de determinarmos se um ideal I é um ideal trivial de A.

Proposição 2.1: Suponha que A é um anel com unidade 1 e I é um ideal de A. Se $1 \in I$, então $I = A$.

Demonstração. Como $I \subset A$. Falta provar que $A \subset I$. Seja a qualquer elemento de A, então $a = a \cdot 1 = 1 \cdot a \in I$. Portanto $A \subset I$, logo $A = I$. □

Definição 2.8: Seja A um anel comutativo com unidade e seja $X = \{x_1, x_2, \ldots, x_n\}$ um subconjunto de A. Então definimos o *ideal* X *de* A, por

$$\langle X \rangle = < x_1, x_2, \ldots, x_n > = \{r_1x_1 + r_2x_2 + \ldots r_nx_n | r_i \in A\}.$$

Note que $\langle X \rangle$ é o menor ideal de A que contém X.
Finalizaremos as propriedades de ideais com a seguinte definição.

Definição 2.9: Seja A um anel comutativo com unidade.

1. Um ideal I de A é dito *finitamente gerado* se $I = \langle X \rangle$, para algum conjunto finito X .

2. Um ideal I de A é dito *principal* se $I =< a >$, para algum elemento $a \in A$. No qual $< a >= \{ra | r \in A\}$.

Vejamos agora a definição de *aneis quocientes*.
Seja I, um ideal de A e considere a seguinte relação entre os elementos de A:
Sejam $a, b \in A$ temos que $a \equiv b \mod I$ (lê-se a é congruente a b módulo I) se, e somente se, $a - b \in I$.
Note que a relação $\equiv$ definida acima é uma relação de equivalência em A e portanto, particiona A em subconjuntos disjuntos chamados classes de equivalência.
Para $a \in A$, a classe de equivalência definida por a é o conjunto,

$$\begin{aligned} \bar{a} = a + I &= \{b \in A \mid b \equiv a \mod I\} \\ &= \{b \in A \mid b - a \in I\}. \end{aligned}$$

Denotemos por A/I o conjunto quociente dessa relação,
$A/I = \{a + I | a \in A\}$.
Em A/I definimos duas operações (soma e multiplicação), conforme o Teorema 2.6.

Teorema 2.6: Seja A um anel e I um ideal de A. Se $\bar{x} = x + I$ e $A/I = \{\bar{x} \colon x \in A\}$, então:

(a) A relação + definida por : $A/I \times A/I \to A/I$; $(\bar{x}, \bar{y}) \to \overline{x + y} = \bar{x} + \bar{y}$ é uma operação em A/I denominada soma;

(b) A relação $\cdot$ definida por : $A/I \times A/I \to A/I$; $(\bar{x}, \bar{y}) \to \overline{x \cdot y} = \bar{x} \cdot \bar{y}$ é uma operação em A/I denominada multiplicação;

(c) $(A/I, +, \cdot)$ é um anel (chamado *anel quociente* de A em I)

(d) Se 1 é a unidade de A então $\bar{1}$ é a unidade de A/I.

(e) Se A é comutativo então A/I é comutativo.

(f) Se 0 é o elemento neutro de A então $\bar{0}$ é o elemento neutro de A/I.

(g) Se $-x$ é o inverso aditivo de x em A então $-\bar{x}$ é o inverso aditivo de $\bar{x}$ em A/I.

Deixaremos para o leitor a verificação da demonstração deste teorema em [7], que segue diretamente da definição de A/I.

As operações definidas em A/I também podem ser denotadas da seguinte forma: Seja $\bar{x} = x + I$ e $\bar{y} = y + I$ então,

$$(x + I) + (y + I) = (x + y) + I$$
$$(x + I) \cdot (y + I) = (x \cdot y) + I$$

Exemplo 2.1.10: Temos $2\mathbb{Z}/6\mathbb{Z} = \{0 + 6\mathbb{Z}, 2 + 6\mathbb{Z}, 4 + 6\mathbb{Z}\}$. Observe que $6\mathbb{Z}$ é um ideal de $2\mathbb{Z}$ e que todo elemento da forma $2n$ pode ser escrito da forma $2(3q + r) = 6q + 2r$ quando aplicamos o Algoritmo de Euclides para n e 3. Então os restos serão múltiplos de 2. Assim os elementos de $2\mathbb{Z}/6\mathbb{Z}$ serão $0 + 6\mathbb{Z}, 2 + 6\mathbb{Z}$ e $4 + 6\mathbb{Z}$.

Ainda sobre ideais, temos duas importantes definições.

Definição 2.10: Sejam A um anel comutativo e $I \subset A$ um ideal. Dizemos que I é um *ideal primo*, se I é um ideal próprio, e:

$$\forall\ a, b \in A, ab \in I \Rightarrow a \in I \text{ ou } b \in I$$

Definição 2.11: Um ideal próprio I de um anel A é *maximal* se um ideal B de A tal que $I \subseteq B \subseteq A$ então $I = B$ ou $B = A$

Exemplo 2.1.11: $\mathbb{Z} \times \{0\}$ é um ideal primo de $\mathbb{Z} \times \mathbb{Z}$.

De fato seja $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$ tal que $(a, b)(c, d) \in \mathbb{Z} \times \{0\}$. Então $ac \in \mathbb{Z}$ e $bd \in \{0\}$. Já que $\mathbb{Z}$ é um domínio de integridade temos que ou $(a, b) \in Z \times \{0\}$ ou $(c, d) \in \mathbb{Z} \times 0$.

Exemplo 2.1.12: Seja p primo. Então $p\mathbb{Z}$ é um ideal maximal de $\mathbb{Z}$. Por exemplo, $5\mathbb{Z} \subset \mathbb{Z}$ é um ideal maximal.

De fato, se I é um ideal tal que $5\mathbb{Z} \subsetneq I \subset \mathbb{Z}$ então $I = \mathbb{Z}$. Vamos mostrar que $1 \in I$. Como $5\mathbb{Z} \subset I$, existe $a \in I$ não divisível por 5. Portanto a e 5 são *coprimos* e $5n + am = 1$ para alguns $n, m \in \mathbb{Z}$. Portanto $1 \in I$.

Os próximos dois teoremas ampliam as propriedades sobres anéis quocientes. E as demonstrações encontram-se em [12]

Teorema 2.7: Seja A um anel comutativo com unidade e I um ideal próprio de A. Então A/I é domínio, se, e somene se, I é primo.

Teorema 2.8: Seja A um anel comutativo com unidade e I um ideal de A. Então A/I é corpo se, e somente se, I é maximal.

Definiremos uma função entre aneis. Chamaremos de homomorfismo de anéis as funções que preservam as operações soma e produto dos anéis.

Definição 2.12: Dados dois anéis A e B, uma função $f\colon A \longrightarrow B$ é chamada de um *homomorfismo de anéis* se para todo $a, b \in A$, vale:

1. $f(a+b) = f(a) + f(b)$;
2. $f(a \cdot b) = f(a) \cdot f(b)$.

Definição 2.13: Um homomorfismo $f\colon A \longrightarrow B$ é chamado de um *isomorfismo* se for, também, uma bijeção. Nesse caso, dizemos que A e B são isomorfos e denotamos $A \approx B$.

Exemplo 2.1.13: Em geral se I é um ideal de um anel A a aplicação que associa a cada elemento a de A a sua classe $a + I$ é um homomorfismo de anéis chamado homomorfismo canônico.

Definição 2.14: O *núcleo* de um homomorfismo de anéis $f\colon A \longrightarrow B$ é o conjunto

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

em que 0_B é o elemento neutro do anel B.

O homomorfismo possui diversas propriedades vejamos algumas.

Proposição 2.2: Seja $f\colon A \longrightarrow B$ um homomorfismo de anéis e $N(f)$ o núcleo de f. Então,

P1 $f(a) = f(b)$ se, e somente se, $b - a \in N(f)$.

P2 f é injetora se, e somente se, $N(f) = \{0_A\}$.

Demonstração. Provaremos $[P1]$. Se $f(a) = f(b)$ então,

$$f(a) - f(b) = 0_B \Rightarrow f(a-b) = 0_B \Rightarrow a - b \in N(f).$$

Reciprocamente, se $a - b \in N(f)$ então,

$$f(a-b) = 0_B \text{ e } f(a) = f(b).$$

Em $[P2]$. Seja f injetora e $a \in N(f)$, mostraremos que $a = 0_A$. De fato, como $f(a) = 0_B$, $f(0_A) = 0_B$, e f é injetiva segue que $a = 0_A$. Portanto $N(f) = 0_A$.

Reciprocamente, seja $N(f) = \{0_A\}$. Se $f(a) = f(b)$, então por $[P1]$ temos que $b - a \in N(f)$. Como estamos considerando $N(f) = \{0_A\}$, se que daí que $b - a = 0_A$, isto é, $a = b$. Portanto f é injetora. □

Vejamos algumas propriedades. Demonstraremos a três primeiras e deixaremos para consulta as outras demonstrações na bibliografia indicada neste capítulo.

Teorema 2.9: Sejam A e B aneis e $\phi : A \longrightarrow B$. Então:

1. $\phi(0) = 0$;
2. $\phi(-r) = -\phi(r)$ para todo r em A
3. Para todo r em A e todo inteiro positivo n, $\phi(nr) = n\phi(r)$ e $\phi(r^n) = \phi(r)^n$.
4. Se C é um subanel de A então $\phi(C)$ é um subanel de B.
5. Se I é um ideal de A e ϕ é sobrejetivo então $\phi(I)$ é um ideal de B.
6. Se J é um ideal de B então $\phi^{-1}(J)$ é um ideal de A
7. Se A é comutativo então $\phi(A)$ é comutativo.
8. Se A tem unidade 1 e ϕ é sobrejetivo então $\phi(1)$ é a unidade de B se B for não nulo.
9. ϕ é um isomorfismo se e somente se ϕ é sobrejetivo e $N(\phi) = \{r \in A \mid \phi(r) = 0\} = \{0\}$.
10. Se ϕ é um isomorfismo de A sobre B então ϕ^{-1} é um isomorfismo de B sobre A.

Demonstração. Para item (1). Aplicando ϕ à expressão $0 + 0 = 0$ teremos $\phi(0 + 0) = \phi(0)$ e assim

$$\phi(0) + \phi(0) = \phi(0)$$

Segue daí que

$$2\phi(0) - \phi(0) = 0$$

Então,

$$\phi(0) = 0$$

Para o item (2). Aplique ϕ à expressão $r + (-r) = 0$ teremos que

$$\phi(r) + \phi(-r) = \phi(0) = 0.$$

Somando de ambos os lados $-\phi(r)$ temos $\phi(-r) = -\phi(r)$.
No item (3). Pela definição de homomorfismo.

$$\begin{aligned}\phi(nr) = \phi(r + r + r + \ldots + r) &= \phi(r) + \phi(r) + \phi(r) \ldots + \phi(r) \\ &= n\phi(r).\end{aligned}$$

E ainda,

$$\begin{aligned}\phi(r^n) = \phi(rr \ldots r) &= \phi(r)\phi(r) \ldots \phi(r) \\ &= \phi(r)^n.\end{aligned}$$

□

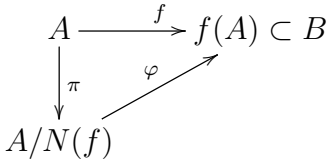
É importante lembrar que anéis isomorfos têm propriedades idênticas, e eles diferem apenas na apresentação de seus elementos. O essencial é que o isomorfismo preserva todas as propriedades algébricas entre tais anéis.

Chamaremos o teorema abaixo de *O teorema fundamental dos homomorfismos*

Teorema 2.10: Dado um homomorfismo $f\colon A \longrightarrow B$, então existe um isomorfismo de anéis

$\varphi\colon A/N(f) \longrightarrow f(A)$ que satisfaz $f = \varphi \circ \pi$, no qual $\pi\colon A \longrightarrow A/N(f)$ é o homomorfismo canônico.

Representamos esse resultado pelo esquema abaixo.



$$A/N(f) \approx f(A)$$

Demonstração. Seja a função $\varphi\colon A/N(f) \longrightarrow f(A)$. Definiremos $\varphi(\bar{a}) = f(a)$ para todo $\bar{a} = a + N(f) \in A/N(f)$. Vamos provar que função φ está bem definida. Suponhamos, que $\bar{a} = \bar{b}$. Como $N(f)$ é um ideal de A. Isto é, seja $x \in A$ é $a \in N(f)$ então

$$f(a \cdot x) = f(a) \cdot f(x) = 0_B \cdot f(x) = 0_B$$

e

$$f(x \cdot a) = f(x) \cdot f(a) = f(x) \cdot 0_B = 0_B,$$

ou seja, $a \cdot x \in N(f)$ e $x \cdot a \in N(f)$. Assim $N(f)$ é um ideal de A. Logo , $a + N(f) = b + N(f) \Rightarrow a - b \in N(f)$ e, portanto, $f(a - b) = 0_B$. Então,

$$f(a) - f(b) = f(a - b) = 0_B \Rightarrow f(a) = f(b)$$

Pela definição de φ, temos, $\varphi(\bar{a}) = \varphi(\bar{b})$

Agora, Vamos mostrar que φ é um homomorfismo. Para isso, basta verificar que φ satisfaz os axiomas de homomorfismo.

Se $\bar{a}, \bar{b}$ $A/N(f)$, temos:

$$\begin{aligned}\varphi(\bar{a} + \bar{b}) &= f(a+b) \text{ pela definição de } \varphi \\ &= f(a) + f(b) \text{ pois } f \text{ é um homomorfismo} \\ &= \varphi(a) + \varphi(b) \text{ pela definição de } \varphi.\end{aligned}$$

$$\begin{aligned}\varphi(\bar{a} \cdot \bar{b}) &= f(a \cdot b) \text{ pela definição de } \varphi \\ &= f(a) \cdot f(b) \text{ pois } f \text{ é um homomorfismo} \\ &= \varphi(a) \cdot \varphi(b) \text{ pela definição de } \varphi.\end{aligned}$$

$$\begin{aligned}\varphi(\bar{1_A}) &= f(1_A) \text{ pela definição de } \varphi \\ &= 1_B \text{ pois } f \text{ é um homomorfismo.}\end{aligned}$$

Portanto,a função φ é um homomorfismo entre os anéis $A/N(f)$ em $f(A)$

Provaremos , agora, que φ é uma função bijetora. Começaremos provando que ela é injetora. Se $\varphi(\bar{a}) = \varphi(\bar{b})$ temos $f(a) = f(b)$. Segue daí que

$$f(a) - f(b) = 0_B \Rightarrow f(a-b) = 0_B$$

isso significa que $a - b \in N(f)$, ou seja, $\bar{a} = \bar{b}$. Pois, $\bar{a} \in A/N(f)$.

Para mostrar que φ ser sobrejetora, seja $y \in f(A)$ arbitrário, então existe $a \in A$ tal que $y = f(a)$ e, como, $\varphi(\bar{a}) = f(a)$ segue daí que $y = \varphi(\bar{a})$.

Portanto a função φ: $A/N(f) \longrightarrow f(A)$, definida por $\varphi(\bar{a}) = f(a)$, é um homomorfismo bijetor, ou seja, é um isomorfismo e, logo, temos $A/N(f) \approx f(A)$

□

Uma consequência imediata do Teorema do Homomorfismo é:

Corolário 2.1: Se $f : A \to B$ é um homomorfismo sobrejetor, então $A/N(f)$ e B são anéis isomorfos, isto é, $A/N(f) \approx B$.

Demonstração. Como f é sobrejetora, temos $f(A) = B$ e, pelo teorema do homomorfismo, temos $A/N(f) \approx f(A)$. Portanto, $A/N(f) \approx B$.

□

Corolário 2.2: Se $n \in \mathbb{Z}, n > 0$. Então os anéis $\mathbb{Z}/n\mathbb{Z}$ e Z_n são isomorfos, isto é, $\mathbb{Z}/n\mathbb{Z} \approx Z_n$

2.2 Corpos

Definição 2.15: Um elemento do anel A será dito *invertível*, se existir um elemento $b \in A$ tal que $a \cdot b = 1$. Um tal elemento b será chamado de *inverso* de a, e denotado por a^{-1} ou $\frac{1}{a}$.

Se um domínio de Integridade $(A, +, \cdot)$ satisfaz a propriedade: $\forall x \in A, x \neq 0, x$ é invertível, dizemos que $(A, +, \cdot)$ é um corpo. Como exemplos de corpos, temos os conjuntos $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, mas $\mathbb{Z}$ não é um corpo, pois os únicos inteiros que têm inversos são 1 e -1.

Usaremos a notação ab^{-1} para indicar a dividido por b. Então podemos dizer que um corpo é um conjunto o qual é fechado em relação à adição, subtração, multiplicação e divisão para elemento não nulos.

Definição 2.16: Um subconjunto F de um corpo K que, com as operações de adição e de multiplicação de K, é ainda um corpo, será chamado de subcorpo de K.

Exemplo 2.2.1: Temos $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, sendo $\mathbb{R}$ um subcorpo de $\mathbb{C}$ e $\mathbb{Q}$ subcorpo de $\mathbb{R}$, logo $\mathbb{Q}$ também é subcorpo de $\mathbb{C}$.

Temos que todo corpo é um domínio, mas a recíproca é falsa. Basta pensarmos em $\mathbb{Z}_6$.

Existem diversas propriedades que são consequências da definição de anel e de corpo. Veremos algumas no próximo capítulo.

3

Polinômios com Coeficientes em Anéis

Durante todo o restante do trabalho, salvo menções específicas, sempre que mencionarmos que um conjunto A é anel, deve ficar subtendido que é um domínio de integridade que possui a relação de ordem, $\leq$. A teoria deste capítulo estará em conformidade com a referência [10].

Seja o anel A e x um elemento não pertence ao anel A. Esse elemento x será chamado de uma indeterminada sobre A. Para essa indeterminada temos os símbolos x^i, para $i = 0$ ou i natural, que representa as potências $x^0 = 1$, $x^1 = x$ e $x^n = x \cdot x \ldots x$ (n vezes).

Definição 3.1: Um polinômio $f(x)$ com coeficientes em A é uma expressão formal do tipo $f(x) = a_0 + a_1x + \ldots + a_nx^n = \sum_{j=0}^{n} a_jx^j$ em que $n \in \mathbb{N} \cup 0, a_i \in A$, para $0 \leq i \leq n$.

Os coeficientes do polinômio $f(x)$ serão os elementos a_i para $0 \leq i \leq n$, e os termos a_ix^i tais que $a_i \neq 0$, são ditos monômios de grau i do polinômio $f(x)$. E o termo constante será o coeficiente a_0.

O conjunto de todos os polinômios com coeficientes em A será denotado $A[x]$. Isto é, $A[x] = \{a_0 + a_1x + \ldots + a_nx^n; a_i \in A, 0 \leq i \leq n, n \in \mathbb{N}\}$.

Ainda sobre o polinômio $f(x)$, há duas nomeclaturas usuais: polinômio constante $f(x) = a_0$, com $a_0 \in A$ e polinômio, nulo, $f(x) = 0$ que poderá ser escrito na forma $f(x) = 0 + 0x + \ldots + 0x^n$, qualquer que seja $n \in \mathbb{N} \cup \{0\}$.

Exemplo 3.0.1: São polinômios em $\mathbb{R}[x]$ e em $\mathbb{Z}[x]$, respectivamente, $f(x) = \frac{4}{3} - \sqrt{11}x + x^2$ e $h(x) = 5 + 3x + 10x^2 - 2x^3$.

Nos dois polinômios do Exemplo (3.0.1) é possível fazermos uma comparação entre os seus coeficientes. Observe que em $f(x)$ não há coeficiente de grau 3, mas podemos tomar $f(x) = \frac{4}{3} - \sqrt{11}x + x^2 + 0x^3$. Note que apenas acrescentamos o termo $0x^3$ em $f(x)$.

Com as convenções feitas acima o polinômio $f(x) = a_0 + a_1x + \ldots + a_nx^n \in A[x]$ pode ser escrito como $f(x) = a_0 + a_1x + \ldots + a_nx^n + 0x^{n+1} + 0x^{n+2} + \ldots + 0x^m$ para

todo número natural $m > n$.

Dois polinômios $f(x) = a_0 + a_1x + \ldots + a_nx^n$ e $g(x) = c_0 + c_1x + \ldots + c_nx^n$ em $A[x]$ são iguais se, e somente se, $a_i = c_i$, para $0 \leq i \leq n$. Então escrevemos $f(x) = g(x)$.

Exemplo 3.0.2: Os polinômios $f(x) = 10 - \sqrt{2}x + x^2 + -9x^3$ e $g(x) = -9x^3 - \sqrt{2}x + 10 + x^2$ em $\mathbb{R}[x]$ são iguais e os polinômios $h(x) = 9 - 5x + x^2 - 9x^3$ e $t(x) = 9 - 5x + 3x^2 - 9x^3$ ambos em $\mathbb{Z}[x]$, são diferentes. Nos dois casos, basta observamos os coeficientes a_i das i-ésimas potências x^i.

Definição 3.2: Em todo polinômio, não identicamente nulo, algum coeficiente deve ser diferente de zero, então há um maior índice n tal que $a_n \neq 0$. Esse índice será o *grau* do polinômio $f(x)$.

Denotamos esse grau por $gr(f(x))$. E o a_n correspondente será chamado de c*oeficiente líder* de $f(x)$. Para $a_n = 1$ chamaremos esses polinômios de *mônicos*. E não definiremos o grau do polinômio nulo: $f(x) = 0$. O polinômio constante $h(x) = k$ para $k \in A$ tem $gr(f(x)) = 0$.

No conjunto $A[x]$, a partir das operações de adição e multiplicação de A, podemos definir operações de adição e multiplicação de polinômios.

Sejam $h(x) = \sum_{j=0}^{n} a_jx^j$ e $u(x) = \sum_{j=0}^{n} b_jx^j$ em $A[x]$. Definimos a operação de adição desses polinômios como segue

$$h(x) + u(x) = \sum_{j=0}^{n} c_jx^j \text{ em que } c_j = a_j + b_j, \text{ para } 0 \leq j \leq n.$$

E para a multiplicação definimos $h(x) = \sum_{j=0}^{n} a_jx^j$ e $u(x) = \sum_{j=0}^{m} b_jx^j$ em $A[x]$, então $h(x) \cdot u(x) = \sum_{j=0}^{n+m} c_jx^j$, no qual

$$\begin{aligned}
c_0 &= a_0 \cdot b_0 \\
c_1 &= a_0 \cdot b_1 + a_1 \cdot b_0 \\
c_2 &= a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0 \\
&\vdots \\
c_j &= a_0 \cdot b_j + a_1 \cdot b_{j-1} + \ldots + a_j \cdot b_0 = \sum_{\lambda+\mu=j} a_\lambda \cdot b_\mu \\
&\vdots \\
c_{n+m} &= a_n \cdot b_m
\end{aligned}$$

E o resultado da multiplicação de dois polinômios é chamado de produto. Segue da definição de multiplicação que, para quaisquer j, $k \in \mathbb{N} \cup \{0\}$, vale a identidade: $x^j \cdot x^k = x^{j+k}$.

Proposição 3.1: Como consequência das propriedades da adição e da multiplicação do anel A, temos que a adição e multiplicação em $A[x]$ satisfazem as propriedades associativa, comutativa, distributiva, existência de elemento neutro aditivo, existência

de simétrico, existência do elemento neutro multplicativo, em $A[x]$, para quaisquer polinômios $f(x)$, $g(x)$ e $h(x)$.

Faremos a demonstração da associatividade da multiplicação e da comutatividade da adição, e deixaremos para o leitor a verificação das outras.

Demonstração. Sejam dados $f(x) = \sum_{j=0}^{n} a_j x^j$, $g(x) = \sum_{j=0}^{m} b_j x^j$ e $h(x) = \sum_{j=0}^{l} c_j x^j$ polinômios em $A[x]$. Iniciaremos com a Associatividade da Multiplicação:

$$(f(x)\cdot g(x))\cdot h(x) = \left(\sum_{j=0}^{n} a_j x^j \cdot \sum_{j=0}^{m} b_j x^j\right)\cdot \sum_{j=0}^{l} c_j x^j \tag{3.1}$$

$$= \sum_{j=0}^{n+m}\left(\sum_{j=\mu+\lambda} a_\mu \cdot b_\lambda\right) x^j \cdot \sum_{j=0}^{l} c_j x^j \tag{3.2}$$

$$= \sum_{j=0}^{n+m+l}\left(\sum_{j=\mu+\lambda+\alpha} a_\mu \cdot b_\lambda \cdot c_\alpha\right) x^j \tag{3.3}$$

$$= \sum_{j=0}^{n+m+l}\left(\sum_{j=\mu+\lambda+\alpha} a_\mu \cdot (b_\lambda \cdot c_\alpha)\right) x^j \tag{3.4}$$

$$= \sum_{j=0}^{n} a_j x^j \cdot \sum_{j=0}^{m+l}\left(\sum_{j=\lambda+\alpha} b_\lambda \cdot c_\alpha\right) x^j \tag{3.5}$$

$$= \sum_{j=0}^{n} a_j x^j \cdot \left(\sum_{j=0}^{m} b_j x^j \cdot \sum_{j=0}^{l} c_j x^j\right) \tag{3.6}$$

$$= f(x)\cdot(g(x)\cdot h(x)) \tag{3.7}$$

no qual em (3.2), (3.3), (3.5) e (3.6) usamos a definição de multiplicação em $A[x]$ e em (3.4) usamos a associatividade da multiplicação em A.

Para comutatividade da adição temos:
Sem perda de generalidade, suponhamos que $n = m$ e reescrevendo os polinômios $f(x)$, $g(x)$ com as mesmas potências de x. Obtemos,

$$f(x) + g(x) = \sum_{j=0}^{n} a_j x^j + \sum_{j=0}^{n} b_j x^j \tag{3.8}$$

$$= \sum_{j=0}^{n} (a_j + b_j) x^j \tag{3.9}$$

$$= \sum_{j=0}^{n} (b_j + a_j) x^j \tag{3.10}$$

$$= \sum_{j=0}^{n} b_j x^j + \sum_{j=0}^{n} a_j x^j \tag{3.11}$$

$$= g(x) + f(x) \tag{3.12}$$

no qual em (3.8) e (3.10), usamos a definição da adição em $A[x]$. E em (3.9) usamos a comutatividade da adição em A. □

Considerando as propriedade das operações em $A[x]$, expressadas na Proposição (3.1), temos que $A[x]$ é um anel.

Note que se $f(x)$ e $g(x)$ são polinômios não nulos em $A[x]$, com coeficientes líderes a_n e b_m respectivamente, então o polinômio $f(x) \cdot g(x)$ tem coeficientes líder $a_n \cdot b_m$.

Além disso se $f(x)$ e $g(x)$ são polinômios não nulos então o produto desses polinômios será diferente zero. Assim, $A[x]$ é um domínio de integridade. E também,

$$gr(f(x) \cdot g(x)) = gr(f(x)) + gr(g(x)).$$

Chamaremos a propriedade acima de *propriedade multiplicativa do grau.*

3.1 Raízes e irredutibilidade

Neste capítulo apresentaremos conceitos sobre decomposição de um polinômio em fatores irredutíveis, relação entre a existência de raízes e a existência de fatores de grau um na decomposição do polinômio e citaremos o teorema fundamental da álgebra em $\mathbb{R}$ e $\mathbb{C}$. Salva menção contrária, A é um *Domínio de Integridade*. A teoria deste capítulo estará em conformidade com [7], [4], [10] e [18]

Dado $f(x) \in A[x]$ e $a \in A$ com A anel, podemos definir o valor de $f(x)$ em a o que denotamos por $f(a)$, da seguinte maneira: Se $f(x) = a_n x^n + \ldots + a_1 x + a_0$; $f(a) = a_n a^n + \ldots + a_1 a + a_0$.

Exemplo 3.1.1: Dado $f(x) \in \mathbb{Z}[x]$ e $a \in \mathbb{Z}$ tal que $f(x) = x^5 + 2x - 3$ então o valor de $f(2) = 2^5 + 2(2) - 3 = 33$.

Definição 3.3: Sejam A um anel e um polinômio $f(x) \in A[x]$. Dizemos que $\alpha \in A$ é uma *raiz* ou um *zero* de $f(x)$ em A se $f(\alpha) = 0$.

Exemplo 3.1.2: Seja $f(x) = x^4 - x^3 - x + 1 \in \mathbb{Z}[x]$, temos que $\alpha = 1$ é uma raiz de $f(x)$ em $\mathbb{Z}$, pois

$$f(1) = 1^4 - 1^3 - 1 + 1 = 0$$

A divisão em $A[x]$, conhecida como *divisão euclidiana*, será apresentada no teorema a seguir e deixaremos a demonstração para o leitor que poderá ser feita inicialmente por indução.

Teorema 3.1: Sejam A um anel e $f(x), g(x) \in A[x]$ dois polinômios, com $g(x)$ não-nulo e coeficiente líder invertível em A. Então existem polinômios $q(x), r(x) \in A[x]$, unicamente determinados, tais que

$$f(x) = q(x)g(x) + r(x) \text{ com } gr(r(x)) < gr(g(x)) \text{ ou } r(x) = 0$$

Exemplo 3.1.3: Efetuando a divisão euclidiana de $f(x) = 4x^4 + 2x^3 + 6x^2 + 4x + 5$ por $g(x) = 3x^2 + 2$ em $\mathbb{Z}_7[x]$, obtemos

$$f(x) = 4x^4 + 2x^3 + 6x^2 + 4x + 5 = (6x^2 + 3x + 5)(3x^2 + 2) - 2x + 2$$

Observe que no Teorema 3.1 é necessário que o coeficiente líder de $g(x)$ seja inversível. Por isso em muitas ocasiões trabalharemos em $K[x]$ com K, corpo, assim não precisaremos nos preocupar com esse detalhe. Uma outra observação a fazer é que, embora $\mathbb{Z}$ não seja corpo, a existência de um algoritmo de divisão em $\mathbb{Z}$ nos garante a existência desse algoritmo em $\mathbb{Z}[x]$ sem a necessidade da hipótese sobre o coeficiente líder de $g(x)$.

Exemplo 3.1.4: Sejam $f(x) = 4x^5 - x^2 + x - 4$ e $g(x) = x^2 - x + 1$, com $f(x)$, $g(x) \in \mathbb{Z}[x]$ satisfazendo a hipótese do Teorema 3.1, temos que $f(x) = g(x)q(x)+r(x)$, no qual $q(x) = 4x^3 + 4x^2 - 5$ e $r(x) = -4x + 1$.

Definição 3.4: Sejam A um anel e $f(x)$, $g(x) \in A[x]$ dois polinômios com $g(x)$ não-nulo. Dizemos que o polinômio $g(x)$ *divide* o polinômio $f(x)$ em $A[x]$, caso haja um polinômio $q(x) \in A[x]$ tal que

$$f(x) = q(x)g(x),$$

e denotamos isso por $g(x) \mid f(x)$. Nesse caso, também dizemos que $g(x)$ é um *divisor* de $f(x)$, ou que $g(x)$ é um *fator* de $f(x)$, ou ainda, que $f(x)$ é um *múltiplo* de $g(x)$ em $A[x]$.

Quando $f(x)$ se expressa como um produto de polinômios,

$$f(x) = p_1(x)p_2(x)\dots p_n(x),$$

dizemos que esse produto é uma *fatoração* de $f(x)$ e, portanto, cada polinômio $p_k(x)$ é um fator de $f(x)$.

Exemplo 3.1.5: Seja $f(x) = x^5 + 3x^3 + 4x^2 + 2x + 3 \in \mathbb{Z}_5[x]$. Uma fatoração de $f(x)$ sobre $\mathbb{Z}_5$ é

$$f(x) = (x^3 + x + 4)(x^2 + 2)$$

Veremos a seguir algumas propriedades da divisão, demonstraremos a primeira e as demais seguem raciocínio análogo.

Proposição 3.2: Sejam A um anel e os polinômios $f(x), g(x)$, e $h(x) \in A[x]$.

D1) Se $h(x) \mid f(x)$ e $h(x) \mid g(x)$ então $h(x) \mid (f(x) + g(x))$ e $h(x) \mid (f(x) - g(x))$.

D2) Se $h(x) \mid f(x)$, então $h(x) \mid f(x)g(x)$.

D3) Se $h(x) \mid f(x)$, $h(x) \mid g(x)$ e $p(x)$, $q(x) \in A[x]$, então $h(x) \mid (p(x)f(x) + q(x)g(x))$.

D4) Se $h(x) \mid f(x)$ e $f(x) \mid g(x)$, então $h(x) \mid g(x)$.

Demonstração. Como $h(x) \mid f(x)$ então existe $q(x) \in A[x]$ tal que $f(x) = q(x)h(x)$. Analogamente, com $h(x) \mid g(x)$ existe $p(x) \in A[x]$ tal que $g(x) = p(x)h(x)$ Logo,

$$f(x) + g(x) = q(x)h(x) + p(x)h(x) = (q(x) + p(x))h(x).$$

Como $q(x) + p(x) \in A[x]$, temos que $h(x)$ divide $f(x) + g(x)$.
Analogamente,

$$f(x) - g(x) = q(x)h(x) - p(x)h(x) = (q(x) - p(x))h(x).$$

Do mesmo modo que anteriormente $h(x)$ divide $f(x) - g(x)$.

□

Proposição 3.3: Sejam A um anel, $f(x) \in A[x]$ e $a \in A$, então o resto na divisão euclidiana de $f(x)$ por $x - a$ é $f(a)$.

Demonstração. Sabemos, pelo algoritmo de divisão de polinômios que, $\exists q(x), r(x) \in A[x]$ tal que

$$f(x) = q(x)(x - a) + r(x) \text{ com } gr(r(x)) < gr(x - a) \text{ ou } r(x) = 0.$$

Como $gr(r(x)) < gr(x-a) = 1$, segue daí que $gr(r(x)) = 0$, então $r(x)$ é constante, digamos $r(x) = \alpha$. Calculando o valor de $f(x)$ em a, temos

$$f(a) = q(a)(a - a) + r(a) = r(a) = \alpha$$

□

Segue da Proposição (3.3) um importante corolário, conhecido também como *teorema da raiz*, *teste da raiz* ou *propriedade do fator linear*.

Corolário 3.1: Sejam $f(x)$ um polinômio com coeficientes no anel A e $a \in A$. Temos que $x - a$ divide $f(x)$ se, e somente se, a for raiz de $f(x)$.

Demonstração. Suponhamos que a é raiz de $f(x)$, assim, da igualdade $f(x) = q(x)(x - a) + r(x)$ com $gr(r(x)) < gr(x - a) = 1$ ou $r(x) = 0$. Temos,

$$0 = f(a) = q(a)(a - a) + r(a) = r(a),$$

mostrando que $f(x) = q(x)(x - a)$.
Reciprocamente, suponhamos $x - a$ divida $f(x)$. Logo, existe um $q(x) \in A[x]$ tal que $f(x) = q(x)(x - a)$. Portanto,

$$f(a) = q(a)(a - a) = 0.$$

□

Exemplo 3.1.6: Seja $f(x) = x^3 + 5x - 5 \in \mathbb{R}[x]$. Então, o resto da divisão de $f(x)$ por $(x - 2)$ e $(x + 2)$ respectivamente é:

$$f(2) = 13 \text{ e } f(-2) = -23$$

Exemplo 3.1.7: Seja $f(x) = 4x^4 + 5x^2 - 7x + 2 \in \mathbb{Q}[x]$. Dado que $\frac{1}{2}$ é raiz de $f(x)$. Então pelo Corolário (3.1) temos

$$f(x) = (x - \tfrac{1}{2})q(x) \text{ em que } q(x) = 4x^3 + 2x^2 + 6x - 4.$$

Um importante método para determinarmos o quociente e o resto de uma divisão de polinômios é o chamado de *algoritmo de Briot-Ruffini*. Considerando a importância da divisão de um polinômio por polinômios da forma $x-a$, segue esse algoritmo.

Sejam um anel A, $f(x) \in A[x]$ e $\alpha \in A$. Pela divisão euclidiana, existe um polinômio $q(x) \in A[x]$ tal que

$$f(x) = (x - \alpha)q(x) + r \text{ tal que } r = f(\alpha).$$

Note que se o $gr(f(x)) = n$ então $gr(q(x)) = n - 1$. E tomando

$$f(x) = a_0 + a_1x + \ldots + a_nx^n$$

encontraremos os coeficientes $b_0, b_1, \ldots, b_{n-1} \in A$ tais que

$$q(x) = b_0 + b_1x + \ldots + b_{n-1}x^{n-1}$$

Assim, substituindo em $f(x) = (x - a)q(x) + r$ obtemos,

$$\begin{aligned} f(x) &= (x - \alpha)(b_0 + b_1x + \ldots + b_{n-1}x^{n-1}) + r \\ &= (r - \alpha b_0) + (b_0 - \alpha b_1)x + \ldots + (b_{n-2} - \alpha b_{n-1})x^{n-1} + b_{n-1}x^n \end{aligned}$$

comparando com os coeficientes de $f(x)$ e determinando os coeficientes b_0,$b_1, \ldots, b_{n-1}$ em função de a_0,$a_1, \ldots, a_{n-1}$ e do escalar α, obtemos as igualdades:

$$\begin{aligned} b_{n-1} &= a_n \\ b_{n-2} &= b_{n-1}\alpha + a_{n-1} \\ b_{n-3} &= b_{n-2}\alpha + a_{n-2} \\ &\vdots \\ b_1 &= b_2\alpha + a_2 \\ b_0 &= b_1\alpha + a_1 \\ r &= b_0\alpha + a_0 \end{aligned}$$

Desta forma concluímos o *algoritmo de Briot-Ruffini*. Vejamos um exemplo:

Exemplo 3.1.8: Vamos determinar o quociente e o resto da divisão euclidiana em $\mathbb{Q}[x]$ de $f(x) = x^3 - 2x^2 + 3$ por $x + 3$, usando o algoritmo de Briot-Ruffini. Nesse

caso, $\alpha = -3$, $gr(f(x)) = 3$ e $gr(q(x)) = 2$.

$$\begin{aligned} b_2 &= 1 \\ b_1 &= (1)(-3) - 2 = -5 \\ b_0 &= (-5)(-3) + 0 = 15 \\ r &= (15)(-3) + 3 = -42 \end{aligned}$$

Logo, $r = 42$, -3 não é raiz de $f(x)$, $q(x) = x^2 - 5x + 15$ e $f(x) = (x^2 - 5x + 15)(x + 3) - 42$.

Definição 3.5: Sejam $f(x) \in A[x]$ e $a \in A$. Dizemos que a é um *raiz de multiplicidade* m de $f(x)$, em que $m \geq 1$, se $(x - a)^m$ divide $f(x)$ e $(x - a)^{m+1}$ não divide $f(x)$. Se $m \geq 2$, dizemos que a é uma raiz múltipla de $f(x)$.

O exemplo abaixo será um complementação do Exemplo (3.1.7).

Exemplo 3.1.9: Seja $f(x) = 4x^4 + 5x^2 - 7x + 2 \in \mathbb{Q}[x]$. Já sabemos que $\dfrac{1}{2}$ é raiz de $f(x)$. Vamos mostrar que a maior potência de $x - \frac{1}{2}$ que divide $f(x)$, é 2 e portanto a multiplicidade da raiz $\dfrac{1}{2}$ é 2.

Sabemos que

$$f(x) = (x - \tfrac{1}{2})(4x^3 + 2x^2 + 6x - 4).$$

E se continuarmos com o algoritmo de Briot-Ruffini fazendo a divisão de $q(x) = 4x^3 + 2x^2 + 6x - 4$ por $x - \frac{1}{2}$ obteremos

$$q(x) = (x - \tfrac{1}{2})(4x^2 + 4x + 8).$$

Assim,

$$\begin{aligned} f(x) &= (x - \frac{1}{2})(4x^3 + 2x^2 + 6x - 4) \\ &= (x - \frac{1}{2})(x - \frac{1}{2})(4x^2 + 4x + 8) \\ &= (x - \frac{1}{2})^2(4x^2 + 4x + 8). \end{aligned}$$

Portanto $\frac{1}{2}$ é uma raiz de $f(x)$ de multiplicidade 2, pois se continuarmos com o processo anterior, ou seja, dividindo $h(x) = 4x^2 + 4x + 8$ por $x - \dfrac{1}{2}$, encontraremos,

$$f(x) = (x - \tfrac{1}{2})^3(4x + 6) + 11.$$

Este exemplo ilustra uma aplicação interessante do algoritmo de Briot-Ruffini, que será a ferramenta para fazer as divisões sucessivas de $f(x)$ por $(x - \alpha)$.

Considere agora A um subanel de $\mathbb{C}$ e $\alpha \in A$. A função $\varphi : A[x] \longrightarrow A[x]$ definida por $\varphi(g(x)) = g(x - \alpha)$ é uma bijeção, pois $\psi : A[x] \longrightarrow A[x]$ definida por

$\psi(g(x)) = g(x+\alpha)$ tem a propriedade de $\varphi \circ \psi = I$ e $\psi \circ \varphi = I$. Portanto, para cada $f(x) \in A[x]$ existe um único polinômio $g(x) \in A[x]$ tal que $f(x) = \varphi(g(x)) = g(x-\alpha)$. Isto é equivalente a dizer que cada polinômio $f(x)$ com coeficientes em A pode ser escrito, de uma única maneira, como um polinômio com coeficientes em A e potências de $x - \alpha$.

Dado $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in A[x]$, com $a_n \neq 0$ e $n \geq 1$, podemos expressá-lo como um polinômio em potências de $x - \alpha$ pela divisão euclidiana de $f(x)$ por $x - \alpha$. De fato,

$$f(x) = (x-\alpha)q_1(x) + r_0, \text{ no qual } r_0 \in A \text{ e } gr(q_1(x)) = n-1.$$

Pela divisão euclidiana de $q_1(x)$ por $x - \alpha$, temos

$$q_1(x) = (x-\alpha)q_2(x) + r_1, \text{ no qual } r_1 \in A \text{ e } gr(q_2(x)) = n-2.$$

Sucessivamente, fazemos a divisão de $q_j(x)$ por $x - \alpha$, obtendo $q_{j+1}(x) \in A[x]$ e $r_j \in A$, para $j = 0, \ldots, n-1$, com $gr(q_{j+1}(x)) = n - j - 1$ e $q_0(x) = f(x)$.

Fazendo $r_n = q_n(x) \in A$ e substituindo, sucessivamente, uma equação na outra, obtemos

$$f(x) = r_0 + r_1(x-\alpha) + \ldots + r_{n-1}(x-\alpha)^{n-1} + r_n(x-\alpha)^n,$$

em que $r_n = a_n$ é o coeficiente líder de $f(x)$.

Exemplo 3.1.10: Seja $f(x) = 2x^5 + 3x^4 - x^3 + x^2 - 4 \in \mathbb{Z}[x]$. Vamos escrevê-lo em potências crescentes de $x + 1$: Fazendo do mesmo modo que no Exemplo (3.1.9) temos

$$f(x) = -1 - 7(x+1) + 2(x+1)^2 + 7(x+1)^3 - 7(x+1)^4 + 2(x+1)^5.$$

A próxima proposição dará a quantidade máxima de raízes de um polinômio.

Proposição 3.4: Sejam A um domínio de integridade e $f(x) \in A[x]$ um polinômio de grau n. Então, $f(x)$ tem, no máximo, n raízes em A, sendo que cada raiz é contada um número de vezes igual à sua multiplicidade.

Demonstração. Faremos por indução em $n = gr(f(x))$. Se $n = 0$, então $f(x) = a \neq 0$ não tem raízes em A e o resultado é valido. Seja $n \geq 0$. Suponhamos que vale para polinômios de grau n e seja $f(x)$ um polinômio com $gr(f(x)) = n + 1$. Se $f(x)$ não tem raízes em A, nada há a demonstrar. Digamos que $f(x)$ tenha uma raiz $\beta \in A$. Pelo Corolário 3.1, $x - \beta$ divide $f(x)$ em $A[x]$, logo existe $q(x) \in A[x]$ tal que

$$f(x) = q(x)(x-\beta), \text{ com } gr(q(x)) = n.$$

Por hipótese de indução, $q(x)$ tem no máximo n raízes em A. Mostramos que se $\alpha \in A$ é raiz de $f(x)$ então ou $\alpha = \beta$ ou $q(\alpha) = 0$. De fato, se $\alpha \in A$ é raiz de $f(x)$ então

$$0 = f(\alpha) = q(\alpha)(\alpha - \beta)$$
$$\Leftrightarrow q(\alpha) = 0 \text{ ou } \alpha - \beta = 0$$
$$\Leftrightarrow \alpha \text{ é raiz de } q(x) \text{ ou } \alpha = \beta,$$

Logo, $f(x)$ tem no máximo $n+1$ raízes em A. □

3.2 O Teorema Fundamental da Álgebra

Ao longo deste trabalho temos falado sobre $\mathbb{C}$, o conjunto dos números complexos. Aqui somente precisamos da noção intuitiva do leitor, no qual $\mathbb{C}$ é o conjunto de elementos $z = a + bi$, no qual $i = \sqrt{-1}$ e $a, b \in \mathbb{R}$. Na Seção 4.2 do Capítulo 4 apresentaremos esse corpo com maiores detalhes.

Um corpo K é algebricamente fechado quando todo polinômio não constante com coeficientes em K tem uma raiz em K. Note que se um corpo K é algebricamente fechado, então todo $f(x) \in K[x]$ não nulo tem todas as raízes em K. *O Teorema Fundamental da Álgebra* diz que, $\mathbb{C}$ é algebricamente fechado. A importância da propriedade abaixo é que ela precede o teorema principal desta seção.

Proposição 3.5: Sejam K um corpo algebricamente fechado e $f(x)$ em $K[x]$, $gr(f(x)) = n \geq 1$. Então, existem $\alpha_1, \ldots \alpha_n \in A$, não necessariamente distintos, e $a \in K \setminus \{0\}$ tais que

$$f(x) = a(x - \alpha_1) \ldots (x - \alpha_n).$$

Demonstração. Faremos por indução sobre o grau de $f(x)$. Se $gr(f(x)) = 1$, então $f(x) = ax + b$, para a,$b \in K$ e $a \neq 0$, logo, colocando em evidência a, temos,

$$f(x) = a(x + a^{-1}b).$$

Note que $\alpha_1 = -a^{-1}b$. Seja $n \geq 1$ e suponhamos o resultado válido para polinômios de grau n, provaremos para $n+1$. Tomamos $f(x) \in A[x]$ com $gr(f(x)) = n + 1$. Por hipótese de indução, $f(x)$ tem uma raiz $\alpha \in A$. Pelo Corolário (3.1),

$$f(x) = q(x)(x - \alpha), \text{ para algum }, q(x) \in A[x] \text{ e } gr(q(x)) = n. \tag{3.13}$$

Por hipótese de indução, existem $a, \alpha_1, \ldots \alpha_n \in A$, com $a \neq 0$, tais que

$$q(x) = a(x - \alpha_1) \ldots (x - \alpha_n).$$

Assim, substituindo em (3.13) , temos

$$f(x) = a(x - \alpha_1) \ldots (x - \alpha_n)(x - \alpha).$$

Tomando $\alpha_{n+1} = \alpha$, obtemos o resultado

$$f(x) = a(x - \alpha_1) \dots (x - \alpha_n)(x - \alpha_{n+1}).$$

□

Temos na proposição anterior que a é o coeficiente lider de $f(x)$ e após a reordenação das raízes de $f(x)$, podemos supor que que $\alpha_1, \dots, \alpha_s, 1 \leq s \leq n$, e α_j ocorre com multiplicidade r_j, para cada $j = 1, \dots, s$, dessa forma

$$f(x) = a(x - \alpha_1)^{r_1} \dots (x - \alpha_s)^{r_s} \text{ , no qual, } r_1 + \dots + r_s = n.$$

Portanto, nos corpos algebricamente fechados, todo polinômio de grau $n \geq 1$ tem exatamente n raízes, contadas com as suas multiplicidades. Agora já temos condições de re-enunciarmos o **Teorema Fundamental da Álgebra** a seguir, como consequência do resultado acima.

Teorema 3.2: Todo polinômio $f(x)$ com coeficientes complexos e grau $n \geq 1$, se escreve de uma única maneira, a menos da ordem dos fatores, como

$$f(x) = a(x - \alpha_1)^{r_1} \dots (x - \alpha_s)^{r_s},$$

em que $a \in \mathbb{C} \setminus 0$ é o coeficiente líder de $f(x)$, $\alpha_1 \dots \alpha_s$ são os números complexos distintos e $r_1, \dots, r_s$ são inteiros positivos tais que $r_1 + \dots + r_s = n$.

Antes de vermos um versão do *teorema fundamental da álgebra* para polinômios com coeficientes em $\mathbb{R}$ devemos compreender o conceito de polinômio irredutível.

Definição 3.6: Seja K um corpo. Dizemos que $f(x) \in K[x]$ é um polinômio *irredutível* sobre K, ou *irretutível* em $K[x]$, se seus únicos divisores em $K[x]$ são os polinômios constantes e os múltiplos constantes dele mesmo, ou seja, se $g(x) \in K[x]$ é tal que

$$g(x) \mid f(x) \Rightarrow g(x) = c \text{ ou } g(x) = d \cdot f(x) \text{ no qual } c \text{ e } d \text{ são constantes.}$$

Dizemos que $f(x)$ é *redutível* em $K[x]$, quando ele não for *irredutível*, ou seja, quando existirem polinômios $g(x)$, $h(x) \in K[x]$ tais que

$$f(x) = g(x)h(x) \text{ com } 0 < gr(g(x)) < gr(f(x)) \text{ e } gr(h(x)) < gr(f(x)).$$

Segue abaixo um exemplo interessante sobre essa definição.

Exemplo 3.2.1: Seja K um corpo qualquer. O polinômio $ax + b$, no qual $a, b \in K$ e $a \neq 0$, é irredutível em $K[x]$. Seja $ax + b = f(x)g(x)$, com $f(x)$,$g(x) \in K[x]$ sendo ambos fatores não nulo. Então

$$1 = gr(ax + b) = gr(f(x)) + gr(g(x)).$$

Segue daí que $gr(f(x)) = 0$ e $gr(g(x)) = 1$ ou o contrário. Portanto, $f(x)$ ou $g(x)$ é um polinômio constante não nulo.

Lembrando da importância do polinômio mônico $x - \alpha$, com $\alpha \in K$, observe que esse polinômio é irredutível em $K[x]$.

Como consequência do exemplo acima e que $\mathbb{C}$ é algebricamente fechado temos que em $\mathbb{C}[x]$ um polinômio é irredutível se, e somente se, ele é de grau 1.

Segue ainda duas importantes propriedades que enunciaremos abaixo.

Proposição 3.6: Os polinômios mônicos irredutíveis em $\mathbb{R}[x]$ são da forma $x - a$, com $a \in \mathbb{R}$ ou $x^2 + bx + c$, com $b^2 - 4c < 0$. Todo polinômio $f(x) \in \mathbb{R}[x]$, com $gr(f(x)) > 2$, é redutível em $\mathbb{R}[x]$.

Demonstração. Já sabemos pela Definição 3.6 e Exemplo 3.2.1 que os polinômios $x - a$, no qual $a \in F$, são irredutíveis em qualquer corpo F. Um polinômio de grau 2 com coeficientes em qualquer corpo F é irredutível em $F[x]$ se não tem raízes em F. Logo, $x^2 + bx + c$ é irredutível em $R[x]$ se, e somente se, $x^2 + bx + c$ não tem raízes em $\mathbb{R}$, o que equivale a ter $b^2 - 4c < 0$.

Para demonstrar a última afirmação, seja $f(x)$ um polinômio em $\mathbb{R}[x]$ tal que $gr(f(x)) > 2$ e chamamos $Re(\beta)$ a parte real de β, no qual $\beta \in \mathbb{C}$ é uma raiz de $f(x)$. Temos dois casos a considerar:

1. Se $\beta \in \mathbb{R}$, então $x - \beta$ divide $f(x)$ em $\mathbb{R}[x]$. Logo, $f(x)$ é redutível em $\mathbb{R}[x]$.
2. Se $\beta \in \mathbb{C} \mid \mathbb{R}$, então $\beta \neq \bar{\beta}$ e $\bar{\beta}$ também é raiz de $f(x)$. Logo, $(x - \beta)(x - \bar{\beta})$ divide $f(x)$ em $\mathbb{C}[x]$. Entretanto,

$$(x - \beta)(x - \bar{\beta}) = x^2 - (\beta + \bar{\beta})x + B\bar{\beta} \tag{3.14}$$

$$x^2 - 2Re(\beta)x + |\beta|^2 \in \mathbb{R}[x], \tag{3.15}$$

em 3.15 usamos o fato que $(a + bi) + (a - bi) = 2a$ e $(a + bi) \cdot (a - bi) = a^2 + b^2 = (\sqrt{a^2 + b^2})^2 = |a^2 + b^2|^2$. Logo $x^2 - 2Re(\beta)x + |\beta|^2$ divide $f(x)$ em $\mathbb{R}[x]$. Então, $f(x)$ é redutível em $\mathbb{R}[x]$.

□

Teorema 3.3: Todo polinômio em $K[x]$, de grau maior do que ou igual a 1, é irredutível ou se escreve como produto (finito!) de polinômios irredutíveis.

Demonstração. A demonstração será feita por indução no grau do polinômio. O resultado é verdadeiro para polinômios de grau 1, pois estes são irredutíveis. Seja $f(x)$ um polinômio de grau n, e suponhamos o resultado verdadeiro para polinômios de grau menor do que n. Se $f(x)$ for irredutível não há nada a fazer. Se $f(x)$ for redutível, então existem polinômios $g, h \in K[x]$ tais que

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

com $gr(g(x)) > 0$ e $gr(h(x)) > 0$. Como $gr(f(x)) = gr(g(x)) + gr(h(x))$ e $gr(f(x)) = n$, temos que

$$gr(g(x)) < n \text{ e } gr(h(x)) < n.$$

Pela hipótese de indução, $g(x)$ e $h(x)$ se escrevem como produto de polinômios irredutíveis (ou são irredutíveis). Portanto, $f(x)$ também pode ser escrito como produto de polinômios irredutíveis.

□

Note que a demonstração apresentada é análoga ao resultado correspondente para inteiros.

Já vimos que se A é um domínio, $A[x]$ também será, assim K corpo implica em $K[x]$ domínio. Os domínios que possuem a propriedade dada pelo Teorema 3.3 são ditos domínio de fatoração única. Como consequência do Teorema (3.3) temos o mais próximo do *Teorema Fundamental da Álgebra*, para o corpo $\mathbb{R}$.

Teorema 3.4: Todo polinômio $f(x)$ com coeficientes reais e grau $n \geq 1$, se escreve de uma única maneira, a menos da ordem dos fatores, como

$$f(x) = a(x-\alpha_1)^{r_1} \dots (x-\alpha_s)^{r_t} p_1(x)^{n_1} \dots p_s(x)^{n_s},$$

no qual: $a \in \mathbb{R} \setminus \{0\}$ é o coeficiente líder de $f(x)$; $\alpha_1 \dots \alpha_t$ são as raízes distintas de $f(x)$; $p_j(x) = x^2 + b_j x + c_j$ são polinômios distintos com coeficiente reais tais que $b_j^2 - 4c_j < 0$, para todo $j = 1, \dots, s$; e $r_1, \dots, r_t, n_1, \dots, n_s \in \mathbb{N} \cup 0$ tais que $r_1 + \dots + r_t + 2n_1 + \dots 2n_s = n$.

O *Teorema Fundamental da Álgebra*, que diz $\mathbb{C}$ ser algebricamente fechado contém elementos de análise em sua demonstração e o leitor encontrará em [10], página 192.

3.3 Polinômios com Coeficienes Inteiros

Vejamos agora como determinar as raízes racionais de polinômios com coeficientes inteiros.

Proposição 3.7: Seja $f(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x] \mid \mathbb{Z}$. Seja $\alpha \in \mathbb{Q}, \alpha \neq 0$, uma raiz de $f(x)$. Escrevendo $\alpha = \frac{r}{s}$, com $r, s \in \mathbb{Z} \setminus \{0\}$ e $mdc(r,s) = 1$, então $r \mid a_0$ e $s \mid a_n$.

Demonstração. Como α é uma raiz de $f(x)$. Temos que

$$a_0 + a_1 \tfrac{r}{s} + \dots + a_{n-1} \tfrac{r^{n-1}}{s^{n-1}} + a_n \tfrac{r^n}{s^n} = 0.$$

Multiplicando essa igualdade por s^n, no intuito de eliminarmos os denominadores, obtemos:

$$a_0 s^n + a_1 r s^{n-1} + \dots + a_{n-1} r^{n-1} s + a_n r^n = 0.$$

Ou ainda,

$$a_n r^n = -(a_0 s^n + a_1 r s^{n-1} + \dots + a_{n-1} r^{n-1} s).$$

Como s divide a expressão à direita da igualdade, então $s \mid a_n r^n$ mas $mdc(r,s) = 1$, logo $s \mid a_n$.

Analogamente se escrevermos a equação anterior da seguinte forma, temos;

$$a_0 s^n = -(a_1 r s^{n-1} + \ldots + a_{n-1} r^{n-1} s + a_n r^n).$$

Como r divide a expressão à direita da igualdade, então $r \mid a_0 s^n$ mas $mdc(r,s) = 1$, logo $r \mid a_0$. □

Mesmo $\mathbb{Z}$ não sendo um corpo, temos para $\mathbb{Z}[x]$ a definição de polinômios irredutíveis.

Definição 3.7: Seja $f(x) \in \mathbb{Z}[x]$ um polinômio não nulo, diferente de 1 e diferente de -1. Dizemos que $f(x)$ é *irredutível* em $\mathbb{Z}[x]$ se, e somente se, sempre que $f(x) = g(x)h(x)$, com $g(x),\ h(x) \in \mathbb{Z}[x]$, então $g(x) = \pm 1$ ou $h(x) = \pm 1$. Caso contrário, dizemos que $f(x)$ é *redutível* ou não é *irredutível* em $\mathbb{Z}[x]$.

Exemplo 3.3.1: Os polinômios $f(x) = 6x - 3$ e $g(x) = 9$ não são irredutíveis em $\mathbb{Z}[x]$, pois $f(x) = 3(2x - 1)$ e $g(x) = 3 \cdot 3$. Note que $h(x) = 2x - 1$ e $m(x) = 3$ são irredutíveis em $Z[x]$.

Definição 3.8: Seja $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$. O conteúdo de $f(x)$ é o máximo divisor comum dos seus coeficientes não nulos e denotamos por $cont(f(x))$.

Se $cont(f(x)) = 1$ dizemos que $f(x)$ é primitivo. Note que se $f(x), g(x) \in \mathbb{Z}[x]$ são polinômios primitivos, então $f(x) \cdot g(x)$ também será primitivo. Além disso,

$$cont(f(x) \cdot g(x)) = cont(f(x)) \cdot cont(g(x)).$$

Um resultado importante dessa teoria é que a irredutibilidade em $\mathbb{Q}[x]$ implica na irredutibilidade em $\mathbb{Z}[x]$, algo pouco evidente que será verificado a seguir.

Proposição 3.8: Seja $f(x) \in Z[x] \setminus \mathbb{Z}$ primitivo. Então, $f(x)$ é redutível em $\mathbb{Z}[x]$ se, e somente se, $f(x)$ é redutível em $\mathbb{Q}[x]$.

Demonstração. Se $f(x) \in Z[x] \mid \mathbb{Z}$ é primitivo e redutível em $\mathbb{Z}[x]$, então $f(x) = g(x)h(x)$, no qual

$$g(x), h(x) \in Z[x] \subset \mathbb{Q}[x] \text{ e } 1 \leq gr(g(x)), gr(h(x)) < gr(f(x)).$$

Logo, $f(x)$ é redutível em $\mathbb{Q}[x]$.

Reciprocamente, suponhamos que $f(x) \in \mathbb{Z}[x]$ primitivo e $f(x) = g(x)h(x)$, no qual

$$g(x), h(x) \in \mathbb{Q}[x] \text{ e } 1 \leq gr(g(x)), gr(h(x)) < gr(f(x)).$$

Sejam a, b, c, d inteiros positivos e $g_1(x), h_1(x)$ polinômios primitivo tais que $g(x) = \dfrac{a}{b} g_1(x)$ e $h(x) = \dfrac{c}{d} h_1(x)$. Então,

$$f(x) = \tfrac{a}{b} g_1(x) \cdot \frac{c}{d} h_1(x) = \frac{ac}{bd} g_1(x) h_1(x),$$

é equivalente a $bdf(x) = acg_1(x)h_1(x)$, com $g_1(x)h_1(x)$ primitivo. Logo, $bd = cont(bdf(x)) = cont(ac(g_1(x)h_1(x)) = ac$. Assim, $\frac{ac}{bd} = 1$ e $f(x) = g_1(x)h_1(x)$, com $gr(g_1(x)) = gr(g(x))$ e $gr(h_1(x)) = gr(h(x))$, isso mostra que $f(x)$ é redutível em $\mathbb{Z}[x]$.

□

Exemplo 3.3.2: Vamos mostrar que $f(x) = x^4 + 1$ é irredutível em $\mathbb{Q}[x]$. Como $f(x) \in \mathbb{Z}[x]$ e é primitivo, basta mostrar que $f(x)$ é irredutível em $\mathbb{Z}[x]$. Primeiramente, $f(1) = f(-1) = 2$, logo $f(x)$ não é divisível por um fator do tipo $x - a$, no qual $a \in \mathbb{Z}$. Sejam $a, b, c, d \in \mathbb{Z}$, e suponhamos, por absurdo, que

$$f(x) = (x^2 + ax + b)(x^2 + cx + d) \quad = x^4 + (a + c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd.$$

Comparando os coeficientes, obtemos:

i $a + c = 0$,

ii $ac + b + d = 0$,

iii $ad + bc = 0$,

iv $bd = 1$.

Segue de (iv) que $b = d = 1$ ou $b = d = -1$. Substituindo (i) em (ii), temos que $c^2 = b + d$. Logo, $c^2 = 2$ ou $c^2 = -2$ uma contradição com o fato de $c \in \mathbb{Z}$. Portanto, $f(x) = x^4 + 1$ é irredutível em $\mathbb{Z}[x]$, assim é irredutível em $\mathbb{Q}[x]$.

Encerraremos este capítulo com o critério de *Eisenstein*. Ferdinand Gotthold Max Eisenstein foi um matemático alemão, especialista em teoria dos números e análise matemática.

Teorema 3.5: (*Critério de Eisenstein*) Seja $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$. Suponhamos que exista um número primo p tal que $p \nmid a_n, p \mid a_0, \ldots, p \mid a_{n-1}$ e $p^2 \nmid a_0$. Então $f(x)$ não se escreve como produto de polinômios de grau ≥ 1 em $Z[x]$. Em particular, $f(x)$ é irredutível sobre $\mathbb{Q}[x]$.

Demonstração. Sejam $d = cont(f(x))$ e $f_1(x)$ primitivo tal que $f(x) = df_1(x)$. Como em $p \mid d$, as condições continuam válidas para os coeficientes de $f_1(x)$. Pela Proposição 3.8 é suficiente provar que $f(x)$ é irredutível sobre $\mathbb{Z}$. Podemos supor que $f(x)$ é primitivo. Suponhamos por contradição que,

$$f(x) = g(x) \cdot h(x), g(x), h(x) \in \mathbb{Z}[x] \text{ e } 1 \leq gr(g(x)), gr(h(x)) < gr(f(x)) = n.$$

Seja,

$$g(x) = b_0 + b_1x + \ldots + b_rx^r \in \mathbb{Z}[x], gr(g(x)) = r$$
$$h(x) = c_0 + c_1x + \ldots + c_sx^s \in \mathbb{Z}[x], gr(g(x)) = s$$

Assim $n = r + s$. Temos que $b_0 \cdot c_0 = a_0$ e assim $p \mid b_0$ ou $p \mid c_0$ e como $p^2 \nmid a_0$ segue que p divide apenas um dos inteiros b_0, c_0. Vamos admitir, sem perda de generalidade, que $p \mid b_0$ e $p \nmid c_0$. Agora $a_n = b_r \cdot c_r$ é coeficiente de $x^n = x^{r+s}$ e portanto $p \nmid b_r$ e $p \mid b_0$. Seja b_i o primeiro coeficiente de $g(x)$ tal que $p \nmid b_i$.

Logo,

$$a_i = b_0 \cdot c_i + b_1 \cdot c_{i-1} + \ldots + b_i \cdot c_0$$

e portanto $p \mid b_0, \ldots, b_{i-1}, p \nmid b_i$ e $p \nmid c_0 \Rightarrow p \nmid a_i \Rightarrow i = n$ o que é um absurdo; pois, $1 \leq i \leq r < n$.

□

Exemplo 3.3.3: Mostre que $f(x) = x^8 + 6x^5 - 12x^3 + 18x^2 - 24x - 60$ é irredutível em $\mathbb{Q}[x]$. Usaremos o critério de Eisenstein com $p = 3$. Segue daí que,

$$3 \nmid 1,\ 3 \mid 6,\ 3 \mid (-12),\ 3 \mid 18,\ 3 \mid (-24), \text{ e } 3 \mid (-60), \text{ mas } 3^2 \nmid (-60).$$

Portanto, $f(x)$ é irredutível em $\mathbb{Q}[x]$.

No próximo capítulo será trabalhado importantes métodos para determinar as raízes de equações algébricas de $2°, 3°$ e $4°$ graus.

4

Equações Algébricas

Neste capítulo veremos fatos históricos que envolvem equações algébricas, introduziremos conceitos relativos a números complexos e raízes de unidade em $\mathbb{C}$. E estudaremos soluções por radicais de equação do $2°, 3°$ e $4°$ graus. Este capítulo estará baseado em [1], [5], [6], [10], [11], [13], [15].

4.1 Fatos Históricos

No período (1700 $a.C.$ - 1700 $d.C.$) observa-se toda uma evolução no simbolismo e na resolução de equações cúbicas e quárticas. Temos três estágios, o retórico (ou verbal), o sincopado (no qual eram usadas abreviações de palavras) e o simbólico. No último estágio, a notação passou por várias modificações e mudanças, até tornar-se razoavelmente estável no tempo de Isaac Newton, século XVII.

A álgebra surgiu por meio de Liberabaci de Fibonacci (1202), Diofanto ($284 - 298$ $a.C.$) com a sua sincopação, e Brahmagupta ($598 - 668$ $d.C.$). Alguns fatores contribuíram para o avanço da álgebra na Europa, entre eles, o sistema de numeração indo-arábico, invenção da imprensa e o ressurgimento da economia.

Na resolução de equações cúbicas e quadráticas houve as contribuições de Niccolo Tartaglia (1500-1557) e Ludovico Ferrari (1522-1565). Somente em 1545, Girolamo Cardano (1501-1576), matemático italiano, publica *"Ars Magna"* com a resolução dessas equações, constituindo-se num marco importante para os algebristas da época. Cardano usava pouca sincopação, ou seja, os seus trabalhos eram baseados na álgebra retórica. Cardano pensava em suas equações com coeficiente numéricos específicos como representantes de categorias gerais. Como exemplo: "seja o cubo e seis vezes o lado igual a 20 (ou $x^3 + 6x = 20$)". Cardano se referia a raízes quadradas de números negativos como *sofísticas* e concluía que o resultado nesse caso era "tão sutil quanto inútil".

François Viète (1540-1603), matemático francês e advogado, destacou-se na álgebra com várias contribuições e foi o mais próximo das ideias modernas. Encontramos em sua obra o conceito de parâmetro e a ideia de uma quantidade desconhecida (incógnita). Ele utilizou uma vogal para representar uma quantidade desconhecida ou indeterminada e uma consoante para representar uma grandeza ou um número supostamente conhecido ou dado. Deste modo, teve um papel primordial na inovação

do simbolismo e na resolução das equações quadráticas, cúbicas e quárticas. Desenvolvendo novos métodos de solução, percebeu algumas relações entre coeficientes e raízes de uma equação, embora seu trabalho tivesse ficado tolhido por sua recusa em aceitar coeficientes ou raízes negativas.

Viète também desenvolveu um método, como descrito em [15], para equações completas de 2º grau sem o uso da fórmula para determinar as raízes da equação. O que pode ser interessante para contextualizar uma aula sobre esse tema. Lembrando que ele recusava em aceitar coeficiente ou raízes negativas.

Girolamo Cardano não foi o descobridor original da solução quer da cúbica quer da quártica, ele afirma que tenha sido dada por Niccolo Tartaglia e Lodovico Ferrari. Cardano publicou os métodos no seu famoso livro Ars Magna, em 1545, no qual não deixou de fazer referência aos descobridores, embora a contragosto de Tartaglia que se considerou traído.

O matemático italiano de Milão Lodovico Ferrari (1522 —1565), estabeleceu-se em Bolonha, Itália e iniciou sua carreira como auxiliar de Girolamo Cardano. Dada sua notável facilidade no aprendizado, Cardano começou por ensinar-lhe matemática. Ferrari ajudou Cardano na descoberta das soluções para as equações quadrática e cúbica e foi ainda imensamente responsável pela solução da equação quártica que Cardano publicou. Ainda jovem (antes dos vinte anos), Ferrari tornou-se apto para o exercício do magistério, recomendou-o o próprio Cardano.

O século XVII apresentou uma intensa atividade em torno da forma dos *imaginários*, terminologia da época. Chamaremos de imaginário o que designamos hoje como números complexos. A associação dos números complexos aos pontos do plano é enfatizada por Gauss. Um fato interessante que segundo Gauss, há muitas confusões quanto ao estatuto destes números, a nomenclatura de positivo, negativo e imaginário respectivamente para $+1, -1$ e $\sqrt{-1}$, foi exatamente o que deu margem a essas confusões, que deveriam ser chamados unidade direta, inversa, e lateral o que mostra seu papel relativo à orientação das direções do plano.

A aplicação da matemática durante a renascença foi na contabilidade, mecânica, mensuração de terras, artes, cartografia, óptica, artes plásticas, entre outras. Demonstrando a relação entre a matemática e a prática cotidiana. Desta forma, formando verdadeiras redes de conhecimento matemático, debates entre matemáticos, e publicações de diversas teorias.

4.2 Introdução aos Números Complexos

Definição 4.1: Consideremos o conjunto $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$. Se $(a, b), (c, d) \in \mathbb{R}^2$, definimos a *adição* e a *multiplicação* da seguinte forma, respectivamente:

$$\begin{aligned}(a+b)+(c+d) =& (a+c, b+d)\\ &\text{e}\\ (a+bi)\cdot(c+di) =& (ac-bd, ad+bc).\end{aligned}$$

O conjunto $\mathbb{R}^2$, munido dessas operações, será chamado conjunto dos números complexos e denotado por $\mathbb{C}$, no qual cada par ordenado é chamado de número

complexo.

Teorema 4.1: As operações em $\mathbb{C}$ têm as seguintes propriedades: a adição e a multiplicação são comutativas, associativas e têm elemento neutro:$(0,0)$ para a adição e $(1,0)$ para a multiplicação. Além disso, dado $(a,b) \in \mathbb{C}$ seu simétrico existe, $-(a,b)$, que é $(-a,-b)$ e, se $(a,b) \neq (0,0)$, seu inverso existe, $(a,b)^{-1}$, que é $(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$. E ainda, a multiplicação é distributiva em relação a adição.

Demonstração. As demonstrações para o inverso de $(a,b) \neq (0,0)$ e a distributividade da multiplicação em relação a adição, deixaremos para consulta do leitor em [6]. Sejam (a,b),(c,d),$(e,f) \in \mathbb{C}$. Iniciaremos com comutatividade da adição. Assim,

$$\begin{aligned}(a,b)+(c,d) &= (a+c, b+d)\\ &= (c+a, d+b)\\ &= (c,d)+(a,b).\end{aligned}$$

Para associatividade da adição.

$$\begin{aligned}(a,b)+((c,d)+(e,f)) &= (a,b)+((c+e,d+f))\\ &= (a+(c+e), b+(d+f))\\ &= ((a+c)+e, (b+d)+f)\\ &= ((a+c, b+d))+(e,f)\\ &= ((a,b)+(c,d))+(e,f).\end{aligned}$$

Para o elemento neutro da adição. Temos $(0,0) \in \mathbb{C}$, então,

$$(a,b)+(0,0) = (a+0, b+0) = (a,b).$$

Para comutatividade da multiplicação.

$$\begin{aligned}(a,b)\cdot(c,d) &= (ac-bd, ad+bc)\\ &= (ca-db, cb+da)\\ &= (c,d)\cdot(a,b)\end{aligned}$$

Para associatividade da multiplicação.

$$\begin{aligned}(a,b)\cdot((c,d)\cdot(e,f)) &= (a,b)\cdot((ce-df,cf+de))\\ &= (a(ce-df)-b(cf+de),a(cf+de)+b(ce-df))\\ &= (ace-adf-bcf-bde,acf+ade+bce-bdf)\\ &= ((ac-bd)e-(ad+bc)f,(ac-bd)f+(ad+bc)e)\\ &= (ac-bd,ad+bc)\cdot(e,f)\\ &= ((a,b)(c,d))\cdot(e,f).\end{aligned}$$

Para elemento neutro da multiplicação. Temos $(1,0)\in\mathbb{C}$, então

$$(a,b)\cdot(1,0) = (a\cdot 1 - b\cdot 0, a\cdot 0 + b\cdot 1) = (a,b).$$

Para o Simétrico de (a,b) igual $(-a,-b)\in\mathbb{C}$.

$$(a,b)+(-a,-b) = (a+(-a),b+(-b)) = (0,0).$$

O simétrico de (a,b) será denotado por $-(a,b)$. □

Note que um número complexo arbitrário (a,b) pode ser escrito como $(a,b) = (a,0)+(b,0)(0,1)$. Admitindo a inclusão $\mathbb{R}\subset\mathbb{C}$, usa-se a identificação $a\longrightarrow(a,0)$ para $a\in\mathbb{R}$, e adota-se o símbolo i para o número complexo $(0,1)$, a expressão $(a,b) = (a,0)+(b,0)(0,1)$, pode ser escrita como $a+bi$, com $a,b\in\mathbb{R}$.

Observe que $i^2 = (0,1)^2 = (-1,0)$, e pode ser identificado por -1. Temos que, os números complexos representados da forma $a+bi$, com $b\neq 0$, chamam-se números imaginários, e se, $a=0$, obtemos os imaginários puros.

Um número complexo $z = a+bi$ se decompõe num soma de duas parcelas a e bi, em que os números reais a e b são chamados de *parte real* e *parte imaginária* de z, respectivamente. Se $z = a+bi$, utilizaremos as notações:

$$a = Re(z) \text{ e } b = Im(z)$$

Temos ainda que o número complexo $a+bi$ é representado no plano $\mathbb{R}^2$ pelo ponto (a,b), veja a Figura 4.1.

Um fato interessante em $\mathbb{C}$ é determinarmos o inverso multiplicativo de $z = a+bi$ não nulo.

Sejam $z = a+bi$ e $z' = a'+b'i$ números complexo não nulos. Como queremos determinar que $z_1z_2 = 1$. Temos,

$$1 = zz' = (a+bi)(a'+b'i) = aa'+ab'i+bia'+bb'i^2 = (aa'-bb')+(ab'+ba')i$$

Recordemos que $1 = 1+0i$ e da igualdade das partes imaginárias e reais, temos o

seguinte sistema nas incógnitas a' e b'.

$$aa' - bb' = 1 \tag{4.1}$$
$$ab' + ba' = 0 \tag{4.2}$$

Segue daí

$$ab' = -ba' \text{ e } b' = \frac{-ba'}{a}.$$

Substituindo na equação (4.1) do sistema acima temos,

$$aa' - b(\frac{-ba'}{a}) = 1 \Rightarrow aa' - b^2a' = a \Rightarrow a'(a^2 + b^2) = a \Rightarrow$$
$$a' = \frac{a}{a^2 + b^2}.$$

Portanto, substituindo em $b' = \frac{-ba'}{a}$ o valor $a' = \frac{a}{a^2 + b^2}$ obtemos,

$$b' = -\frac{b}{a^2 + b^2}$$

Denotaremos o inverso multiplicativo de um número complexo não nulo z por z^{-1} ou $\frac{1}{z}$. Assim,

$$z^{-1} = \frac{1}{z} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i$$

Um número complexo pode ser representado também como um par ordenado de números reais, isto é, $z = a + bi$ é o par ordenado (a,b). Desse modo, a cada número complexo $z = a + bi$ corresponde um ponto $P = (a,b)$ no plano cartesiano. E o plano passa a ser denominado plano de Argand-Gauss. Observe que os números reais $z = a + 0i$, são representados no eixo x, que passará a ser chamado de eixo real. E os da forma $z = 0 + bi$, com $b \neq 0$, são representados no eixo y, que chamaremos de eixo imaginário.

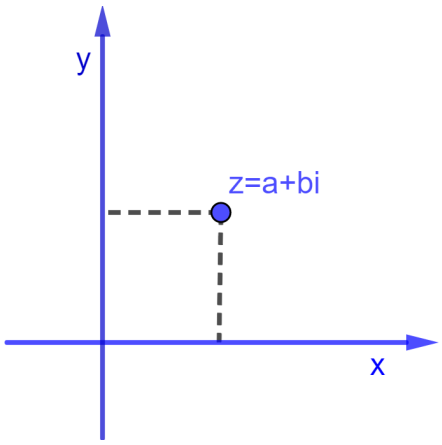


Figura 4.1: Representação de números complexos por pontos do plano
Fonte: Elaborado pelo autor

Definição 4.2: O *conjugado* do número complexo $z = a + bi$ será $\bar{z} = a - bi$.

O conjugado de z, $\bar{z} = a - bi$, representa geometricamente o simétrico de z em relação ao eixo horizontal.

Definição 4.3: O *módulo* de um número complexo $z = a + bi$ é o *módulo* do vetor que o representa, ou seja, é o valor r da distância de sua imagem P à origem. Portanto,

$$|z| = r = \sqrt{x^2 + y^2}.$$

Definição 4.4: O número real θ é chamado *argumento principal de* z e é denotado por $arg(z) = \theta$.

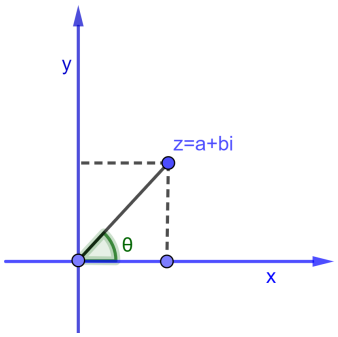


Figura 4.2: Argumento principal θ de $z = a + bi$
Fonte: Elaborado pelo autor

Observe que na Figura 4.2 observe que $a = r\cos\theta$ e $b = r\,\mathrm{sen}\,\theta$. Neste caso, se substituirmos esses valores em $z = a + bi$, encontramos

$$z = r\cos\theta + r\,\mathrm{sen}\,\theta i = r(\cos\theta + i\,\mathrm{sen}\,\theta) \tag{4.3}$$

E (4.3) é conhecida por *forma polar* ou *forma trigonométrica* do número complexo $z = a+bi$ não nulo, com módulo $|z| = r = \sqrt{x^2 + y^2}$ e argumento principal $arg(z) = \theta$.

Exemplo 4.2.1: Para o complexo $z = -1 + \sqrt{3}i$, temos

$$|z| = r = \sqrt{x^2 + y^2} = \sqrt{(-1)^2 + (\sqrt{3})^2} = 2$$

E ainda,

$$\cos\theta = \frac{x}{r} = \frac{1}{2} \text{ e } \mathrm{sen}\,\theta = \frac{y}{r} = \frac{\sqrt{3}}{2}$$

Logo, o $arg(z) = \dfrac{2\pi}{3}$.

Note que todo complexo não-nulo tem uma infinidade de argumentos, dois quaisquer deles diferindo entre si por um múltiplo de 2π.

Os próximos teorema relata sobre o produto e a divisão dos complexos z e z', z' não é necessariamente o conjugado. Deixaremos para o leitor ver a demonstração em [11].

Teorema 4.2: Se $z = r\cos\theta + r\,\mathrm{sen}\,\theta i$ e $z' = r'\cos\theta' + r\,\mathrm{sen}\,\theta' i$, então,

$$zz' = rr'[\cos(\theta+\theta') + i\,\mathrm{sen}(\theta+\theta')]$$

e, se $r' \neq 0$,

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

Exemplo 4.2.2: Calcule $(\sqrt{3}+i)^2$

Logo, $z = \sqrt{3}+i$, $r = \sqrt{3+1} = 2$, $\cos\theta = \dfrac{\sqrt{3}}{2}$ e $\mathrm{sen}\,\theta = \dfrac{1}{2}$. Portanto, $\theta = \dfrac{\pi}{6}$.

$$z = 2\left(\cos\frac{\pi}{6} + \mathrm{sen}\,\frac{\pi}{6}\right)$$
$$z^2 = 2^2\left(\cos\frac{2\pi}{6} + \mathrm{sen}\,\frac{2\pi}{6}\right)$$
$$z^2 = 4\left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) = (2+2i\sqrt{3}).$$

No exemplo acima $z = z'$, o que facilitou a determinação do $arg(z) = \theta$. No entanto, o processo é similar para $z \neq z'$. O argumento principal zz' é dado por

$$arg(zz') = \theta'' \in [0,2\pi), \text{ tal que, } \theta'' \equiv \theta + \theta' \mod 2\pi.$$

A fórmula a seguir é utilizada para o cálculo de potências de um número complexo, conhecida por *Fórmula de De Moivre*, francês Abraham de Moivre (1667-1754), matemático probabilista e atuário, foi eleito membro da Royal Society em 1697 e estudou, entre outras teorias, números complexos.

Proposição 4.1: Dado $z = r(\cos\theta + i\,\mathrm{sen}\,\theta)$ um número complexo não nulo na forma polar, então, para cada número inteiro n, tem-se

$$z^n = r^n(\cos(n\theta) + i\,\mathrm{sen}(n\theta)).$$

Demonstração. Faremos por indução em $n \in \mathbb{N}$. Para $n = 1$ temos,

$$z = r(\cos(\theta) + i\,\mathrm{sen}(\theta))$$

Suponhamos que a igualdade vale para n, provaremos para $n+1$. Seja $n \geq 1$, então

$$z^{n+1} = zz^n,$$

Pela hipótese de indução, temos,

$$z^{n+1} = r(\cos(\theta) + i\,\mathrm{sen}(\theta)(r^n(\cos(n\theta) + i\,\mathrm{sen}(n\theta)),$$

A multiplicação de números complexos na forma polar. Segue que,

$$z^{n+1} = r^{n+1}(\cos(\theta + n\theta) + i\,\mathrm{sen}(\theta + n\theta)),$$

Então,

$$z^{n+1} = r^{n+1}(\cos((n+1)\theta) + i\,\mathrm{sen}((n+1)\theta))$$

Portanto, vale para todo $n \geq 1$. Falta determinarmos para $n = 0$ e $n < 0$.

Seja $n = 0$, ao substituir, obtemos:

$$z^0 = r^0(\cos(0\theta) + i\,\mathrm{sen}(0\theta)) \Rightarrow (\cos(0) + i\,\mathrm{sen}(0)) = 1.$$

O que é verdadeiro já que $\cos 0 = 1$ e $\mathrm{sen}\, 0 = 0$.

Finalizaremos com $n < 0$. Para usarmos os conceitos demonstrado acima, será necessário adotarmos a seguinte estratégia $-n > 0$ e $z^n = (z^{-1})^{-n}$. Aprendemos no início desta seção determinar o inverso multiplicativo. Assim,

$$\begin{aligned} z^{-1} &= \frac{\bar{z}}{|z|^2} \\ &= \frac{a}{\sqrt{a^2-b^2}} - \frac{b}{\sqrt{a^2-b^2}}i = \frac{a-bi}{\sqrt{a^2-b^2}}. \end{aligned}$$

Por meio da a forma polar da definição de módulo e do fato que o conjugado de um número complexo é simétrico em relação ao eixo horizontal, temos

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

Assim, pela fórmula já demonstrada para $n \geq 1$,

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

Portanto, a igualdade vale para todo $n \in \mathbb{Z}$. □

Exemplo 4.2.3: Calcule $(1 + i\sqrt{3})^{20}$.

Ao realizar os cálculos obtemos $r = 2$ e $\theta = \dfrac{\pi}{3}$. Logo, pela fórmula de Moivre,

$$\begin{aligned} (1 + i\sqrt{3})^{20} &= \left(2[\cos\frac{\pi}{3} + i\,\mathrm{sen}\,\frac{\pi}{3}]\right)^{20} \\ &= 2^{20}\left[\cos\frac{20\pi}{3} + i\,\mathrm{sen}\,\frac{20\pi}{3}\right] \\ &= 2^{20}\left[\cos\frac{2\pi}{3} + i\,\mathrm{sen}\,\frac{2\pi}{3}\right], \end{aligned}$$

pois $\dfrac{20\pi}{3} = \dfrac{2\pi}{3} + 3(2)\pi$. Portanto,

$$\begin{aligned} (1 + i\sqrt{3})^{20} &= 2^{20}\left[-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right] \\ &= 2^{19}\left[-1 + i\sqrt{3}\right] \end{aligned}$$

No que segue mostramos agora como calcular raízes de números complexos. Sabemos que um elemento de um corpo F tem no máximo n raízes n-ésimas em F. Note que $w = 1, -1, i, -i$ tem a propriedade $w^4 = 1$ e é chamado de uma raiz quarta complexa da unidade.

Proposição 4.2: Para cada número natural n, um número complexo $z \neq 0$ tem exatamente n raízes complexas denominadas raízes n-ésimas, a saber,

$$z_l = \sqrt[n]{r}\left(\cos\left(\frac{\theta + 2\pi l}{n}\right) + i\,\mathrm{sen}\left(\frac{\theta + 2\pi l}{n}\right)\right)\ l = 0,1,\ldots,n-1,$$

no qual $r = |z| > 0$ e $\theta = arg(z)$.

Demonstração. Para $n \geq 2$, encontraremos um complexo z tal que,

$$\sqrt[n]{r(\cos\theta + i\,\mathrm{sen}\,\theta)} \Leftrightarrow z^n = r(cos\theta + i\,\mathrm{sen}\,\theta)$$

Suponhamos que $z = \rho(\cos\alpha + i\,\mathrm{sen}\,\alpha)$, obtemos da igualdade acima,

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

Pela fórmula de Moivre,

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

Já que complexos iguais têm módulos iguais e argumentos congruentes, $\rho^n = r$ e $n\alpha = \theta + 2\pi\lambda, \lambda \in \mathbb{Z}$. Daí $\rho = \sqrt[n]{r}$ e $\alpha = \dfrac{\theta + 2\pi\lambda}{n}$. Portanto,

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

Determinaremos os possíveis valores de l. Sejam $\lambda, \mu \in \mathbb{Z}$. Da igualdade de números complexos na forma polar, temos que, para algum $s \in \mathbb{Z}$

$$\begin{aligned} z_\lambda = z_\mu &\Leftrightarrow \frac{\theta + 2\pi\lambda}{n} - \frac{\theta + 2\pi\mu}{n} = 2\pi s \\ &\Leftrightarrow \frac{\lambda}{n} - \frac{\mu}{n} = s, \\ &\Leftrightarrow \lambda - \mu = sn, \\ &\Leftrightarrow \lambda \equiv \mu \mod n. \end{aligned}$$

Assim, para cada resto μ há uma raiz n-ésima de z. Como há n restos possíveis. E o resto é sempre menor que o divisor, neste caso ser o n. Temos então, $l = 0,1,\ldots,n-1$.

$$z_l = \sqrt[n]{r}\left(\cos\left(\frac{\theta + 2\pi l}{n}\right) + i\,\mathrm{sen}\left(\frac{\theta + 2\pi l}{n}\right)\right)\ l = 0,1,\ldots,n-1.$$

□

Exemplo 4.2.4: Calcule em $\mathbb{C}$, $\sqrt[3]{-64}$.

Como, $-64 = 64.(cos\pi + i\,\text{sen}\,\pi)$ temos,

$$\sqrt[3]{-64} = \sqrt[3]{64}\left(cos\frac{\pi + 2l\pi}{3} + i\,\text{sen}\,\frac{\pi + 2l\pi}{3}\right)$$
$$z_1 = 4\left(\cos\frac{\pi}{3} + i\,\text{sen}\,\frac{\pi}{3}\right) = 2 + 2\sqrt{3}i$$
$$z_2 = 4\left(\cos\pi + i\,\text{sen}\,\pi\right) = -4$$
$$z_3 = 4\left(\cos\frac{5\pi}{3} + i\,\text{sen}\,\frac{5\pi}{3}\right) = 2 - 2\sqrt{3}i.$$

Definição 4.5: As raizes complexas n-ésimas de 1 são chamadas de *raízes n-ésimas da unidade.*

Como $arg(1) = 0$, as raízes complexas n-ésimas da unidade são vértices de um polígono regular de n lados inscrito no círculo de centro na origem e raio 1 em $\mathbb{C}$, com um dos vértices no ponto 1.

Proposição 4.3: As n raízes complexas da unidade, denotadas $U_n(\mathbb{C})$, são obtidas como potências de $\xi = cos\frac{2\pi}{n} + isen\frac{2\pi}{n}$.

Demonstração. Temos $\xi = \cos\frac{2\pi}{n} + i\,\text{sen}\,\frac{2\pi}{n}$. Chamemos $\xi = z_1$. Assim, pela fórmula de Moivre,

$$\xi^l = z_l = \cos\frac{2\pi l}{n} + i\,\text{sen}\,\frac{2\pi l}{n},\ l = 0,1,\ldots,n-1.$$

Logo, $U_n(\mathbb{C}) = 1, \xi, \ldots, \xi^{n-1}$, note que $\xi^n = 1$. □

Exemplo 4.2.5: Raízes cúbicas da unidade.

Seja, $U_3(\mathbb{C}) = \{1, \xi, \xi^2\}$, as 3 raízes complexas cúbicas da unidade. Então, pela Proposição 4.3 obtemos.

$$\xi^0 = 1$$
$$\xi = cos\frac{2\pi}{3} + isen\frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$$
$$\xi^2 = cos\frac{4\pi}{3} + isen\frac{4\pi}{3} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$$

A proposição abaixo será fundamental para encontrarmos as raízes de uma equação de grau 3.

Proposição 4.4: Seja z um número complexo não nulo, $w \in \mathbb{C}$ uma raiz n-ésima de z e $\xi = \cos\frac{2\pi}{n} + i\,\text{sen}\,\frac{2\pi}{n}$. Então, as raízes n-ésimas de z são $w\xi^r$, $r = 0,\ldots,n-1$.

Demonstração. Seja, $(w\xi^r)^n = w^n(\xi^n)^r = z \cdot 1^r = z$.Assim, $w\xi^r$ é raiz n-ésima de z tal que $r = 0, \ldots, n-1$.

Seja $\alpha \in \mathbb{C}$ uma raiz n-ésima de z. Então, $\alpha^n = z = w^n$ e $1 = \alpha^n w^{-n} = (\alpha w^{-1})^n$. Portanto , αw^{-1} é uma raiz n-ésima da unidade. Segue daí que $\alpha w^{-1} = \xi^r$ para $r = 0, \ldots, n-1$. Portanto $\alpha = w\xi^r$, para algum $r = 0, \ldots, n-1$. □

Exemplo 4.2.6: Uma raiz quarta de 16 é o número real positivo 2. As quatro raízes complexas quartas de 16 são:

i $z_0 = 2$

ii $z_1 = 2\xi = 2i$

iii $z_2 = 2\xi^2 = -2$

iv $z_3 = 2\xi^3 = -2i$

Para finalizarmos o estudo de raízes de unidade, enunciaremos três propriedades, cujas verificações são obtidas diretamente da definição.

1 O produto de duas raízes n-ésimas da unidade é também uma raiz n-ésima da unidade;

2 O inverso de uma raiz n-ésima da unidade é também uma raiz n-ésima da unidade;

3 Temos que $U_n(\mathbb{C})$ tem estrutura de grupo.

Definição 4.6: Uma raiz complexa n-ésima da unidade α é chamada de *raíz primitiva n-ésima da unidade* se

$$U_n(\mathbb{C}) = \{\alpha^m; m \in \mathbb{Z}\}.$$

Isto é equivalente ao fato das potências de α determinarem todas as raízes n-ésimas da unidade e $U_n(\mathbb{C})$ é grupo cíclico (veja Capítulo 6) gerado pela raiz primitiva.

Exemplo 4.2.7: -1 é a única raiz primitiva quadrada da unidade.

Exemplo 4.2.8: i e $-i$ são as únicas raízes primitivas quartas da unidade, pois

$$\begin{aligned}
\{i^m; m \in \mathbb{Z}\} &= \{1, i, i^2 = -1,, i^3 = -i\} = U4(\mathbb{C}),\\
\{(-i)^m; m \in \mathbb{Z}\} &= \{1, -i, (-i^2) = -1, (-i)^3 = i\} = U_4(C)\\
\{1^m; m \in \mathbb{Z}\} &= 1 \neq U_4(C),\\
\{(-1)^m; m \in \mathbb{Z}\} &= \{1, -1\} \neq U_4(C).
\end{aligned}$$

Com o conhecimento acumulado nesta seção temos condições de avançarmos um pouco no estudo de raízes complexas de polinômios em $\mathbb{R}[x]$. Para isso, considere a definição de conjunção de polinômios.

Definição 4.7: Seja $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{C}[x]$. O polinômio conjugado de $f(x)$ é $\bar{f}(x)$ dada por

$$\bar{f}(x) = \bar{a}_n x^n + \bar{a}_{n-1}x^{n-1} + \ldots + \bar{a}_1 x + \bar{a}_0$$

no qual $\bar{a}_j$ é conjugado de a_j, $j = 0, 1, \ldots, n$.

Note que para $f(x), g(x), h(x) \in \mathbb{C}[x]$, valem as seguintes propriedades que seguem, obtidas diretamente da definição de conjugação.

i se $f(x) = g(x) + h(x)$, então $\bar{f}(x) = \bar{g}(x) + \bar{h}(x)$;

ii se $f(x) = g(x) + h(x)$, então $\bar{f}(x) = \bar{g}(x) \cdot \bar{h}(x)$;

iii $\bar{f}(x) = f(x)$ se, e somente se, $f(x) \in \mathbb{R}[x]$;

iv se $\beta \in \mathbb{C}$, então $\bar{f}(\bar{\beta}) = \overline{f(\beta)}$.

Além disso, temos que se $\beta \in \mathbb{C}$ é uma raiz de $f(x) \in \mathbb{C}[x]$ de multiplicidade m, então $\bar{\beta}$ é uma raiz de $\bar{f}(x)$ com multiplicidade m também. De fato basta observar que se $f(x) = (x - \beta)^m q(x)$ então $\bar{f}(x) = (x - \bar{\beta})^m \bar{q}(x)$.

Dessa maneira, podemos concluir que $\beta \in \mathbb{C}$ é raiz de $f(x) \in \mathbb{R}[x]$ com multiplicidade m. Assim, as raízes complexas não reais de $f(x) \in \mathbb{R}[x]$ ocorrem em pares (cada raiz com sua conjugada) e todo polinômio de grau ímpar em $R[x]$ tem pelo menos uma raiz real.

4.3 Soluções de equações de grau 2, 3 e 4

4.3.1 Equação do 2ºgrau

A resolubilidade de uma equação de grau 2 é conhecida desde o tempo dos babilônios. Ela também por grande partes dos estudantes do Ensino Fundamental e Médio. Leva o nome de *fórmula de Bhaskara*, já que foi publicada pelo matemático indiano Bháskara, que viveu no século XII. O método usado por ele é o de completar quadrados. Usaremos esse método para encontrar a fórmula dessa equação.

Definição 4.8: Diz-se que $p : \mathbb{R} \longrightarrow \mathbb{R}$ é uma *função polinomial* quando existem números $a_0, a_1, \ldots, a_n$ tais que, para todo $x \in \mathbb{R}$, tem-se

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

Se $a_n \neq 0$, dizemos que p tem *grau* n.

Observe que podemos, na definição acima, alterar o corpo $\mathbb{R}$ para $\mathbb{C}$, e analogamente definir um função polinomial complexa.

Definição 4.9: Uma função polinomial $f : \mathbb{R} \longrightarrow \mathbb{R}$ chama-se *quadrática* quando existem números reais a, b, c com $a \neq 0$,tais que $f(x) = ax^2 + bx + c$ para todo $x \in R$.

Definição 4.10: Uma *equação algébrica* é um equação da forma $f(x) = 0$, em que f é um função polinomial.

Considere o trinômio $f(x) = ax^2 + bx + c$ em $\mathbb{C}[x]$ e $a \neq 0$. Assim,

$$ax^2 + bx + c = a\left(x^2 + \frac{bx}{a} + \frac{c}{a}\right).$$

Completando quadrados, tendo como referência as duas primeiras parcelas dos parênteses, encontramos,

$$\begin{aligned} ax^2 + bx + c &= a\left(x^2 + 2 \cdot \frac{b}{2a} \cdot x + \frac{b^2}{4a^2} - \frac{b^2}{4a^2} + \frac{c}{a}\right) \\ &= a\left[\left(x + \frac{b}{2a}\right)^2 + \frac{4ac - b^2}{4a^2}\right]. \end{aligned}$$

Esta última maneira de escrevermos o trinômio do segundo grau, será chamada de *forma canônica*.

Temos as seguintes equivalências, para $f(x) = 0$,

$$\begin{aligned} ax^2 + bx + c = 0 &\Leftrightarrow \left(x + \frac{b}{2a}\right)^2 + \frac{4ac - b^2}{4a^2} = 0 \\ &\Leftrightarrow \left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2} \\ &\Leftrightarrow x + \frac{b}{2a} = \pm\frac{\sqrt{b^2 - 4ac}}{2a} \\ &\Leftrightarrow x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \end{aligned}$$

Note que a extração da raiz do *discriminante* $\Delta = b^2 - 4ac$ tem sentido para qualquer Δ, já que estamos no corpo $\mathbb{C}$. Assim, a equação quadrática sempre terá raiz complexa.

Considerando coeficientes reais, se os coeficientes $a, b, c \in \mathbb{R}$, o discriminante fornece as seguintes relações com a raiz:

O discriminante fornece as seguintes relações com a raiz: se os coeficientes a, b e c da equação $ax^2 + bx + c = 0$ são reais, então, pela fórmula resolvente, temos o seguinte resultado:

$\Delta > 0$ se, e somente se, a equação tem duas raízes reais distintas;

$\Delta = 0$ se, e somente se, a equação tem duas raízes reais iguais;

$\Delta < 0$ se, e somente se, a equação tem duas raízes complexas distintas conjugadas.

Exemplo 4.3.1: Sejam x_1 e x_2 as raízes da equação $ax^2 + bx + c = 0$. Mostre que $x_1 + x_2 = \dfrac{-b}{a}$ e $x_1 x_2 = \dfrac{c}{a}$.

Logo,

$$\begin{aligned} x_1 + x_2 &= \frac{-b + \sqrt{b^2 - 4ac}}{2a} + \frac{-b - \sqrt{b^2 - 4ac}}{2a} \\ &= \frac{-2b}{2a} = \frac{-b}{a}. \end{aligned}$$

$$\begin{aligned} x_1 x_2 &= \frac{-b + \sqrt{b^2 - 4ac}}{2a} \cdot \frac{-b - \sqrt{b^2 - 4ac}}{2a} \\ &= \frac{(-b)^2 - (b^2 - 4ac)}{4a^2} = \frac{4ac}{4a^2} = \frac{c}{a} \end{aligned}$$

4.3.2 Equação do 3ºgrau

As soluções de uma equação de terceiro grau com coeficientes complexos. Embora não seja prático a resolução com o uso da fórmula desenvolvida por del Ferro e Tartaglia e publicada por Cardano, ela contribui para entender a origem de certos problemas. Vejamos abaixo um exemplo que ilustra esse fato.

Exemplo 4.3.2: Mostre que o número $\sqrt[3]{2 + \sqrt{5}} + \sqrt[3]{2 - \sqrt{5}}$ é inteiro.

Observe que a soma acima representa um número real. Tomando

$$x = \sqrt[3]{2 + \sqrt{5}} + \sqrt[3]{2 - \sqrt{5}}.$$

e elevando ao cubo ambos os lados e desenvolvendo o cubo da soma, obtemos:

$$x^3 = (2 + \sqrt{5}) + 3\left(\sqrt[3]{2 + \sqrt{5}}\right)^2 \sqrt[3]{2 - \sqrt{5}} + 3\sqrt[3]{2 + \sqrt{5}}\left(\sqrt[3]{2 - \sqrt{5}}\right)^2 + \left(2 - \sqrt{5}\right).$$

Observe que temos termos comuns nas parcelas. Simplificando, temos:

$$x^3 = 4 + 3\left(\sqrt[3]{2 + \sqrt{5}} + \sqrt[3]{2 - \sqrt{5}}\right)\sqrt[3]{2 + \sqrt{5}}\sqrt[3]{2 - \sqrt{5}}.$$

No entanto a expressão entre parênteses é o próprio x. Se efetuarmos o produto, temos,

$$\sqrt[3]{2 + \sqrt{5}}\sqrt[3]{2 - \sqrt{5}} = \sqrt[3]{4 - 5} = -1.$$

Portanto, ao fazermos as devidas substituições por x, obtemos

$$x^3 = 4 - 3x \Leftrightarrow x^3 + 3x - 4 = 0.$$

O enunciado afirmou que x é inteiro. Note que se escolhermos aleatoriamente qual seria a raiz dessa equação, bastando para isso usar a Proposição 3.7, conseguiríamos obter $x_1 = 1$. Então usando o algoritmo de Briot-Ruffini, temos a seguinte relação

$$x^3 + 3x - 4 = 0 \Leftrightarrow (x-1)(x^2+x+4) = 0$$

Mas o trinômio do segundo grau não tem raízes reais. Logo, 1 é única raiz real da equação. De fato o número $\sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}}$ é um número inteiro já que representa a raiz real da equação $x^3 + 3x - 4$.

Vejamos as soluções de uma equação de terceiro grau com coeficientes complexos.

Consideramos a equação geral do terceiro grau em coeficientes complexos que, sem perda de generalidade, podemos supor que esteja na forma:

$$x^3 + a_2x^2 + a_1x + a_0 = 0 \tag{4.4}$$

Por meio de uma mudança de variável, vamos colocar o polinômio em (4.4) numa forma em que não figure o termo do segundo grau. Substituindo x por $y + d$ na Equação (4.4) após desenvolver o cubo da soma, o quadrado da soma temos,

$$\begin{aligned} x^3 + a_2x^2 + a_1x + a_0 &= (y+d)^3 + a_2(y+d)^2 + a_1(y+d) + a_0 \\ &= y^3 + (3d + a_2)y^2 + (3d^2 + 2da_2 + a_1)y + (d^3 + d^2a_2 + da_1 + a_0). \end{aligned}$$

Após tomarmos $d = -\dfrac{a_2}{3}$ na expressão acima temos que,

$$\begin{aligned} &y^3 + (3d + a_2)y^2 + (3d^2 + 2da_2 + a_1)y + (d^3 + d^2a_2 + da_1 + a_0) = \\ &y^3 + \left(3\left(\frac{-a_2}{3}\right) + a_2\right)y^2 + \left(3\left(-\frac{a_2}{3}\right)^2 + 2\left(-\frac{a_2}{3}\right)a_2 + a_1\right)y \\ &+ \left(\left(-\frac{a_2}{3}\right)^3 + \left(-\frac{a_2}{3}\right)^2 a_2 + \left(-\frac{a_2}{3}\right)a_1 + a_0\right) \end{aligned}$$

Observe que após a substituição temos $\left(3\left(\dfrac{-a_2}{3}\right) + a_2\right)y^2$=0. Então eliminaremos o termo do segundo grau, que é nosso primeiro objetivo. Logo, fazendo as devidos simplificações e igualando ao polinômio $x^3 + a_2x^2 + a_1x + a_0$, determinamos

$$x^3 + a_2x^2 + a_1x + a_0 = y^3 + py + q = 0,$$

para

$$x = y + d \Rightarrow x = y - \frac{a_2}{3},\ p = a_1 - \frac{a_2^2}{3},\ q = \frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0.$$

Na resolução da equação obtemos

$$y^3 + py + q = 0 \tag{4.5}$$

Sejam u e v duas novas indeterminadas. Façamos em (4.5) a mudança de varáveis: $y = u + v$. Teremos,

$$y^3 + py + q = (u+v)^3 + p(u+v) + q \tag{4.6}$$
$$= u^3 + 3u^2v + 3uv^2 + v^3 + pv + pu + q \tag{4.7}$$
$$= (u^3 + v^3 + q) + (u+v)(p+3uv) = 0. \tag{4.8}$$

Se tomarmos $u^3 + v^3 = -q$ no primeiro parenteses de (4.6). e, ainda, se substituirmos $uv = -\frac{p}{3}$ no terceiro parenteses de (4.6) teremos a expressão igual a zero. Logo,

A solução (u,v) do sistema

$$\begin{cases} u^3 + v^3 = -q \\ uv = -\frac{p}{3} \end{cases}$$

nos fornece uma solução (u,v) de (4.6). Sendo da forma $y = u + v$ de (4.5).

Note que ao elevarmos ao cubo a segunda equação do sistema acima, $u^3v^3 = -\frac{p^3}{27}$, segue que (u,v) é uma solução do sistema , então u^3 e v^3 são soluções da seguinte equação do segundo grau:

$$z^2 + qz - \frac{p^3}{27} = 0 \tag{4.9}$$

Já que, ao tomarmos as raízes z_1 e z_2 da equação acima, obtemos a soma e produto dessas raízes como no exemplo (4.3.1). Ou seja,

$$z_1 + z_2 = \frac{-q}{1} = -q = u^3 + v^3$$
$$z_1 z_2 = \frac{\frac{-p^3}{27}}{1} = -\frac{p^3}{27} = u^3v^3$$

Resolvendo a Equação (4.9) como mostramos na Subseção (4.3.1)

$$z_1 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \text{ e } z_1 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

O surgimento do número 4 nas expressões acima é devido a "colocação" do número 2 na raiz quadrada. Pela simetria do papel que desempenham u e v, podemos supor que $u^3 = z_1$ $v^3 = z_2$.

Tomando uma das raízes cúbicas de z_1 e denotando-a por $\sqrt[3]{z_1}$, segue-se da Proposição (4.4) que as soluções de $u^3 = z_1$ são $\sqrt[3]{z_1}$, $w\sqrt[3]{z_1}$, e $w^2\sqrt[3]{z_1}$, em que $w = \frac{-1 + i\sqrt{3}}{2}$ é uma raízes cúbicas da unidade, (veja Corolário 4.3).

Denotando $v_1 = \sqrt[3]{z_2}$ tal que $\sqrt[3]{z_1}\sqrt[3]{z_2} = -\frac{p}{3}$, de modo que a segunda equação do

sistema acima seja satisfeita, esse sistema admite as seguintes soluções:

$$\begin{aligned} u_1 &= \sqrt[3]{z_1},\ v_1 = \sqrt[3]{z_2};\\ u_1 &= w\sqrt[3]{z_1},\ v_1 = w^2\sqrt[3]{z_2};\\ u_1 &= w^2\sqrt[3]{z_1},\ v_1 = w\sqrt[3]{z_2}; \end{aligned}$$

Para verificar a condição, basta observarmos que $w \cdot w^2 = w^3 = 1$ satisfazendo a segunda equação do sistema e que w^2 e w^4 são diferentes de 1, logo, não satisfaz a condição.

Segue então, que a Equação (4.5) possui como soluções as chamadas *fórmulas de Cardan*

$$\begin{aligned} y_1 = u_1 + v_1 &= \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\\ y_2 = u_2 + v_2 &= w\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + w^2\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\\ y_3 = u_3 + v_3 &= w^2\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + w\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \end{aligned}$$

No Exemplo (4.3.2) trabalhamos com a equação $x^3+3x-4=0$. Abaixo usaremos a fórmula de Cardano para solucioná-la.

Exemplo 4.3.3: Consideremos a equação $x^3 + 3x - 4 = 0$ em $\mathbb{C}[x]$.

A fórmula de Cardano fornece

$$\begin{aligned} y_1 &= \sqrt[3]{-\frac{-4}{2} + \sqrt{\frac{(-4)^2}{4} + \frac{3^3}{27}}} + \sqrt[3]{-\frac{-4}{2} - \sqrt{\frac{(-4)^2}{4} + \frac{3^3}{27}}}\\ &= \sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}} = 1.\\ y_2 &= w\sqrt[3]{-\frac{-4}{2} + \sqrt{\frac{(-4)^2}{4} + \frac{3^3}{27}}} + w^2\sqrt[3]{-\frac{-4}{2} - \sqrt{\frac{(-4)^2}{4} + \frac{3^3}{27}}}\\ &= w\sqrt[3]{2+\sqrt{5}} + w^2\sqrt[3]{2-\sqrt{5}}\\ y_3 &= w^2\sqrt[3]{-\frac{-4}{2} + \sqrt{\frac{(-4)^2}{4} + \frac{3^3}{27}}} + w\sqrt[3]{-\frac{-4}{2} - \sqrt{\frac{(-4)^2}{4} + \frac{3^3}{27}}}\\ &= w^2\sqrt[3]{2+\sqrt{5}} + w\sqrt[3]{2-\sqrt{5}}, \end{aligned}$$

em que $w = \dfrac{-1+i\sqrt{3}}{2}$.

Como $a_2 = 0$ não é necessário fazermos a mudança de variável $x = y - \frac{a_2}{3}$ logo, $y_1 = x_1, y_2 = x_2$ e $y_3 = x_3$ são as raízes da equação original. E perceba que, de fato, 1 é única raiz real.

Além do que foi exposto aqui, nas equações de 3ºgrau temos as seguintes relações entre as raízes e os seus coeficientes, conhecidas como *as relações de Girard*. Albert Girard foi um matemático francês, trabalhou em álgebra, trigonometria e aritmética.

Sejam x_1,x_2 e x_3 raízes da equação $ax^3 + bx^2 + cx + d = 0$. Então,

$$\begin{aligned} x_1 + x_2 + x_3 &= -\frac{b}{a}; \\ x_1 \cdot x_2 + x_1 \cdot x_3 + x_2 \cdot x_3 &= \frac{c}{a}; \\ x_1 \cdot x_2 \cdot x_3 &= -\frac{d}{a}. \end{aligned}$$

Exemplo 4.3.4: Resolva a equação $x^3 - x^2 - 2x + 2 = 0$, sabendo que o produto de duas de suas raízes é igual a -2.

Sejam x_1, x_2 e x_3 as raízes da equação. Acrescentando a condição acima às relações entre coeficientes e raízes, obtemos o sistema:

$$\begin{cases} x_1 + x_2 + x_3 = 1 \\ x_1x_2 + x_1x_3 + x_2x_3 = -2 \\ x_1x_2x_3 = -2 \\ x_1x_2 = -2 \end{cases}$$

Da terceira e quarta equação segue-se que $x_3 = 1$. Da primeira, temos $x_1 + x_2 = 0$, que juntamente com a quarta nos fornece $x_1 = \pm\sqrt{2}$. Como $x_2 = -x_1$, as raízes da equação são $1, \sqrt{2}$ e $-\sqrt{2}$.

4.3.3 Equação do 4ºgrau

Apresentaremos o método de Ferrari para resolução de equações do quarto grau.

Considere a equação:

$$x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0 \tag{4.10}$$

Encontramos que $x^4 + a_3x^3 = -(a_2x^2 + a_1x + a_0)$. Completando o quadrado no primeiro membro desta equação

$$x^4 + a_3x^3 + \frac{a_3^2x^2}{4} = \frac{a_3^2x^2}{4} - a_2x^2 - a_1x - a_0$$

e reagrupando o segundo membro, obtemos

$$\left(x^2+\frac{1}{2}a_3x\right)^2=\left(\frac{1}{4}a_3^2-a_2\right)x^2-a_1x-a_0. \tag{4.11}$$

Transformaremos o segundo membro de (4.11) em um quadrado perfeito, sem eliminar o quadrado perfeito do primeiro membro. Para isso ocorrer, somaremos a expressão $y^2+2y\left(x^2+\frac{1}{2}a_3x\right)$ a ambos membros de (4.11),

$$\left(x^2+\frac{1}{2}a_3x\right)^2+y^2+2y\left(x^2+\frac{1}{2}a_3x\right)=\left(\frac{1}{4}a_3^2-a_2\right)x^2-a_1x-a_0+y^2+2y\left(x^2+\frac{1}{2}a_3x\right) \Leftrightarrow$$
$$\left(x^2+\frac{1}{2}a_3x\right)^2+2y\left(x^2+\frac{1}{2}a_3x\right)+y^2=\left(\frac{1}{4}a_3^2-a_2\right)x^2-a_1x-a_0+y^2+2yx^2+\frac{2ya_3x}{2}$$

Portanto,

$$\left[\left(x^2+\frac{1}{2}a_3x+y\right)\right]^2=\left(2y+\frac{1}{4}a_3^2-a_2\right)x^2+(ya_3-a_1)x+(y^2-a_0). \tag{4.12}$$

Determinaremos os valores de y que transformarão o segundo membro de (4.12) em um quadrado perfeito. Sabemos que se o discriminante de um trinômio do segundo grau é igual a zero, este trinômio será um quadrado perfeito. Segue que,

$$\Delta=(ya_3-a_1)^2-4\cdot\left(2y+\tfrac{1}{4}a_3^2-a_2\right)\cdot(y^2-a_0)=0$$

Efetuando os cálculos, encontramos uma equação do terceiro grau, isto é,

$$8y^3-4a_2y^2+(2a_1a_3-8a_0)y+(4a_0a_2-a_0a_3^3-a_1^2)=0 \tag{4.13}$$

Tomando y como uma das raízes da Equação (4.13), o segundo membro da Equação (4.12) será um quadrado perfeito, ou seja,

$$\left[\left(x^2+\frac{1}{2}a_3x\right)^2+y\right]^2=(\alpha x+\beta)^2 \tag{4.14}$$

com α e β convenientes. Esta equação se resolve mediante a resolução das duas seguintes equações do segundo grau:

$$\left(x^2+\frac{1}{2}a_3x\right)+y=(\alpha x+\beta),\left(x^2+\frac{1}{2}a_3x\right)+y=-(\alpha x+\beta).$$

Portanto, temos que a Equação (4.10) é equivalente a Equação (4.14). Isso que a resolução de uma equação do quarto grau pose ser reduzida à resolução de equações de graus dois e três.

Exemplo 4.3.5: Resolvamos a equação $x^4 - 2x^3 - x^2 - 2x - 2 = 0$

Para encontrarmos o y que satisfaz a Equação (4.13). Mostraremos o método de Ferrari. Logo,

$$8y^3 - 4a_2y^2 + (2a_1a_3 - 8a_0)y + (4a_0a_2 - a_0a_3^3 - a_1^2) = 8y^3 + 4y^2 + 24y + 12 \Rightarrow$$
$$2y^3 + y^2 + 6y + 3 = 0.$$

Resolvendo a equação do terceiro grau, encontramos, $y = -\frac{1}{2}$.
Pelas Equações (4.12) e (4.14), temos:

$$\left(x^2 - x - \frac{1}{2}\right)^2 = x^2 + 3x + \frac{9}{4} = \left(x + \frac{3}{2}\right)^2$$

Deste modo, temos as seguintes equações do segundo grau:

$$x^2 - x - \frac{1}{2} = x + \frac{3}{2} \text{ e } x^2 - x - \frac{1}{2} = -x - \frac{3}{2}$$

Determinando as raízes das equações acima, temos as soluções da equação proposta. Então,

$$1 + \sqrt{3}, 1 - \sqrt{3}, i, \text{ e } -i.$$

As relações de Girard para uma equação do quarto grau são:
Sejam x_1,x_2, x_3 e x_4 raízes da equação $ax^4 + bx^3 + cx^2 + dx + e = 0$. Então,

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= -\frac{b}{a}; \\ x_1 \cdot x_2 + x_1 \cdot x_3 + x_1 \cdot x_4 + x_2 \cdot x_3 + x_2 \cdot x_4 + x_3 \cdot x_4 &= \frac{c}{a}; \\ x_1 \cdot x_2 \cdot x_3 + x_1 \cdot x_2 \cdot x_4 + x_1 \cdot x_3 \cdot x_4 + x_2 \cdot x_3 \cdot x_4 &= -\frac{d}{a}; \\ x_1 \cdot x_2 \cdot x_3 \cdot x_4 &= \frac{e}{a}. \end{aligned}$$

Deixaremos para o leitor o estudo da demonstração das relações entre coeficientes e raízes de uma equação algébrica ou *relações de Girard*, que podem ser vista em [10].

No próximo capítulo continuaremos com as propriedades das equações algébricos e abordaremos a teoria de Corpos.

5

Extensões Algébricas dos Racionais e Corpos

O objetivo deste capítulo é ampliar os conceitos abordados no Capítulo 2. Os conceitos aqui abordados estarão de acordo com [2], [4], [7], [9], [10] e [12]

5.1 Extensões de corpos

Relembrando que se em um domínio de Integridade todo elemento não nulo for invertível, então o domínio será chamado de corpo. O teorema seguinte diz que no caso finito, corpos e domínios são definições equivalentes.

Teorema 5.1: Se K é um domínio finito então K é um corpo.

Demonstração. Basta provar que todo elemento não nulo é inversível. Seja $K = \{r_1, \ldots, r_n\}$ (todos distintos) um domínio de integridade. Tomamos $r \in K$, $r \neq 0$ qualquer. Considere $\{rr_1, rr_2, \ldots, rr_n\}$. Se para algum i e j maiores do que n temos que $rr_i = rr_j$, então $r_i = r_j$ pela lei do cancelamento. Portanto $\{rr_1, rr_2, \ldots, rr_n\}$ é um conjunto de n elementos distintos de K, dado que o conjunto é finito e a multiplicação é fechada em K. Logo, qualquer r_i pode ser escrito como rr_j para algum j. Como K tem n elementos,

$$\{rr_1, rr_2, \ldots, rr_n\} = K = \{r_1, r_2, \ldots, r_n\}.$$

Em particular, $rr_j = 1$ para algum j, portanto $r_j = r^{-1}$. □

Outro fato importante sobre corpos está representado no corolário abaixo:

Corolário 5.1: $\mathbb{Z}_p$ é um corpo se, e somente se, p é primo.

Vejamos um exemplo interessante sobre corpos. Seja $p \geq 2$ primo, o conjunto $Q[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Q}\}$ é um corpo entre $\mathbb{Q}$ e $\mathbb{R}$. De fato, $\mathbb{Q}[\sqrt{p}]$ é fechado para operação soma e produto em que, para $a, b, c, d \in \mathbb{Q}$ temos

$$(a + b\sqrt{p}) + (c + d\sqrt{p}) = (a + c) + (b + d)\sqrt{p}$$
e
$$(a + b\sqrt{p}) \cdot (c + d\sqrt{p}) = (ac + pbd) + (ad + bc)\sqrt{p}.$$

O elemento neutro da soma é $0 + 0\sqrt{p}$ e da multiplicação é $1 = 1 + 0\sqrt{p}$. Por uma conta aritmética simples, verificamos que existe simétrico aditivo, para todo $x = a + b\sqrt{p} \in \mathbb{Q}[p]$ temos $-x = -a - b\sqrt{p}$. Ainda, existe inverso multiplicativo, bastando observar que para $x = a + b\sqrt{p} \neq 0$ em $\mathbb{Q}[\sqrt{p}]$, o elemento $y \in \mathbb{Q}[\sqrt{p}]$ dado por

$$y = \frac{1}{a + b\sqrt{p}} \cdot \frac{a - b\sqrt{p}}{a - b\sqrt{p}} = \frac{a - b\sqrt{p}}{a^2 - b^2 p}, \text{ é tal que } x \cdot y = y \cdot x = 1.$$

Note que $a^2 - b^2 p$ é sempre diferente de zero já que $a, b \in \mathbb{Q}$. De fato, se $a^2 = b^2 p$ então $a = |b|\sqrt{p}$ ou $a = -|b|\sqrt{p}$ o que é absurdo já que $\sqrt{p}$ é irracional e $a, b \in \mathbb{Q}$. Logo, $a^2 - b^2 p \neq 0$.

Além disso a soma e a multiplicação em $\mathbb{Q}[p]$ são comutativas e associativas. Mais adiante retomaremos esse exemplo, definindo $F[\alpha]$ para F, corpo e $\alpha \in E$, um corpo que contém F.

Definição 5.1: Dois corpos F e E, tais que $F \subset E$, e as operações de adição e multiplicação em F se restringem às correspondentes operações em E, diremos que F é um *subcorpo* de E, ou que E é uma *extensão* de F. Em tal caso, escrevemos $E \mid F$.

Definição 5.2: Seja $E \mid F$ uma extensão de corpos e $\alpha \in E$. Definimos a *adjunção* de α a F como sendo o menor subcorpo de E contendo $F \cup \{\alpha\}$ e o denotamos por $F(\alpha)$. Note que esse corpo é único; Assim, $F \subset F(\alpha) \subset E$ e $\alpha \in F(\alpha)$

Definição 5.3: Dada uma extensão $E \mid F$ e um elemento $\alpha \in E$. Diremos que α é *algébrico sobre* F se α for raiz de um polinômio não nulo $p(x)$ em $F[x]$.

Exemplo 5.1.1: O elemento $\sqrt[5]{4 + \sqrt{7}}$ é algébrico sobre Q.

De fato, denotando este elemento por α e elevando à quinta potência, obtemos

$$\alpha = \sqrt[5]{4 + \sqrt{7}} \Rightarrow \alpha^5 = 4 + \sqrt{7}.$$

Elevando a expressão $\alpha^5 - 4 = \sqrt{7}$ ao quadrado, temos

$$(\alpha^5 - 4)^2 = (\sqrt{7})^2 \Rightarrow \alpha^{10} - 8\alpha^5 + 9 = 0$$

Logo, α é algébrico sobre Q.

Quando α não é algébrico sobre F dizemos que é *transcendente* sobre F. Como exemplo de número transcendente, temos π, transcendente sobre $\mathbb{Q}$.

Na definição abaixo veremos um tipo de polinômio que está incluso em diversas propriedades deste capítulo. Da definição de polinômio mônico, visto no início do Capítulo 3, temos que:

Definição 5.4: Dada uma extensão $E \mid F$ e um elemento $\alpha \in E$ algébrico sobre F, definimos o *polinômio mínimo* de α sobre F como sendo o polinômio mônico de menor grau com coeficientes em F que se anula em α.

Exemplo 5.1.2: Os números $\sqrt[5]{4}$ e $\sqrt[6]{4}$ são algébricos sobre $\mathbb{Q}$, com polinômios mínimos $x^5 - 4$ e $x^6 - 4$, respectivamente.

A partir de um elemento $\alpha \in E$, com $E \mid F$, definimos o conjunto $F[\alpha] = \{f(\alpha) \mid f(x) \in F[x]\}$. Verifica-se que $F[\alpha]$ é um subdomínio de E, observe que em $F[\alpha]$ não há divisores de zero, além disso, $F \subset F[\alpha]$ (basta considerar, na definição de $F[\alpha]$ os polinômios constantes).

Exemplo 5.1.3: Se $\alpha = \sqrt{2} \in E = \mathbb{R}$ é extensão de $F = \mathbb{Q}$, vamos mostrar que $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. De fato, por definição temos

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

Se $f(x) \in \mathbb{Q}$, segue pelo algoritmo da divisão que existe $q(x), r(x) \in \mathbb{Q}[x]$ tais que $f(x) = q(x)(x^2 - 2) + r(x)$, em que $r(x) = a + bx, a, b \in \mathbb{Q}$. E daí,

$$f(\sqrt{2}) = r(\sqrt{2}) = a + b\sqrt{2}, a, b \in \mathbb{Q}.$$

Exemplo 5.1.4: Seja $\alpha = \sqrt[n]{p} \in \mathbb{R}$, ≥ 2 um número primo. Nesse caso α é uma raiz real do polinômio $p(x) = x^n - p$ que é, pelo Teorema 3.5, irredutível sobre $\mathbb{Q}$, então $p(\alpha)$ é o polinômio mínimo de $\sqrt[n]{p}$ sobre $\mathbb{Q}$. Como, $\mathbb{Q}[\alpha]$ é um subdomínio de $\mathbb{R}$ contendo $\mathbb{Q}$ e ainda, se $f(x) \in \mathbb{Q}[x]$ então pelo algoritmo da divisão existe $q(x), r(x) \in \mathbb{Q}[x]$ tais que,

$$f(\alpha) = q(\alpha) \cdot p(\alpha) + r(\alpha) = r(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}.$$

Assim $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbb{Q}\ i = 0, \ldots, n-1\}$. Segue daí que,

$$\begin{aligned}
\mathbb{Q}[\sqrt{7}] &= \{a_0 + a_1\sqrt{7} \mid a_0, a_1 \in \mathbb{Q}\} \\
\mathbb{Q}[\sqrt[3]{7}] &= \{a_0 + a_1\sqrt[3]{7} + a_2(\sqrt[3]{7})^2 \mid a_0, a_1, a_2 \in \mathbb{Q}\} \\
\mathbb{Q}[\sqrt[4]{11}] &= \{a_0 + a_1\sqrt[4]{11} + a_2(\sqrt[4]{11})^2 + a_3(\sqrt[4]{11})^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}.
\end{aligned}$$

Se β é uma raiz cúbica complexa de 7, $\beta \notin \mathbb{R}$, temos que,

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{R},\ \mathbb{Q} \subset \mathbb{Q}[\beta] \subset \mathbb{C}$$

e ainda, $\mathbb{Q}[\sqrt[3]{7}] \approx \mathbb{Q}[\beta]$ pois $\sqrt[3]{7} \in \mathbb{R}$ e $\beta \in \mathbb{C}$ são raízes do mesmo polinômio irredutível $x^3 - 7$ sobre $\mathbb{Q}$ (provaremos isso mais adiante).

As caracterizações do polinômio mínimo estão na proposição a seguir e deixaremos para o leitor a verificação da demonstração em [10].

Proposição 5.1: Sejam $K \mid F$ uma extensão de corpos e $\alpha \in K$. Seja $p(x)$ um polinômio mônico com coeficientes em F, tal que $p(\alpha) = 0$. As seguintes condições são equivalentes:

1. $p(x)$ é o polinômio mínimo de α;

2. se $q(x) \in F[x]$ é tal que $q(\alpha) = 0$, então $p(x)$ divide $q(x)$;

3. $p(x)$ é irredutível.

Note que,

$$F(\alpha) = \left\{ \frac{p(\alpha)}{q(\alpha)}; p(x), q(x) \in F[x] \text{ e } q(\alpha) \neq 0 \right\}.$$

E também, quando $F[a]$ for um corpo então $F[a] = F(a)$. Isto ocorre quando a é algébrico. Por exemplo $Q(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$ e $\mathbb{R}[i] = \mathbb{R}(i)$. O mesmo ocorre para

$$F(\alpha, \beta) = F(\alpha)(\beta) = \left\{ \frac{p(\alpha, \beta)}{q(\alpha, \beta)}; p(x, y), q(x, y) \in F[x, y] \text{ e } q(\alpha, \beta) \neq 0 \right\}.$$

Enunciaremos o teorema abaixo que relaciona polinômios irredutíveis e ideais maximais. A demonstração encontra-se em [7]

Teorema 5.2: Sejam F um corpo e $p(x) \in F[x]$. Então as seguintes condições são equivalentes:

(a) $p(x)$ é irredutível sobre F.

(b) $< p(x) >$ é um ideal maximal em $F[x]$.

(c) $\frac{F[x]}{<p(x)>}$ é um corpo.

Teorema 5.3: Seja F um corpo e $p(x) \in F[x]$ um polinômio irredutível sobre F. Se a é um zero de $p(x)$ em alguma extensão E de F, então $F(a)$ é isomorfo a $\dfrac{F[x]}{< p(x) >}$. E mais, se o grau $p(x) = n$, então todo elemento de $F(a)$ pode ser escrito unicamente na forma

$$c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \ldots + c_1 a + c_0,$$

em que c_0,$c_1, \ldots, c_{n-1} \in F$.

Demonstração. Considere a função ϕ de $F[x]$ para $F(a)$ dada por $\phi(f(x)) = f(a)$. Temos que ϕ é um homomorfismo de anéis. Como $p(a) = 0$ temos que $< p(x) > \subset N(\phi)$. Como $p(x)$ é irredutível sobre F temos que $< p(x) >$ é um ideal maximal de $F[x]$ (veja Teorema 5.2), e sendo $N(\phi) \neq F[x]$ temos que $N(\phi) =< p(x) >$. Pelo teorema fundamental dos homomorfismo teremos

$$\phi(F[x]) \approx \frac{F[x]}{< p(x) >}.$$

Assim concluímos que o subanel $\phi(F[x])$ de $F(a)$ é um corpo. Note que $\phi(F[x]) = F[a]$. Logo,

$$F(a) = F[a] \approx \frac{F[x]}{< p(x) >}.$$

Na segunda parte do teorema os elementos de $\frac{F[x]}{< p(x) >}$ podem ser representados de forma única como

$$c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \ldots + c_1x + c_0 + < p(x) >,$$

em que $c_0, c_1, \ldots, c_{n-1} \in F$. De fato, senão existiria um polinômio de grau menor que n em $< p(x) >= \{p(x)q(x) \mid q(x) \in F[x]\}$. Como $\frac{F[x]}{< p(x) >} \approx F[a]$ temos que $x + < p(x) >$ é levado em a, e então $c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \ldots + c_1x + c_0 + < p(x) >$, é levado em

$$c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \ldots + c_1a + c_0.$$

□

Note que, com as notações do teorema acima,

$F(\alpha) \approx \frac{F[x]}{< p(x) >}$ para α algébrico e $p(x)$ o seu polinômio mínimo.

Assim, se a é uma raiz de $p(x)$ irredutível, então

$$F(a) = F[a] \approx \frac{F[x]}{< p(x) >}.$$

Mas, sempre existe uma extensão de F que possui uma raiz de $p(x) \in F[x]$ irredutível ? O *Teorema de Kronecker* no responde. Leopold Kronecker (1823 - 1891) foi o matemático alemão que se dedicou a teoria dos números, álgebra e lógica.

Teorema 5.4: (*Teorema de Kronecker*) Seja F um corpo e $f(x)$ um polinômio não constante em $F[x]$. Então existe uma extensão E do corpo F no qual $f(x)$ tem um zero (ou raiz).

Demonstração. Seja $F[x]$ um domínio de fatoração única e $p(x)$ um fator irredutível neste domínio. Tomamos $E = \frac{F[x]}{< p(x) >}$. Assim pelo Teorema 5.2 este anel quociente é um corpo. A aplicação ϕ: $F \longrightarrow E$ dada por $\phi(a) = a + < p(x) >$ é um homomorfismo de anéis injetivo. Assim E contém F se identificamos cada elemento a de F com a classe $a + < p(x) >$ de E. Como exemplo $\mathbb{R} \subset \mathbb{C}$.

Suponhamos que

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

Então, em E, $x+ < p(x) >$ é um zero de $p(x)$. De fato,

$$p(x+ < p(x) >) = a_n(x+ < p(x) >)^n + a_{n-1}(x+ < p(x) >)^{n-1} + \ldots + a_0.$$
$$p(x+ < p(x) >) = a_n(x^n+ < p(x) >) + a_{n-1}(x^{n-1}+ < p(x) >) + \ldots + a_0.$$

Usando a identificação de F em E temos

$$p(x+ < p(x) >) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 + < p(x) >= p(x) + < p(x) >= 0 + < p(x) > .$$

□

Exemplo 5.1.5: Seja $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Em $E = \dfrac{\mathbb{Q}[x]}{< x^2 - 2 >}$, $f(x)$ possui raiz pois

$$\begin{aligned} f(x+ < x^2 - 2 >) &= (x+ < x^2 - 2 >)^2 - 2 \\ &= (x^2+ < x^2 - 2 >) - 2 \\ &= x^2 - 2 + < x^2 - 2 >= 0 + < x^2 - 2 > . \end{aligned}$$

Sabemos que a raiz do polinômio $f(x) = x^2 + 1$ é o número complexo $\sqrt{-1}$ mas, o que queremos enfatizar aqui, é uma construção da extensão E que contém $\mathbb{Q}$ e uma raiz de $f(x)$ usando somente o conjunto dos números racionais. Nenhum conhecimento dos números complexos é necessário. Esse método utiliza somente o corpo que é dado. Perceba que, no exemplo acima, $E = \dfrac{\mathbb{Q}[x]}{< x^2 + 1 >} \approx \mathbb{Q}[i]$, o isomorfismo é a aplicação

$$\varphi \colon E \longrightarrow \mathbb{Q}[i] \text{ tal que } \varphi(a) = a \ \forall a \in \mathbb{Q} \text{ e } \varphi(x+ < f(x) >) = i.$$

Exemplo 5.1.6: $Q(\sqrt{2}) \approx \frac{Q[x]}{<x^2-2>} = \mathbb{Q} + \mathbb{Q}\sqrt{2}$.

Exemplo 5.1.7: $\mathbb{R}(\sqrt{-1}) \approx \dfrac{\mathbb{R}[x]}{< x^2 + 1 >} = \mathbb{R} + \mathbb{R}\sqrt{-1} = \mathbb{R} + \mathbb{R}i = \mathbb{C}$

Exemplo 5.1.8: $\mathbb{Q}(\pi) \approx \mathbb{Q}(x) = \left\{ \dfrac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{Q}[x] \text{ e } g(x) \neq 0 \right\}$

Definição 5.5: Sejam F um corpo, $f(x) \in F[x]$ e E um extensão de F. Dizemos que $f(x)$ se *fatora* em E se $f(x)$ se escreve como produto de fatores lineares em $E[x]$.

Definição 5.6: Sejam F um corpo, $f(x) \in F[x]$ e E um a extensão de F. Dizemos que E é *corpo de fatoração* ou de *decomposição* de $f(x)$ sobre F se $f(x)$ se fatora em E e não se fatora em nenhum subcorpo próprio de E.

Denotaremos o corpo de fatoração ou de decomposição de um polinômio $f(x) \in F[x]$ por $Gal(f,E)$.

Exemplo 5.1.9: O polinômio $x^2+1 \in \mathbb{Q}[x]$ se fatora em $\mathbb{C}$, mas $\mathbb{C}$ não é corpo de fatoração x^2+1 sobre $\mathbb{Q}$ pois x^2+1 se fatora em $Q[i] \subset \mathbb{C}$ e $\mathbb{Q}[i] \neq \mathbb{C}$. Note que $Gal(x^2+1, \mathbb{R}) = \mathbb{R}[i] \approx \mathbb{C}$.

Exemplo 5.1.10: $Gal(x^3+x+1, \mathbb{Z}_7) = \mathbb{Z}_7[\alpha] = \mathbb{Z}_7(\alpha) = \{a+b\alpha+c\alpha^2 \mid a,b,c \in \mathbb{Z}_7$ e $\alpha^3+\alpha+1=0\}$.

De fato, para $f(x) \in \mathbb{Z}_7[x]$ e $\alpha \in E \mid \mathbb{Z}_7$ uma raiz de $f(x)$ em E, temos que

$$\begin{aligned} f(x) &= (x-\alpha)(x^2+\alpha x+\alpha^2+1)+\alpha^3+\alpha+1 \\ &= (x-\alpha)(x^2+\alpha x+\alpha^2+1) \\ &= (x-\alpha)(x-6-2\alpha^2)(x-1-6\alpha-5\alpha^2) \end{aligned}$$

Exemplo 5.1.11: $Gal((x^2-3)(x^2-12), \mathbb{Q}) = \mathbb{Q}(\sqrt{3})$.

De fato, seja $Q(\sqrt{3}) = \{a+c\sqrt{3} \mid a,c \in \mathbb{Q}\}$, A raiz do polinômio x^2-3 igual a $\alpha = \pm\sqrt{3} \in \mathbb{Q}(\sqrt{3})$, e ainda, a raiz de x^2-12 igual $\beta = \pm 2\sqrt{3} \in \mathbb{Q}(\sqrt{3})$. Então, $\mathbb{Q}(\sqrt{3})$ é o corpo de fatoração por definição $\mathbb{Q}[\sqrt{3}]$ é o menor corpo que contém $\sqrt{3}$ e $\mathbb{Q}$.

Exemplo 5.1.12: $Gal((x^2-3)(x^2-5), \mathbb{Q}) = Q(\sqrt{3}, \sqrt{5}) = \{c+d\sqrt{3}+m\sqrt{5}+n\sqrt{3}\sqrt{5} \mid a,b,m,n \in \mathbb{Q}\}$.

De fato, note que as raízes são $\alpha = \pm\sqrt{3}$ e $\beta = \pm\sqrt{5}$. Sabemos que o menor corpo que contém $\mathbb{Q}$ e $\sqrt{3}$ é $\mathbb{Q}(\sqrt{3})$ Segue daí que, o menor corpo que contém $\mathbb{Q}(\sqrt{3})$ e $\sqrt{5}$ é

$$\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \{a+b\sqrt{5} \mid a,b \in \mathbb{Q}(\sqrt{3})\}.$$

Como $\mathbb{Q}(\sqrt{3}) = \{c+d\sqrt{3} \colon c,d \in \mathbb{Q}\}$, então, substituindo encontramos o seguinte corpo de fatoração,

$$\mathbb{Q}(\sqrt{3}, \sqrt{5}) = c+d\sqrt{3}+(m+n\sqrt{3})\sqrt{5} = \{c+d\sqrt{3}+m\sqrt{5}+n\sqrt{3}\sqrt{5} \mid a,b,m,n \in \mathbb{Q}\}$$

5.2 Extensões Algébricas

Definição 5.7: Uma extensão E de F é chamada de *extensão algébrica* se todo elemento de E for algébrico sobre F. Se E não for uma extensão algébrica de F dizemos que $E \mid F$ é uma extensão transcendente. Uma extensão E do corpo F da forma $E = F(a)$ para algum $a \in E$ é chamada de extensão simples.

O próximo exemplo mostra que todo número complexo é raiz de algum trinômio do segundo em $\mathbb{R}[x]$.

Exemplo 5.2.1: A extensão $\mathbb{C} \mid \mathbb{R}$ é algébrica.

De fato, se $\alpha = a + bi$, com a,$b \in \mathbb{R}$, então, reagrupando e elevando ao quadrado, temos, $(\alpha - a)^2 = -b^2$, desenvolvendo encontramos

$$\alpha^2 - 2a\alpha + b^2 + a^2 = 0$$

logo, α é raiz de $x^2 - 2ax + b^2 + a^2 \in \mathbb{R}[x]$.

Na Definição 5.4 definimos polinômio mínimo. Usaremos para polinômio mínimo de a sobre F a seguinte notação: $p\,|_{a,F}\,(x)$.

Se $E \mid F$, podemos considerar E espaço vetorial sobre F.

Definição 5.8: A dimensão do espaço vetorial E sobre F será chamada de *grau da extensão* e denotada por $[E : F]$.

Ainda, uma extensão $E \mid F$ será dita *finita*, se E como espaço vetorial sobre F for finito, ou seja, se $[E : F] < \infty$. Caso contrário, dizemos E é uma extensão infinita de F.

Usaremos o seguinte fato para determinarmos o grau de uma extensão. Se a for algébrico sobre F, e se grau $p_{|_{a,F}} = n$ então $\{1,a,a^2,\ldots,a^{n-1}\}$ forma uma base para o espaço $F(a)$ sobre F e $[F(a)\colon F] = n$. Veja o Teorema 5.3.

Exemplo 5.2.2: $\mathbb{C}$ é uma extensão de grau 2 sobre $\mathbb{R}$ pois $\{1,i\}$ forma uma base para o espaço vetorial $\mathbb{C}$ sobre $\mathbb{R}$.

Se $L \mid E$ e $E \mid F$ dizemos que E é extensão intermediária de $L \mid F$.

Teorema 5.5: Se $L \mid E$ e $E \mid F$ são duas extensões finitas, então a extensão $L \mid F$ é finita e

$$[L\colon F] = [L\colon E][E\colon F].$$

Demonstração. Seja $\{\alpha_k; k = 1,\ldots,m\} \subset E$ uma base de $E \mid F$ e seja $\{\beta_j; j = 1,\ldots,n\} \subset L$ uma base de $L \mid E$. Vamos mostrar que o conjunto $\{\alpha_k\beta j; k = 1,\ldots,m$ e $j = 1,\ldots,n\} \subset L$ é uma base de $L \mid F$.

Seja $\beta \in L$. Como $\{\beta_j; j = 1,\ldots,m\}$ gera $L \mid E$, existem $b_j \in E$ tais que

$$\beta = \textstyle\sum_{j=1}^{n} b_j\beta_j.$$

Como $\{\alpha_k; k = 1,\ldots,m\}$ gera $E \mid F$, então, para cada $b_j \in E$ existem $a_kj \in F$ tais que

$$b_j = \textstyle\sum_{k=1}^{m} a_{kj}\alpha_k.$$

Logo,

$$\begin{aligned}\beta = \sum_{j=1}^{n} b_j\beta_j &= \sum_{j=1}^{n}\left(\sum_{k=1}^{m} a_{kj}\alpha_k\right)\beta_j \\ &= \sum_{j=1}^{n}\left(\sum_{k=1}^{m} a_{kj}\alpha_k\beta_j\right) \\ &= \sum_{j=1}^{n}\sum_{k=1}^{m} a_{kj}(\alpha_k\beta_j),\end{aligned}$$

mostrando que $\{\alpha_k\beta_j; k = 1,\ldots,m \text{ e } j = 1,\ldots,n\}$ gera $L \mid F$.

Suponhamos agora que $\sum_{j=1}^{n}\sum_{k=1}^{m} a_{kj}\alpha_k\beta_j = 0$, com $a_kj \in F$. Segue daí que,

$$\sum_{j=1}^{n}\sum_{k=1}^{m} a_{kj}\alpha_k\beta_j = \sum_{j=1}^{n}\left(\sum_{k=1}^{m} a_{kj}\alpha_k\right)\beta_j = 0$$

com $\sum_{k=1}^{m} a_{kj}\alpha_k \in E$, para cada j. Como $\{\beta_j; j = 1,\ldots,n\}$ é linearmente independente sobre E temos que para cada $j = 1,\ldots n$,

$$\sum_{1}^{m} a_{kj}\alpha_k = 0.$$

E como, $\{\alpha_k; k = 1,\ldots,m\}$ é linearmente independente sobre F, obtemos que $a_{kj} = 0$ para cada $k = 1,\ldots,m$.

□

Exemplo 5.2.3: Vamos calcular o grau da extensão $E \mid \mathbb{Q}$ em que $E = Gal(x^3 - 2, \mathbb{Q})$.

Sabemos pelo Capítulo 4 que $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$ no qual ω é uma raiz 3-ésima primitiva da unidade. Se tomarmos $\alpha = \sqrt[3]{2}$ e $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{1}i$ determinamos conforme Exemplo 5.2.1 que

$$p_{|\sqrt[3]{2},\mathbb{Q}}(x) = x^3 - 2 \text{ e que } p_{|\omega,\mathbb{Q}}(x) = x^2 + x + 1.$$

Assim temos,

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \text{ e } [\mathbb{Q}(\omega) : \mathbb{Q}] = 2.$$

Como $\mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2})(\omega)$ é uma extensão simples, para determinar o grau $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})]$, basta sabermos o grau do polinômio mínimo de ω sobre $\mathbb{Q}(\sqrt[3]{2})$. Como ω é raiz de $x^2 + x + 1$ e $\omega \notin \mathbb{Q}(\sqrt[3]{2})$ temos que $x^2 + x + 1$ é irredutível sobre $\mathbb{Q}(\sqrt[3]{2})$ e $p\,|_{\omega,\mathbb{Q}(\sqrt[3]{2})}\,(x) = x^2 + x + 1$. Analogamente, temos que $p\,|_{\sqrt[3]{2},\mathbb{Q}(\omega)}\,(x) = x^3 - 2$. Assim,

$$[\mathbb{Q}(\sqrt[3]{2})(\omega) : \mathbb{Q}(\sqrt[3]{2})] = 2 \text{ e } [\mathbb{Q}(\sqrt[3]{2})(\omega) : \mathbb{Q}(\omega)] = 3$$

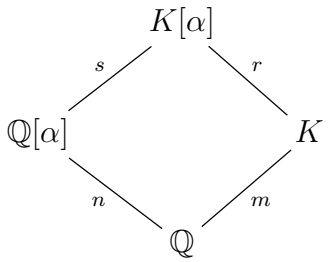
Logo, pelo Teorema 5.5 obtemos

$$[\mathbb{Q}(\sqrt[3]{2})(\omega) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2})(\omega) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6$$

Esse exemplo ilustra corolário seguinte.

Corolário 5.2: Seja $K \subset \mathbb{Q}$ tal que $[K\colon \mathbb{Q}] = m$ e seja $p(x) \in \mathbb{Q}[x]$ um polinômio irredutível sobre $\mathbb{Q}$ de grau n. Se $MDC(m,n) = 1$ então $p(x)$ é um polinômio irredutível sobre K.

Demonstração. Seja $\alpha \in \mathbb{C}$ uma raiz de $p(x)$. Considere agora os corpos $\mathbb{Q}[\alpha] \subset K[\alpha]$ e suponhamos que $[K[\alpha]\colon K] = r$, $[K[\alpha]\colon \mathbb{Q}[\alpha]] = s$. Temos $[\mathbb{Q}[\alpha] : \mathbb{Q}] = n$ e $[K[\alpha] : K] = r = n$. Veja esquema abaixo:



De fato, pelo Teorema 5.5 temos que $n \cdot s = m \cdot r$. Como $MDC(n,m) = 1$ vem $n \setminus r$; mas, $r \leq n$ nos diz que $n = r$ e, assim, $p(x)$ é também irredutível sobre K. □

Finalizaremos este capítulo com o enunciado de algumas propriedades sobre extensões algébricas.

Definição 5.9: Se $E \mid F$ é uma extensão simples, um elemento a tal que $E = F(a)$ é chamado de *elemento primitivo de* E.

Exemplo 5.2.4: Considere a extensão $\mathbb{Q}(\sqrt{3}, \sqrt{5}) \mid \mathbb{Q}$. Essa extensão é simples?

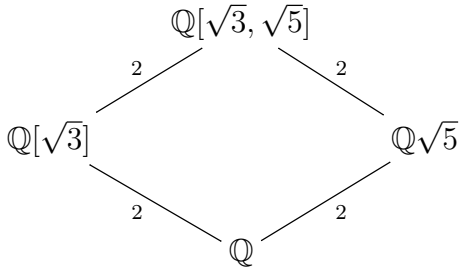
Observe que o fato de $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ não estar escrita como $\mathbb{Q}(c)$ não significa que a extensão não seja simples. Pode existir $c \in \mathbb{Q}(\sqrt{3}, \sqrt{5})$ tal que $\mathbb{Q}(c) \in \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

Temos,

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

E assim,

$$[\mathbb{Q}(\sqrt{3}, \sqrt{5} : \mathbb{Q}] = 4$$



Note que $p_{\sqrt{3},\mathbb{Q}} = x^2 - 3$ e $p_{\sqrt{5},\mathbb{Q}} = x^2 - 5$.

Veja que $\mathbb{Q}(\sqrt{3} + \sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Além disso,

$$(\sqrt{3}, \sqrt{5})^{-1} = \frac{1}{\sqrt{3} + \sqrt{5}} \cdot \frac{\sqrt{3} - \sqrt{5}}{\sqrt{3} - \sqrt{5}} = -\frac{1}{2} \cdot (\sqrt{3} - \sqrt{5}),$$

ainda sabendo que $\sqrt{3}-\sqrt{5}$ deve pertencer a $\mathbb{Q}(\sqrt{3}+\sqrt{5})$ pois ($\mathbb{Q}(\sqrt{3}+\sqrt{5})$ é corpo e contém $(\sqrt{3}-\sqrt{5})^{-1}$).

Assim,

$$\sqrt{3}+\sqrt{5} \in \mathbb{Q}(\sqrt{3}+\sqrt{5}) \text{ e } \sqrt{3}-\sqrt{5} \in \mathbb{Q}(\sqrt{3}+\sqrt{5})$$

Implica que,

$$[(\sqrt{3}+\sqrt{5})+(\sqrt{3}-\sqrt{5})]\cdot\frac{1}{2}=\sqrt{3} \text{ e } [(\sqrt{3}+\sqrt{5})-(\sqrt{3}-\sqrt{5})]\cdot\frac{1}{2}=\sqrt{5}$$

pertencem a $\mathbb{Q}(\sqrt{3}+\sqrt{5})$.

O que garante que $\mathbb{Q}(\sqrt{3},\sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3}+\sqrt{5})$ e, portanto,

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

e a extensão é simples.

O exemplo acima mostra que devemos ter cuidado ao dizer se uma extensão é ou não simples. O teorema a seguir facilitará essa conclusão para corpos de característica zero.

Teorema 5.6: Se F é um corpo de característica 0 e a e b são algébricos sobre F, então existe um elemento c em $F(a,b)$ tal que $F(a,b)=F(c)$.

Corolário 5.3: Seja $K \mid F$ e $F \mid \mathbb{Q}$ tal que $[K\colon F]<\infty$. Então, $\exists\ \alpha \in K$ tal que $K=F[\alpha]$

A demonstração desse teorema poderá ser feita por indução sobre o grau $[K\colon F]<\infty$. Temos então que toda extensão finita de $\mathbb{Q}$ é simples.

Teorema 5.7: Se K é uma extensão algébrica de E e E é uma extensão algébrica de F, então K é uma extensão algébrica de F.

O capítulo seguinte refere-se a teoria de grupos. Essa teoria possui um papel primordial na Teoria de Galois do Capítulo 7, principalmente na resolubilidade de radicais.

6

Grupos

Introduziremos importantes propriedades sobre grupos. O assunto aqui abordado está baseado com [4] e [7].

6.1 Conceitos básicos

Um *grupo* é um conjunto não vazio G munido de uma operação binária (denotaremos por $\cdot$ ou $+$) que satisfaz os seguintes axiomas:

G1. A operação é associativa $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ para todo a,b,$c \in G$;

G2. A operação tem um elemento neutro: existe um elemento $e \in G$, tal que $a \cdot e = e \cdot a = a$, para todo $a \in G$;

G3 Todo elemento de G possui um elemento inverso: para todo $a \in G$, existe um $a' \in G$, tal que $a \cdot a' = a' \cdot a = e$.

Note que a operação $\cdot$ é fechada em G, o elemento neutro e o elemento inverso são únicos.

Quando a operação estiver clara no contexto, denotaremos o grupo $(G, \cdot)$ ou $(G, +)$ simplesmente por G. Também, algumas vezes, denotaremos $a \cdot b$ simplesmente por ab.

Exemplo 6.1.1: Seja $(\mathbb{Z}, +, \cdot)$ o anel dos números inteiros. Então, dos axiomas satisfeitos pela operação de adição, temos que $(\mathbb{Z}, +)$ é um grupo. Com elemento neutro 0 e o inverso aditivo de $a \in \mathbb{Z}$ é o elemento simétrico $-a$. Do mesmo modo, para o anel das classes residuais módulo n $(\mathbb{Z}_n, +, \cdot)$ temos que $(\mathbb{Z}_n, +)$ é um grupo.

Definição 6.1: Se em um grupo $(G, \cdot)$ verifica-se a propriedade:

G4 $a \cdot b = b \cdot a, \forall\ a$,$b \in G$

dizemos que o grupo $(G, \cdot)$ é um *grupo abeliano*.

Definição 6.2: Um grupo G é chamado de *grupo finito* quando G contiver um número finito de elementos. Neste caso, a *ordem* de G, denotada por $|G|$, é o número de elementos de G. Quando G não é um grupo finito, dizemos que G é um *grupo de ordem infinita*, ou seja, isto ocorre quando o grupo G contém infinitos elementos.

O próximo exemplo ajudará a compreendermos o conteúdo abordado no Capítulo 7.

Exemplo 6.1.2: Seja S um conjunto finito não vazio e seja $G = \{f : S \longrightarrow S \mid f \text{ bijetiva}\}$. Se $*$ é a operação composição de funções, isto é,

$$\begin{gathered} * : G \times G \longrightarrow G \\ (g, f) \longrightarrow g \circ f \end{gathered}$$

então $(G, *)$ é um grupo tendo

$$\begin{gathered} I_s : S \longrightarrow S \\ x \longrightarrow x \end{gathered}$$

como identidade.

Esse grupo é chamado de *grupo das Permutações do conjunto* S, cada elemento desse grupo é dito uma permutação. Se $S = \{1,2,\ldots,n\}$ denotaremos esse grupo por S_n, e temos que o número de elementos de S_n é exatamente $n!$.

Agora vejamos o grupo das permutações de 3 elementos: S_3. Representaremos a permutação da seguinte forma:

$$\sigma = \begin{bmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{bmatrix}$$

S_3 é um exemplo de um grupo não abeliano com exatamente $3! = 6$ elementos. O elemento neutro da operação de composição de funções é a identidade. Neste caso, em S_3, o elemento neutro é representado pela permutação

$$I = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$$

Logo S_3 é formado por

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

Se definirmos em S_3 que

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

obtemos,

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \alpha^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I, \beta^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I,$$
$$\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \beta \circ \alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \beta \circ \alpha^2.$$

Portanto, S_3 pode ser escrito como $S_3 = \{I, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$.

Na Tabela 6.1 podemos verificar que S_3 munido da operação de composição de funções, é um grupo não-abeliano finito de ordem 6 e ainda, determinar os pares de elementos inversos.

$\circ$	I	α	α^2	β	$\beta\alpha$	$\beta\alpha^2$
I	I	α	α^2	β	$\beta\alpha$	$\beta\alpha^2$
α	α	α^2	I	$\beta\alpha^2$	β	$\beta\alpha$
α^2	α^2	I	α	$\beta\alpha$	$\beta\alpha^2$	β
β	β	$\beta\alpha$	$\beta\alpha^2$	I	α	α^2
$\beta\alpha$	$\beta\alpha$	$\beta\alpha^2$	β	α^2	I	α
$\beta\alpha^2$	$\beta\alpha^2$	β	$\beta\alpha$	α	α^2	I

Tabela 6.1: Tabela da operação de composição de funções de S_3
Fonte: Elaborada pelo autor

6.2 Subgrupos e grupos cíclicos

Definição 6.3: Sejam $(G, \cdot)$ um grupo e H um subconjunto não-vazio de G. Dizemos que H é um *subgrupo* de G se H, munido da operação $\cdot$ do grupo G, for um grupo, ou seja, se $(H, \cdot)$ for um grupo.

Se H for um subgrupo de G denotamos $H \leq G$.

Dado o grupo G, então $\{e_G\}$ e G são subgrupos de G, chamados subgrupos triviais de G. Se H é um subgrupo de G, diferente de $\{e_G\}$ e G, então dizemos que H é um subgrupo próprio de G.

Exemplo 6.2.1: Considere o grupo $(\mathbb{Z}_4, +)$. Então pela Definição 6.3 o subgrupo próprio de $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ é $H = \{\bar{0}, \bar{2}\}$

Seja $(G, \cdot)$ um grupo e $a \in G$. Denotamos por $< a >$ o conjunto de todas as potências de a, isto é,

$$< a >= \{a^n \mid n \in \mathbb{Z}\}$$

Esse conjunto é um subgrupo de G, chamado de subgrupo gerado por a. No caso de G ser um grupo aditivo, $(G, +)$ as potências de serão os múltiplos de a. O subgrupo gerado por a se escreve como:

$$< a >= \{na \mid n \in \mathbb{Z}\}$$

Exemplo 6.2.2: Dado o grupo $(\mathbb{Z}, +)$, então $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z} =< n >\}$. Tomando $n = 2$ temos, $2\mathbb{Z} =< 2 >$. Note ainda que $\mathbb{Z} =< 1 >$.

Definição 6.4: Um grupo G é chamado grupo *cíclico* se $G =< a >$ para algum $a \in G$, ou seja, G é gerado por um elemento. Neste caso, dizemos que a é um gerador de G.

Em geral o gerador de um grupo G não é único, por exemplo, $\mathbb{Z}_4 =< \bar{1} >$ e $Z_4 =< \bar{3} >$.

Definição 6.5: Seja G um grupo e seja $a \in G$. Se o subgrupo $< a >$ for finito, então dizemos que a *ordem* de a, denotado por $ord(a)$ ou $|< a >|$, é o número de elementos de $< a >$, ou seja, é igual a *ordem* de $< a >$. Agora, se $< a >$ for um grupo infinito, então dizemos que a *ordem* de a é infinita.

Exemplo 6.2.3: Considere o grupo aditivo $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$. A $ord(\bar{0}) = 1, ord(\bar{1}) = 4, ord(\bar{2}) = 2, ord(\bar{3}) = 4$.

De fato, $< \bar{0} >= \{\bar{0}\}, < 1 >= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = \mathbb{Z}_4, < \bar{2} >= \{\bar{0}, \bar{2}\}, < 3 >= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = \mathbb{Z}_4$. Note que o único subgrupo próprio de $\mathbb{Z}_4$ é $H = \{\bar{0}, \bar{2}\}$.

Definição 6.6: Seja G um grupo e H um subgrupo de G. Dado $a \in G$, chamamos de uma *classe lateral* à esquerda ou à direita, respectivamente, aos conjuntos:

$$aH = \{a \cdot h \mid h \in H\} \text{ e } Ha = \{h \cdot a \mid h \in H\}.$$

Se G é um grupo aditivo, então denotamos as classes laterais aH e Ha por

$$a + H = \{a + h \mid h \in H\} \text{ e } H + a = \{h + a \mid h \in H\}$$

Proposição 6.1: Se a função $f : H \longrightarrow aH$ é definida por $f(h) = a \cdot h$, então f é bijetora.

Demonstração. Por definição de aH a $Im(f) = aH$, ou seja, f é sobrejetora. Para provar que é injetora, sejam $x, y \in H$ tais que $f(x) = f(y)$. Segue daí que

$$\begin{aligned} f(x) = f(y) &\Rightarrow a \cdot x = a \cdot y \\ &\Rightarrow a^{-1} \cdot (a \cdot x) = a^{-1} \cdot (a \cdot y) \\ &\Rightarrow (a^{-1} \cdot a) \cdot x = (a^{-1} \cdot a) \cdot y \\ &\Rightarrow x = y \end{aligned}$$

Logo, f é injetora. Portando aH e H têm o mesmo número de elementos, isto é, $|aH| = |H|$. □

Exemplo 6.2.4: Dado o subgrupo $H = \{I, \beta\}$ de $S_3 = \{I, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$, (veja Exemplo 6.1.2), vamos obter elementos $a_1, a_2, \ldots, a_k \in S_3$, tal que $S_3 = a_1H \cup a_2H \cup \ldots \cup a_kH$ seja uma união disjunta.

As classes laterais distintas do subgrupo $H = \{I, \beta\}$ de S_3 são:

$$H = \{I,\beta\}, \alpha H = \{\alpha, \beta\alpha^2\} \text{ e } \alpha^2 H = \{\alpha^2,\beta\alpha\}.$$

Logo, temos $a_1 = I$, $a_2 = \alpha$ e $a_3 = \alpha^2$ e temos que, $S_3 = H \cup \alpha H \cup \alpha^2 H$ é uma união disjunta. Um caso importante é quando $aH = Ha$ para todo $a \in G$. Neste caso, poderemos fazer a construção dos chamados grupos quocientes que são semelhantes aos anéis quocientes. A condição $aH = Ha$ para todo $a \in G$ permitirá definir uma operação binária no conjunto

$$G/H = \{aH \mid a \in G\}$$

das classes laterais que fará deste conjunto um grupo, chamado *grupo quociente*.

Definição 6.7: Seja G um grupo e H um subgrupo de G. Denotamos por

$$G/H = \{aH \mid a \in G\}$$

conjunto das classes *laterais à esquerda com respeito a* H.

Exemplo 6.2.5: Seja G o grupo $(\mathbb{Z}, +)$ e $H = 4\mathbb{Z} = \{4t \mid t \in \mathbb{Z}\}$. A únicas classes laterais à esquerda com respeito a $H = 4\mathbb{Z}$ são $0 + H, 1 + H, 2 + H, 3 + H$.

Logo, $G/H = \{0 + H, 1 + H, 2 + H, 3 + H\}$.

A operação binária em G/H, de modo a torná-lo um grupo, será construída de forma semelhante ao que foi realizado para os anéis quocientes.

Definição 6.8: Seja G um grupo e H um subgrupo de G. Definimos a seguinte operação no conjunto das classes laterais $G/H = \{aH \mid a \in G\}$:

$$a \cdot H = b \cdot H = (ab)H \text{ para todo } aH, bH \in G/H.$$

Para a operação binária estar bem definida em G/H, as classes laterais à esquerda e à direita devem coincidir, ou seja, $aH = Ha$ para todo $a \in G$.

6.3 Subgrupos normais

Nesta seção omitiremos as demonstrações as quais o leitor pode consultar nas bibliografias indicadas neste capítulo. Enunciaremos a seguir que a operação binária em G/N está bem definida.

Proposição 6.2: Sejam G um grupo e N um subgrupo de G, tal que $gN = Ng$ para todo $g \in G$. Se $aN = a_1N$ e $bN = b_1N$, com $a,a_1,b,b_1 \in G$, então,

$$aN \cdot bN = a_1N \cdot b_1N,$$

ou equivalentemente,

$$(ab)N = (a_1b_1)N.$$

Definição 6.9: Um subgrupo N de um grupo G é chamado de um *subgrupo normal* de G quando $gN = Ng$ para todo $g \in G$. Notação $H \trianglelefteq G$.

Vejamos uma caracterização de um subgrupo normal.

Sejam H um subconjunto do grupo G e $a \in G$. Então, definimos o subconjunto aHa^{-1} de G por $aHa^{-1} = \{aha^{-1} \mid h \in H\}$. Segue daí a seguinte proposição.

Proposição 6.3: Sejam G um grupo, H um subgrupo de G e $a \in G$.

(a) aHa^{-1} é um subgrupo de G

(b) $aH = Ha$ se, e somente se, $aHa^{-1} = H$.

Assim temos um critério que facilita na decisão quando um subgrupo N é um subgrupo normal de G.

Proposição 6.4: Sejam G um grupo e N um subgrupo de G. Então N é um subgrupo normal de G, se, e somente se, $gNg^{-1} \subset N$ para todo $g \in G$.

O critério acima também pode ser reescrito da seguinte forma: N é um subgrupo normal de G se, e somente se, $gxg^{-1} \in N$ para todo $x \in N$ e para todo $g \in G$.

Exemplo 6.3.1: Seja G um grupo. Então os subgrupos triviais de G, $N_1 = \{e_G\}$ e $N_2 = G$, são subgrupos normais de G.

Faremos a demonstração para N_1 e deixaremos para o leitor o caso para N_2. Seja $N_1 = \{e_G\} = \{e\}$, como e é o único elemento de N_1, então:

$$g^{-1}eg = g^{-1}g = e \in N_1$$

Logo,

$$gN_1g^{-1} \subset N_1 \text{ para todo } g \in G.$$

Pela Proposição 6.4 $N_1 = \{e_G\}$ é um subgrupo normal de G.

Exemplo 6.3.2: Seja G um grupo abeliano, então todo subgrupo N de G é normal.

De fato, para quaisquer $x \in N$ e $g \in G$ temos que:

$$g^{-1}xg = g^{-1}gx = ex = x \in N.$$

Portanto , temos de modo análogo ao exemplo anterior que $gNg^{-1} \subset N$ para todo G. Assim, N é um subgrupo normal de G.

6.4 Grupo quociente

Teorema 6.1: Sejam G um grupo e N um subgrupo normal de G. Então G/N, munido da operação definida na Definição 6.8, é um grupo. Chamamos este grupo de grupo quociente de G módulo N.

O elemento neutro do grupo será $e_{G/N} = eN = N$ e como elemento inverso aN teremos $(aN)^{-1} = a^{-1}N$.

Demonstração. Como $aN = Na$ para todo $a \in G$ e a operação de G/N está bem definida. Vamos verificar os axiomas de grupo para G/N . A operação é associativa:

$$\begin{aligned} aH \cdot (bN \cdot cN) &= aH \cdot (bc)N \\ &= (a(bc))N \\ &= ((ab)c)N; \text{pela a associatividade em } G \\ &= (ab)N \cdot cN \\ &= (aN \cdot bN) \cdot cN. \end{aligned}$$

O elemento neutro é $eN = N$ com e o elemento neutro de G:

$$\begin{gathered} aN \cdot eN = (ae)N = aN \\ \text{e} \\ eN \cdot aN = (ea)N = aN. \end{gathered}$$

O elemento inverso $aN \in G/N$ é $a^{-1}N$:

$$\begin{gathered} aN \cdot a^{-1}N = (aa^{-1})N = eN \\ \text{e} \\ a^{-1}N \cdot aN = (a^{-1}a)N = eN. \end{gathered}$$

□

O subgrupo H de S_3, dado por $H = \{I, \alpha, \alpha^2\}$ é normal. Basta observamos a Tabela 6.1. Logo,

$$G/H = G/N = \{N, \beta N\}$$

Proposição 6.5: Sejam G um grupo, e N um subgrupo normal de G. Então:

(a) Se G é um grupo abeliano, então o grupo quociente G/N é um grupo abeliano.

(b) Se G é um grupo cíclico, então o grupo quociente G/N é um grupo cíclico.

Demonstração. (a) Sejam aN e bN duas classes laterais de G/N. Temos que

$$\begin{aligned} (aN) \cdot (bN) &= abN, \\ &= baN, \\ &(bN) \cdot (aN). \end{aligned}$$

Portanto, G/N é um grupo abeliano.

(b)Seja G um grupo gerado por $x \in G$. Logo, qualquer elemento G será uma potência x. Afirmamos que a classe lateral xN é gerador de G/N. De fato, se $aN \in G/N$ com $a \in G$, então podemos escrever $a = x^k$ para algum $k \in \mathbb{Z}$. Então,

$$aN = x^kN = (xN)^k, \text{ para algum } k \in \mathbb{Z}.$$

Portanto, G/N é um grupo cíclico. □

Definição 6.10: Definimos o índice de H em G como sendo a cardinalidade de G/H. Denotamos por $[G\colon H]$.

Se o índice $[G\colon H] = n$, temos que $G/H = \{x_1H, x_2H, \ldots, x_nH\}$ para $x_i \in G$.

Exemplo 6.4.1: Se $n \in \mathbb{Z}$, então o subgrupo $n\mathbb{Z} = \{nt \mid t \in \mathbb{Z}\}$ é um subgrupo normal do grupo aditivo $\mathbb{Z}$. E que existem n classes laterais $n\mathbb{Z}$ em $\mathbb{Z}$.

Seja as n classes laterais $n\mathbb{Z}$ em $\mathbb{Z}$ iguais a $0+n\mathbb{Z}, 1+n\mathbb{Z}, 2+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}$. Como o grupo aditivo $\mathbb{Z}$ é cíclico gerado pelo elemento 1, temos que o grupo quociente $\mathbb{Z}/nZ$ também é cíclico e é gerado pela classe lateral $1+n\mathbb{Z}$. Sendo um grupo cíclico de ordem n, temos que $\mathbb{Z}/nZ$ e $\mathbb{Z}_n$ são isomorfos, veremos o motivo na próxima seção. As vezes por abuso de linguagem escrevemos $\mathbb{Z}/nZ = \mathbb{Z}_n$

Enunciaremos um importante teorema, conhecido por *Teorema de Lagrange*. Veja demonstração em [7].

Teorema 6.2: Se G é um grupo finito e H é um subgrupo de G então $|G| = |H| \cdot [G\colon H]$.

Corolário 6.1: Se G é finito e $H \leq G$, então $|H|$ divide $|G|$.

6.5 Homomorfismo de grupos

Pela Definição 2.12, temos que um homomorfismo de anéis é um função entre dois anéis que preserva as operações destes anéis. Da mesma forma temos que o homomorfismo de grupos é um função entre dois grupos que preserva as operações destes grupos. Assim:

Definição 6.11: Sejam G e H grupos e $f\colon G \longrightarrow H$ uma função. Dizemos que f é um *homomorfismo de grupos* quando

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

Note que a operação em $f(x \cdot y)$ é a do grupo G, enquanto a operação em $f(x) \cdot f(y)$ é a operação do grupo H e que f preserva as operações dos grupos G e H.Quando estiver claro no contexto, também denotaremos da seguinte forma:

$$f(xy) = f(x)f(y) \ \forall \ x, y \in G.$$

Definição 6.12: Se um homomorfismo $f\colon G \longrightarrow H$ for bijetivo dizemos que f é um *isomorfismo* (de grupos) e nesse caso dizemos que G é *isomorfo* a H e denotamos por $G \approx H$.

Um isomorfismo $f\colon G \longrightarrow G$ diz-se um *automorfismo* de G. Denotaremos por *Aut* G o conjunto dos automorfismos de G.

Corolário 6.2: Se G é um grupo e $f_1, f_2 \in$ *Aut* G então:

(a) $f_1 \circ f_2 \in Aut\ G$

(b) $f_1^{-1} \in Aut\ G$, em que f_1^{-1} é a função inversa de f_1

Demonstração. Para o item (a) temos,

$$(f_1 \circ f_2)(xy) = f_1(f_2(xy)) = f_1(f_2(x) \cdot f_2(y)) = f_1(f_2(x)) \cdot f_1(f_2(y)) = (f_1 \circ f_2)(x) \cdot (f_1 \circ f_2)(y)\ \forall\ x, y \in G,$$

como a composição $f_1 \circ f_2$ de funções é também bijetiva temos, $f_1 \circ f_2 \in Aut\ G$.

No item (b) temos, se $f_1 \in Aut\ G$ então $\forall\ x', y' \in G$ existem $x, y \in G$ tais que

$$x' = f_1(x) \text{ e } y' = f_1(y).$$

Logo, se $h = f_1^{-1}$ temos,

$$h(x', y') = h(f_1(x) \cdot f_2(x)) = h(f_1(xy)) = (h \circ f_1)(xy) = xy = h(x') \cdot h(y'),$$

como $h = f_1^{-1}$ é uma função inversa de f_1, por hipótese, temos $f_1^{-1} = h \in Aut\ G$. □

Assim, $(Aut\ G, \circ)$ é um grupo.

Definição 6.13: O *núcleo* de um homomorfismo de grupos $f\colon G \longrightarrow H$ é o conjunto

$$N(f) = \{x \in G \mid f(x) = e_H\},$$

no qual e_H é o elemento neutro do grupo H.

Exemplo 6.5.1: Sejam $G = (\mathbb{R}, +)$ o grupo aditivo dos números reais e $H = (\mathbb{R}_+^*, \cdot)$ o grupo multiplicativo dos números reais positivos. Consideremos a função $f\colon G \longrightarrow H$ definida por

$$f(x) = 2^x \quad \forall\ x \in \mathbb{R}$$

Seja x,$y \in \mathbb{R}$ temos,

$$f(x + y) = 2^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y).$$

Logo, f é um homomorfismo. Já que a função exponencial $f(x) = 2^x$ é bijetiva em $\mathbb{R}$ e $\mathbb{R}_+^*$, então f é um isomorfismo de grupos. Como em $e_H = 1$ temos

$$f(x) = 1 \Leftrightarrow 2^x = 1 \Leftrightarrow x = 0 = e_G$$

Então o núcleo de f é $N(f) = \{0\}$.

A demonstração da proposição seguinte encontra-se para verificação em [4] e [7]. Provaremos (a) e (b) e deixaremos para o leitor a consulta dos outros itens.

Proposição 6.6: Se $f\colon G \longrightarrow H$ um homomorfismo de grupos. Então,

(a) $f(e_G) = e_H$

(b) $f(a)^{-1} = f(a^{-1})$

(c) Se N é um subgrupo de G, então $f(N)$ é um subgrupo de H. Em particular $Im(f) = f(G)$ é um subgrupo de H.

(d) $N(f)$ é um subgrupo normal de G.

(e) f é injetora se, e somente se, $N(f) = \{e_G\}$.

(f) Se f for bijetora, então, $f^{-1}\colon H \longrightarrow G$ será um homomorfismo de grupos.

Demonstração. Em (a) temos,

$$\begin{aligned} f(e_G) &= f(e_G \cdot e_G) \\ &= f(e_G) \cdot f(e_G) \end{aligned}$$

Multiplicando ambos os lados da equação $f(e_G) = f(e_G) \cdot f(e_G)$ por $f(e_G)^{-1}$, obtemos,

$$\begin{aligned} f(e_G) \cdot f(e_G)^{-1} &= (f(e_G) \cdot f(e_G)) \cdot f(e_G)^{-1}; \\ f(e_G) \cdot f(e_G)^{-1} &= f(e_G) \cdot (f(e_G) \cdot f(e_G)^{-1}) \end{aligned}$$

Como $f(e_G) \cdot f(e_G)^{-1} = e_H$. Obtemos,

$$\begin{aligned} f(e_G) \cdot f(e_G)^{-1} &= f(e_G) \cdot (f(e_G) \cdot f(e_G)^{-1}) \\ e_H &= f(e_G) \cdot e_H \\ e_H &= f(e_G) \\ f(e_G) &= e_H \end{aligned}$$

Para o item (b), sabemos que $f(a) \cdot f(a)^{-1} = e_H$. Então,

$$\begin{aligned} f(a) \cdot f(a^{-1}) &= f(a \cdot a^{-1}) \\ &= f(e_G) \\ &= e_H; \text{pelo item (a)} \end{aligned}$$

Analogamente $f(a^{-1}) \cdot f(a) = e_H$. Assim, pela unicidade do elemento neutro, $f(a)^{-1} = f(a^{-1})$. □

Exemplo 6.5.2: Sejam G um grupo e $g \in G$. Considere a aplicação $i_g\colon G \longrightarrow G$ definida por $i_g(x) = gxg^{-1}$. Temos que i_g é um isomorfismo do grupo G nele mesmo, ou seja, um automorfismo do grupo G.

Inicialmente verificaremos o homomorfismo de grupos de i_g. Dados a,$b \in G$, temos

$$\begin{aligned} i_g(a,b) &= g(ab)g^{-1} \\ &= g(ae_gb)g^{-1} \\ &= g(ag^{-1}gb)g^{-1} \\ &= (gag^{-1})(gbg^{-1}) \\ &= i_g(a) \cdot i_g(b). \end{aligned}$$

Portanto, i_g é um homomorfismo de grupos. Verificaremos que i_g é sobrejetora. Dado $b \in G$ queremos encontrar $a \in G$ tal que $i_g(a) = b$, ou seja, queremos que $gag^{-1} = b$. Suponhamos que seja verdadeiro que $gag^{-1} = b$. Logo,

$$\begin{aligned} gag^{-1} = b \Rightarrow \\ (g^{-1}g)ag^{-1} = g^{-1}b \Rightarrow \\ (g^{-1}g)a(g^{-1}g) = g^{-1}bg \Rightarrow \\ e_Gae_G = g^{-1}bg \Rightarrow \\ a = g^{-1}bg \end{aligned}$$

Tomando $a = g^{-1}bg$ temos,

$$\begin{aligned} i_g(a) &= i_g(g^{-1}bg) \\ &= gg^{-1}bgg^{-1} \\ &= (gg^{-1})b(gg^{-1}) \\ &= e_Gbe_G = b. \end{aligned}$$

Portanto, i_g é sobrejetora.
Por último, para verificar que i_g é injetora, vamos calcular seu núcleo. Então,

$$\begin{aligned} a \in N(i_g) &\Leftrightarrow i(a) = i_G \\ &\Leftrightarrow gag^{-1} = e_G \\ &\Leftrightarrow ga = e_Gg = g; \text{mutiplicando a direita por } g \\ &\Leftrightarrow a = g^{-1}g; \text{multipliando a esquer por } g^{-1} \\ &\Leftrightarrow a = e_G. \end{aligned}$$

Por ser $N(i_g) = \{e_G\}$ e pela Proposição 6.6 segue i_g ser injetora. Assim, como $i_g \colon G \longrightarrow G$ é um homomorfismo bijetor, temos que i_g é um automorfismo G.

Veremos abaixo importante exemplo que está relacionado com o teorema do homomorfismo de grupos.

Exemplo 6.5.3: Sejam G um grupo e H um subgrupo normal de G. Considere a

aplicação entre G e o grupo quociente G/H, $\pi\colon G \longrightarrow G/H$, definida por $\pi(a) = aH$. Vamos verificar que π é um homomorfismo de grupo.

Dados a,$b \in G$, temos

$$\begin{aligned}\pi(a \cdot b) &= (a \cdot b)H \\ &= aH \cdot bH \\ &= \pi(a) \cdot \pi(b)\end{aligned}$$

Portanto, π é um homomorfismo de grupos, chamado homomorfismo canônico.

Proposição 6.7: Sejam G um grupo e H um subgrupo normal de G. Seja $\pi\colon G \longrightarrow G/H$, $\pi(a) = aH$, o homomorfismo canônico. Então,

(a) π é um homomorfismo sobrejetor;

(b) $N(\pi) = H$.

Demonstração. Para o item (a). Seja $aH \in G/H$, $a \in G$, um elemento arbitrário do quociente G/H. Logo, da própria definição de homomorfismo canônico, temos que $\pi(a) = aH$, segue daí que π é sobrejetor.

Para o item (b), temos:

$$\begin{aligned}&a \in N(\pi) \Leftrightarrow \pi(a) = e_{G/H} \\ &\Leftrightarrow \pi(a) = H; \text{pois } e_{G/H} = e_G H = H. \\ &\Leftrightarrow aH = H; \text{pois } \pi(a) = aH \\ &\Leftrightarrow a \in H.\end{aligned}$$

Portanto, $N(\pi) = H$.

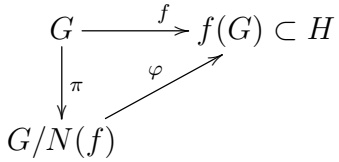
□

É importante ressaltar que, se H é um subgrupo normal do grupo G, diferente do subgrupo trivial $\{e_G\}$, então, o homomorfismo canônico $\pi : G \longrightarrow G/H$ não é uma função injetora.

Finalizaremos este capítulo com importantes propriedades. A demonstração das mesmas encontram-se em [7] para consulta do leitor. Iniciaremos com o teorema conhecido como *Teorema do Homomorfismos para Grupos*, Proposição 6.8.

Proposição 6.8: Dado um homomorfismo de grupos $f : G \longrightarrow H$, então existe um isomorfismo de grupos $\varphi\colon G/N(f) \longrightarrow f(G)$ que satisfaz $f\colon \varphi \circ \pi$, no qual $\pi\colon G \longrightarrow G/N(f)$ é o homomorfismo canônico.

Representamos esse resultado pelo seguinte esquema:



$$G/N(f) \approx f(G).$$

Corolário 6.3: Sejam G um grupo finito e $f: G \longrightarrow H$ um homomorfismo de grupos. Então, $|f(G)|$ é um divisor de $|G|$.

O teorema abaixo é também conhecido por *Teorema da Representação*.

Teorema 6.3: Se G um grupo e H um subgrupo de G de índice $[G : H] = n$. Então, $\exists\ N \subseteq H$, com N subgrupo normal de G tal que G/N é um grupo isomorfo a um subgrupo do grupo S_n. Mais ainda, N é o 'maior' subgrupo normal em G que está contido em H.

Por último, apresentaremos como corolário do Teorema 6.3, *O Teorema de Cayley*. Arthur Cayley (1821 - 1895), matemático britânico, foi professor da Universidade Cambridge. Para demonstrar o corolário abaixo devemos tomar $H = \{e\}$ no enunciado do Teorema 6.3.

Corolário 6.4: Se G é um grupo ordem $|G| = n$ então G é isomorfo a um subgrupo do grupo S_n.

Exemplo 6.5.4: Temos para o grupo aditivo $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ que $|\mathbb{Z}_4| = 4$ então $\mathbb{Z}_4$ é isomorfo a um subgrupo do grupo S_4,

6.5.1 Grupos Solúveis

Apresentaremos agora uma definição importante no estudo de solubilidade de radicais.

Definição 6.14: Um grupo G diz-se *solúvel* se existem subgrupos $\{e\} = G_0 \leq G_1 \leq G_2 \leq \ldots \leq G_{n-1} \leq G_n = G$ tais que:

(a) G_{i-1} é um subgrupo normal $G_i \quad \forall\ i \in \{1,2,\ldots,n\}$

(b) G_i/G_{i-1} é abeliano $\quad \forall\ i \in \{1,2,\ldots,n\}$

Proposição 6.9: (a) Todo subgrupo de um grupo solúvel é solúvel.

(b) Todo quociente de um grupo solúvel é solúvel.

(c) Sejam G um grupo e N um subgrupo normal de G. Então, G/N solúvel e N solúvel implica que G solúvel.

Exemplo 6.5.5: Vamos verificar que S_3 é solúvel.

Temos que $\langle(123)\rangle$ é um subgrupo normal de G de ordem 3. Basta tomarmos

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

Então, encontraremos que conforme Exemplo 6.1.2 e Definição 6.9, o subgrupo normal de G de ordem 3 é $S_3 = \{I, \alpha, \alpha^2\}$ e a cadeia

$$\{e\} \leq \langle(123)\rangle \leq S_3.$$

Logo é solúvel. E ainda $S_3/\langle(123)\rangle$ é abeliano de ordem 2 e $\langle(123)\rangle/\{e\} = \langle(123)\rangle$ é abeliano, grupo cíclico.

Proposição 6.10: O grupo S_n, $n \geq 5$, não é solúvel.

A demonstração acima encontra-se em [7].

No capítulo seguinte introduziremos as noções elementares da teoria de Galois. Iniciaremos o estudo com o grupo de Galois de uma extensão e finalizaremos com a correspondência de Galois entre subgrupos do grupo de Galois e corpos intermediários.

7

Introdução a Teoria de Galois

Neste capítulo focaremos extensões finitas tais que $\mathbb{Q} \subset F \subset K \subset \mathbb{C}$. Todas extensões $F \subset K$ serão consideradas subcorpos de $\mathbb{C}$ contendo $\mathbb{Q}$. As propriedades e definições deste capítulo estarão em consonância com [3], [7], [14] e [19].

7.1 Grupo de Galois

Enunciaremos dois teoremas que serão chamados de *Teoremas de Extensão*. Sendo $\phi(p(x))$ o polinômio obtido de $p(x)$ aplicando o isomorfismo ϕ a todos coeficientes de $p(x)$, ou seja, $\phi(p(x)) = \phi(a_0) + \phi(a_1)x + \ldots + \phi(a_n)x^n$.

Teorema 7.1: Sejam F um corpo, $p(x) \in F[x]$ irredutível sobre F, e seja a um zero de $p(x)$ em alguma extensão de F. Se ϕ é um isomorfismo de F em F_1 e b é um zero de $\phi(p(x))$ em alguma extensão de F_1, então existe um isomorfismo de $F(a)$ em $F_1(b)$, o qual coincide com ϕ em F e leva a em b.

Teorema 7.2: Sejam ϕ um isomorfismo de um corpo F para um corpo F_1 e $f(x) \in F[x]$. Se K é um corpo de fatoração de $f(x)$ sobre F e K_1 é um corpo de fatoração de $\phi(f(x))$ F_1, então existe um isomorfismo de K em K_1, o qual é igual a ϕ em F.

Retomando que todo polinômio $p(x)$ definido num corpo F possui todas as suas raízes em uma extensão K de F; o corpo de fatoração de $p(x)$ sobre F, o qual é o menor corpo que contém F e todas as raízes de $p(x)$ e este corpo é obtido através de adjunções de raízes de $p(x)$.

Para caracterizar as raízes de $p(x)$, Galois conseguiu fazer uma correspondência entre as extensões do tipo $F(\sqrt[n]{\alpha})$ com subgrupos de um grupo, grupo este que nada mais é que o grupo das permutações das raízes do polinômio.

Definição 7.1: Sejam $p(x) \in F[x]$ um polinômio definido no corpo F e K o corpo de fatoração de $p(x)$ sobre F. O *Grupo de Galois* de $p(x)$ sobre F é o grupo $Aut_F(K)$ dos $F - automorfismo$ de K, isto é, automorfismos de K, que quando restritos a F são a identidade.

Como consequência dos teoremas de extensão, temos que o corpo de fatoração é único. E ainda temos a primeira ligação, (Corolário 7.1), da teoria de corpos com a teoria de grupos feita por Galois.

Corolário 7.1: Seja $f(x) \in F[x]$, e seja K um corpo de fatoração de $f(x)$ sobre F. Se ϕ: $K \longrightarrow K$ é um $F - automorfismos$ de K e α é uma raiz de $f(x)$, então $\phi(\alpha)$ também é uma raiz de $f(x)$.

Demonstração. Seja $f(x) = a_0 + a_1x + \ldots + a_nx^n$. Logo,

$$f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0.$$

Aplicando ϕ, obtemos

$$\begin{aligned} 0 = \phi(0) =& \phi(a_0) + \phi(a_1)\phi(\alpha) + \ldots + \phi(a_n)\phi(\alpha)^n \\ =& a_0 + a_1\phi(\alpha) + \ldots + a_n\phi(\alpha)^n \\ =& f(\phi(\alpha)) \end{aligned}$$

Logo, $F - automorfismo$ levam raízes de p em raízes de p. □

O enunciado do Corolário 7.1 poderia ser reescrito da seguinte forma. Se $f(x) \in F$ e K é seu corpo de fatoração sobre F, então todo $F - automorfismo$ de K permuta as raízes de $f(x)$.

Se σ e τ são dois automorfismo de K, extensões da identidade em F, então a composição $\sigma \circ \tau$ também é um automorfismo de K. Dessa maneira, a composição define uma operação em Aut_FK.

O isomorfismo identidade em K é uma extensão da identidade em F. E, se $\sigma \in Aut_FK$ então $\sigma(c) = c \ \forall \ c \in F$. Aplicando o isomorfismo inverso σ^{-1} a ambos termos da igualdade obtém-se:

$$\begin{aligned} \sigma(c) &= c \\ \Rightarrow \sigma^{-1}(\sigma(c)) &= \sigma^{-1}(c) \\ \Rightarrow \sigma^{-1} \circ \sigma(c) &= \sigma^{-1}(c) \\ \Rightarrow c &= \sigma^{-1}(c) \end{aligned}$$

Logo, Aut_FK é fechado em relação a inversos.

Definição 7.2: Se α é algébrico sobre um corpo F, os *conjugados* de α são todas as raízes do polinômio mínimo $p_{|_{\alpha,F}} \in F[x]$

Definição 7.3: Um extensão algébrica $K \mid F$ de corpos é chamada de *extensão normal* se para todo $\alpha \in K$, os conjugados de α pertencem a K.

Exemplo 7.1.1: Note que $\mathbb{Q}(\sqrt[3]{2})$ não é um extensão normal de $\mathbb{Q}$ pois não contém todos os conjugados de $\sqrt[3]{2}$, isto é, não contém as raízes complexas não reais de $\sqrt[3]{2}$. Já a extensão $\mathbb{Q}(\sqrt[3]{2}, w)$, com w a 3-ésima raiz primitiva da unidade, é normal a $\mathbb{Q}$.

Outros exemplos de extensões normais podem ser obtidos por meio do corolário a seguir:

Corolário 7.2: Seja $E \mid F$ um extensão finita. K é corpo de fatoração de algum polinômio $f(x) \in F[x]$ se e somente se para todo $\alpha \in K$, $p_{|_{\alpha,F}}$ se fatora em fatores lineares em K, isto é, $K \mid F$ é uma extensão normal.

Um fato que precisamos nos preocupar é com as raízes múltiplas que podem aparecer no polinômio, pois não teremos permutações das raízes. No entanto, quando um corpo possui característica 0, por exemplo os racionais, ele não terá raízes múltiplas.

Definição 7.4: (a) Sejam F um corpo e $f(x) \in F[x]$, $f(x)$ irredutível. Dizemos que $f(x)$ é *separável sobre* F se no seu corpo de fatoração, f ter todas as suas raízes distintas.

(b) Se $f(x) \in F[x]$ for redutível, $f(x)$ é *separável sobre* F se todas os seus fatores irredutíveis forem separáveis.

(c) Se $K \mid F$ é um extensão algébrica de corpos e $\alpha \in K$, dizemos que é α *separável sobre* F se $p_{|_{\alpha,F}}$ for separável, isto é, todos os conjugados de α são distintos.

Temos, então, dois fatos interessantes. São eles: em um corpo de característica zero, todo polinômio irredutível é separável e todo polinômio irredutível $f(x) \in F[x]$, sendo F um corpo finito é separável.

Segue abaixo algumas importantes propriedades que envolvem a relação entre o grau da extensão e a ordem de grupo. As demonstrações omitidas encontra-se nas bibliografias indicadas para consulta do leitor.

Corolário 7.3: Seja $K \mid F$ e $F \mid \mathbb{Q}$ tal que $[K\colon F] < \infty$. Então, $[K\colon F] \geq |Aut_F K|$ em que $|Aut_F K|$ denota o número de elementos do grupo $Aut_F K$.

Demonstração. Como $[K\colon F] < \infty$ existe $\alpha \in K$ tal que $K = F[\alpha]$. Se

$$\sigma \in Aut_F K \text{ e } p(x) = p_{|_{\alpha,F}}$$

Segue do Corolário 7.1 que $\alpha' = \sigma(\alpha)$ é também raiz de $p(x)$, $\alpha' \in K$. Mas, $F[\alpha'] \subset K$ e $[F[\alpha'] : F] = [K\colon F]$ e igual ao grau de $p(x) = p_{|_{\alpha,F}}$. Isso diz que

$$K = F[u] = F[u'].$$

Como $\sigma(a) = a$ para todo $a \in F$ σ fica completamente determinado pelo valor $\alpha' = \sigma(\alpha)$. Assim o número $|Aut_F K|$ é no máximo igual ao número de raízes α' de $p(x)$ que pertencem a K. Esse número é no máximo o grau do polinômio

$$p(x) = p_{|_{\alpha,F}} = [K\colon F].$$

□

Definição 7.5: Dizemos que uma extensão finita $K \mid F$ é uma *extensão galoisiana* se $\exists f(x) \in F[x]$ tal que $K = Gal(f,F)$ e, ainda,

A extensão $K = Gal(f,F)$ é normal e separável. Este fato segue imediatamente do Corolário 7.2.

Para continuarmos nossos estudos vejamos, ainda, alguns corolários dos teoremas de extensão apresentados no início desta seção.

Corolário 7.4: Se $F \subset K$ galoisiana então:

1. $[K : F] =\mid Aut_F K \mid$
2. Se $\alpha \in K - F$, $\exists\ \sigma \in Aut_F K$ tal que $\sigma(\alpha) \neq \alpha$

O teorema abaixo descreve que se $K = Gal(f,F)$ no qual F é um corpo de característica zero então $[K\colon F] = |Aut_F K|$.

Teorema 7.3: Se $K \mid F$ um extensão finita. Então as seguintes condições são equivalentes:

(1) $K \mid F$ galoisiana;

(2) $K \mid F$ normal;

(3) Para todo $\alpha \in K - F$ $\exists\ \sigma \in Aut_F K$ tal que $\sigma(\alpha) \neq \alpha$;

(4) $[K : F] = |Aut_F K|$

Demonstração. (1) $\Rightarrow$ (2): segue imediatamente do Corolário 7.2.

(2) $\Rightarrow$ (3): segue imediatamente dos Corolários 7.2 e 7.4.

Para (3) $\Rightarrow$ (4): Sabemos do Corolário 7.3 que $[K : F] \geq |Aut_F K|$. Suponhamos (3) e por absurdo que $[K : F] > |Aut_F K|$. Suponha que $Aut_F K$ tenha n elementos, $Aut_F K = \{\theta_1 = I_K, \theta_2, \ldots, \theta_n\}$ no qual I_K representa o automorfismo identidade em K. Se $[K : F] > n$, existem $n+1$ vetores, $u_1, \ldots, u_n, u_{n+1} \in K$, LI sobre o corpo F.

Consideremos agora o seguinte sistema linear homogêneo com n equações e $(n+1)$

incógnitas a_1,a_2,$\ldots$ a_{n+1} em K:

$$(*)\begin{cases}\theta_1(u_1)a_1+\theta_1(u_2)a_2+\ldots+\theta_1(u_j)a_j+\ldots\theta_1(u_n)a_n+\theta_1(u_{n+1})a_{n+1}=0\\ \theta_2(u_1)a_1+\theta_2(u_2)a_2+\ldots+\theta_2(u_j)a_j+\ldots\theta_2(u_n)a_n+\theta_2(u_{n+1})a_{n+1}=0\\ \quad\cdot\\ \quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\\ \quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\\ \theta_i(u_1)a_1+\theta_i(u_2)a_2+\ldots+\theta_i(u_j)a_j+\ldots\theta_i(u_n)a_n+\theta_i(u_{n+1})a_{n+1}=0\\ \quad\cdot\\ \quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\\ \quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\\ \theta_n(u_1)a_1+\theta_n(u_2)a_2+\ldots+\theta_n(u_j)a_j+\ldots\theta_n(u_n)a_n+\theta_n(u_{n+1})a_{n+1}=0\end{cases}$$

Como o número de equações de $(*)$ é menor que o número de incógnitas então $(*)$ admite uma solução a_1,a_2,$\ldots$, a_{n+1} não trivial. Consideremos uma solução não trivial de $(*)$ com o maior número de zeros possível e denotaremos os $a_i's$ não nulos dessa solução por a_1,a_2,$\ldots$, a_r. Podemos assumir $a_1=1$ (se necessário multiplicamos por a_1^{-1}). Assim, 1,a_2,a_3,$\ldots$,a_r são não nulos tais que $1,a_2,\ldots,a_r,0,\ldots,0$ é uma solução de $(*)$ com um número máximo de zeros.

Então temos,

$$\forall\ i\in\{1,2,\ldots,n\},\ \theta_i(u_1)+\theta_i(u_2)a_2+\ldots+\theta_i(u_r)a_r=0.$$

Como $\theta_1=I_K$ e $u_1,\ldots,u_r,\ldots,u_{n+1}$ são LI sobre F, segue que existe $a_i\in K$ tal que $a_i\notin F$. Seja $a_r\notin F$. Assim, por (c) temos que existe $\sigma\in Aut_FK$ tal que

$$\sigma(a_r)\neq a_r.$$

Logo, para todo $i\in\{1,\ldots,n\}$

$$(\sigma\circ\theta_i)(u_1)+(\sigma\circ\theta_i)(u_2)\sigma(a_2)+\ldots+(\sigma\circ\theta)(u_r)\sigma(a_r)=0$$

Como Aut_FK é um grupo e $\sigma\in Aut_FK$, segue imediatamente que

$$Aut_FK=\{\theta_1,\theta_2,\ldots,\theta_n\}=\{\sigma\theta_1,\sigma\theta_2,\ldots,\sigma\theta_n\}$$

portanto se $\sigma\theta_i=\theta_F$, teremos para todo $F\in\{1,\ldots,n\}$,

$$\theta_k(u_1)+\theta_k(u_2)\sigma(a_2)+\ldots+\theta_k(u_r)\sigma(a_r)=0$$

Daí segue que para todo $j\in\{1,\ldots,n\}$

$$\theta_j(u_2)(\sigma(a_2)-a_2)+\ldots+\theta_j(u_r)(\sigma(a_r)-a_r)=0$$

.

O que nos dá uma solução para $(*)$. Mas como $\sigma(a_r) - a_r \neq 0$, essa solução é não trivial, e possui mais zeros do que a solução escolhida anteriormente. Isso resulta em um absurdo.

(4) $\Rightarrow$ (1): Seja $K = F[u]$. Tomando $h(x) = irr(u,F)$, então

$$\forall \quad \sigma \in Aut_F K \text{ tem-se } \sigma(u) \text{ é raiz de } h(x).$$

Logo, $|Aut_F K|$ é menor ou igual ao número de raizes de $h(x)$ em K.

Se $[K : F] = |Aut_F K|$ então $|Aut_F K|$ é igual ao grau de $h(x)$ e, portanto, igual ao número de raizes de $h(x)$ em K. Daí segue que K contém todas as raizes de $h(x)$, ou seja,

$$K = Gal(h, F).$$

□

Proposição 7.1: Se $K \mid F$ é uma extensão galoisiana de grau n, então $G = Aut_F K$ é isomorfo a um subgrupo de S_n.

Demonstração. Sejam $K = F[\alpha], p(x) = p_{|_{\alpha,F}}, [K\colon F]$=grau $p(x) = n$, e $R = \{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n\}$ o conjunto de todas as raízes complexas de $p(x)$. Como $K \mid F$ galoisiana temos

$$R \subset K.$$

Sabemos também que para todo $\sigma \in G = Aut_F K$ e para $\alpha_i \in R$ tem -se $\sigma(\alpha_i) \in R$. Como R é um conjunto finito e σ é injetiva segue que

$$\sigma_0 = \sigma \mid_R \colon R \longrightarrow R$$

Isso define uma permutação do conjunto R. Se $P(R)$ denota o grupo das permutações do conjunto R então é suficiente provarmos que G é isomorfo a um subgrupo de $P(R)$ pois $P(R) \approx S_n$. Assim temos a seguinte função Ψ que define um homomorfismo de grupos pois $(\sigma \circ \tau) \mid_R = \sigma \mid_R \cdot \tau \mid_R$.

$$\begin{aligned} \Psi\colon G &\longrightarrow P(R) \\ \sigma &\longrightarrow \sigma_0 = \sigma|_R \end{aligned}$$

Mais ainda, se $\sigma_0 = \sigma \mid_R = I_R$ identidade em R segue que $\sigma(\alpha) = \alpha$ e isto nos diz que $\sigma = I_K$ pois para $b \in K, b = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$, no qual $a_i \in F$ e para todo $\sigma \in G = Aut_F K$ tem-se:

$$\sigma(b) = a_0 + a_1\sigma(\alpha) + \ldots + a_{n-1}\sigma(\alpha)^{n-1} = a_0 + \ldots + a_{n-1}\alpha^{n-1} = b$$

Portanto Ψ é injetiva; logo, temos $G \approx \Psi(G)$ e $\Psi(G)$ é subconjunto de $P(R)$.

□

Para determinarmos $Aut_F K$ seguiremos as seguintes afirmações:

1. Seja K uma extensão de um corpo F e $f(x) \in F[x]$. Se $\alpha \in K$ é raiz de $f(x)$ e $\sigma \in Aut_F K$ então $\sigma(\alpha)$ é também raiz de $f(x)$.

2. Sendo K o corpo de fatoração da raízes de $f(x) \in F[x]$ sobre F e sejam $\alpha, \beta \in K$. Então, existe $\sigma \in Aut_F K$ tal que $\sigma(\alpha) = \beta$ se e somente se α e β tem o mesmo polinômio mínimo.

3. Para $K = F(\alpha_1 \dots \alpha_n)$ uma extensão algébrica sobre F. Se $\sigma, \tau \in Aut_F K$ e $\sigma(\alpha_i) = \tau(\alpha_i)$, para todo, $i = 1,2,\dots,n$ então $\sigma = \tau$. Ou seja, um automorfismo em $Aut_F K$ é completamente determinado pelas imagens de $\alpha_1 \dots \alpha_n$.

4. Se K é um corpo de raízes de um polinômio separável $f(x) \in F[x]$ de grau n então $Aut_F K$ é isomorfo à um subgrupo de S_n.

Exemplo 7.1.2: O Grupo de Galois de $\mathbb{C}$ sobre $\mathbb{R}$.

Sabemos que $\mathbb{C} = \mathbb{R}(i)$. Em seguida, determinamos os polinômios mínimos de cada gerador, neste caso, $p_{|_{i,\mathbb{R}}}$. Seguiremos afirmações acima para determinarmos $Aut_{\mathbb{R}}\mathbb{C}$. Logo,

$$\begin{aligned}
&\sigma \in Aut_{\mathbb{R}}\mathbb{C} \\
&\Leftrightarrow \sigma(i) \text{ é raiz de } x^2 + 1 \\
&\Leftrightarrow \sigma(i) = i \text{ ou } \sigma(i) = -i.
\end{aligned}$$

Assim, só podem existir no máximo dois $F - automorfismos$ de $\mathbb{C}$, isto é, $|Aut_{\mathbb{R}}\mathbb{C}| \leq 2$.

Como i e $-i$ são raízes do mesmo polinômio mínimo, temos a existência de

$$\tau, \sigma \in Aut_{\mathbb{R}}\mathbb{C}, \text{ tal que, } \sigma(i) = i \text{ e } \tau(i) = -i.$$

Um elemento $\sigma \in Aut_{\mathbb{R}}\mathbb{C}$ fica completamente determinado pelas imagens dos geradores da extensão, neste caso pela imagem de i. De fato, para todo $z = a+bi \in \mathbb{C}$, temos:

$$\sigma(z) = \sigma(a + bi) = \sigma(a) + \sigma(bi) = \sigma(a) + \sigma(b)\sigma(i) = a + bi$$

pois por definição $\sigma(c) = c$ se $c \in \mathbb{R}$ e $\sigma(i) = i$ por construção. Portanto, $\sigma = \iota$ a identidade em $\mathbb{C}$. E ainda,

$$\tau(z) = \tau(a + bi) = \tau(a) + \tau(bi) = \tau(a) + \tau(b)\tau(i) = a - bi.$$

Assim, τ é a aplicação conjugação em $\mathbb{C}$.

Como, $|Aut_{\mathbb{R}}\mathbb{C}| \leq 2$ e $\{\iota, \tau\} \subset Aut_{\mathbb{R}}\mathbb{C}$ segue que $Aut_{\mathbb{R}}\mathbb{C} = \{\iota, \tau\}$

Por fim, o grupo de Galois do corpo de raízes de um polinômio separável de grau n é um subgrupo de S_n . Neste caso, temos o isomorfismo entre $Aut_{\mathbb{R}}\mathbb{C}$ e S_2. Definido por

$$\begin{aligned}\phi\colon Aut_{\mathbb{R}}\mathbb{C} &\longrightarrow S_2\\ \iota &\longrightarrow \iota\\ \tau &\longrightarrow (1,2);(1,2) \text{ representa o ciclo.}\end{aligned}$$

Exemplo 7.1.3: O grupo de Galois de $\mathbb{Q}(\sqrt{p},\sqrt{q})$ sobre $\mathbb{Q}$ para p,q primos.

A extensão está na forma finitamente gerada. Porém, com dois geradores. Sejam os polinômios mínimos dos geradores $p_{|_{\sqrt{p},\mathbb{Q}}}(x) = x^2 - p$, com raízes $\sqrt{p}$ e $-\sqrt{p}$, e ainda, $p_{|_{\sqrt{p},\mathbb{Q}}}(x) = x^2 - q$, com raízes $\sqrt{q}$ e $-\sqrt{q}$.

Como $\sqrt{p}$ e $-\sqrt{p}$ são raízes do mesmo polinômio mínimo. Do mesmo modo para $\sqrt{q}$ e $-\sqrt{q}$, temos a existência de 4 possíveis elementos de $Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q})$,

$$\iota,\sigma_1,\sigma_2,\sigma_3 \in Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q})$$

tal que,

$$\iota(\sqrt{p}) = \sqrt{p} \text{ e } \iota(\sqrt{q}) = \sqrt{q}$$

$$\sigma_1(\sqrt{p}) = \sqrt{p} \text{ e } \sigma_1(\sqrt{q}) = -\sqrt{q}$$

$$\sigma_2(\sqrt{p}) = -\sqrt{p} \text{ e } \sigma_2(\sqrt{q}) = \sqrt{q}$$

$$\sigma_3(\sqrt{p}) = -\sqrt{p} \text{ e } \sigma_3(\sqrt{q}) = -\sqrt{q}$$

Determinaremos agora $\iota,\sigma_1,\sigma_2,\sigma_3$. Seja,

$$I_{\mathbb{Q}(\sqrt{p})} : \mathbb{Q}(\sqrt{p}) \longrightarrow \mathbb{Q}(\sqrt{p})$$

em que $I_{\mathbb{Q}(\sqrt{p})}$ denota a identidade em $\mathbb{Q}(\sqrt{p})$. Como $p_{|_{\sqrt{q},\mathbb{Q}(\sqrt{p})}}(x) = p_{|_{-\sqrt{q},\mathbb{Q}(\sqrt{p})}}(x) = x^2 - q$, segue que o isomorfismo identidade $I_{\mathbb{Q}(\sqrt{p})}$ estende-se à um isomorfismo,

$$\phi\colon \mathbb{Q}(\sqrt{p},\sqrt{q}) \longrightarrow \mathbb{Q}(\sqrt{p},-\sqrt{q}) \text{ que fixa os elementos de } \mathbb{Q}(\sqrt{p})$$

é tal que $\phi(\sqrt{q}) = -\sqrt{q}$. Como ϕ fixa os elementos de $\mathbb{Q}(\sqrt{p})$, em particular fixa cada elemento em $\mathbb{Q}$. Deste modo, $\phi \in Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q})$. Façamos $\sigma_1 = \phi$.

Para σ_2 é análogo. Por último o σ_3. Seja, $p_{|_{\sqrt{p},\mathbb{Q}}} = p_{|_{-\sqrt{p},\mathbb{Q}}} = x^2 - p$, implica que existe um isomorfismo

$$\xi\colon \mathbb{Q}(\sqrt{p}) \longrightarrow \mathbb{Q}(-\sqrt{p})$$

extensão da identidade que leva $\sqrt{p}$ em $-\sqrt{p}$. Do mesmo modo, $p_{|_{\sqrt{q},\mathbb{Q}(\sqrt{p})}}(x) = p_{|_{-\sqrt{q},\mathbb{Q}(\sqrt{p})}}(x) = x^2 - q$, implica a existência de um isomorfismo

$$\sigma_3\colon \mathbb{Q}(\sqrt{p},\sqrt{q}) \longrightarrow \mathbb{Q}(-\sqrt{p},-\sqrt{q})$$

extensão de ξ que leva $\sqrt{q}$ em $-\sqrt{q}$. Então, do mesmo modo que σ_1, temos que σ_3 é um elemento de $Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q})$. Portanto, $|Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q})| \leq 4$ e existem quatro elementos distintos $\iota,\sigma_1,\sigma_2,\sigma_3$ em $Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q})$. Segue que,

$$Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q}) = \{\iota, \sigma_1, \sigma_2, \sigma_3\}.$$

Como $\mathbb{Q}(\sqrt{p},\sqrt{q})$ é o corpo de raízes do polinômio separável $(x^2-p)(x^2-q)$. Pelo grau ser 4, segue que $Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q})$ é isomorfo à um subgrupo de S_4.

Vejamos como montar um tal isomorfismo. Primeiro, estabeleça uma bijeção entre os conjunto das quatro raízes distintas de $(x^2-p)(x^2-q)$ com o conjunto {1,2,3,4} ou seja,

$$\begin{aligned}\sqrt{p} &\longleftrightarrow 1\\ \sqrt{q} &\longleftrightarrow 2\\ -\sqrt{p} &\longleftrightarrow 3\\ -\sqrt{q} &\longleftrightarrow 4\end{aligned}$$

Assim, podemos relacionar um elemento do grupo $Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q})$ como uma permutação em {1,2,3,4} de acordo com sua ação em $\sqrt{p}$ e $\sqrt{q}$. Para σ_1 temos em notação de permutação:

$$\begin{pmatrix} \sqrt{p} & \sqrt{q} & -\sqrt{p} & -\sqrt{q} \\ \sqrt{p} & -\sqrt{q} & -\sqrt{p} & \sqrt{q} \end{pmatrix}$$

ou, equivalentemente, segundo correspondência biunívoca adotada:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

Em notação de ciclos temos (24). Logo determinamos a seguinte correspondência:

$$\begin{aligned}\iota &\longrightarrow (1)\\ \sigma_1 &\longrightarrow (2,4)\\ \sigma_2 &\longrightarrow (1,3)\\ \sigma_3 &\longrightarrow (1,3)(2,4)\end{aligned}$$

Assim, podemos construir as tabelas 7.1 e 7.2 de operações de composição do grupo $Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q})$

$\circ$	ι	σ_1	σ_2	σ_3
ι	ι	σ_1	σ_2	σ_3
σ_1	σ_1	ι	σ_3	σ_2
σ_2	σ_2	σ_3	ι	σ_1
σ_3	σ_3	σ_2	σ_1	ι

Tabela 7.1: Tabela de operações de composição do grupo $Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q})$
Fonte: elaborada pelo autor

$\circ$	e	θ_1	θ_2	θ_3
e	e	θ_1	θ_2	θ_3
θ_1	θ_1	e	θ_3	θ_2
θ_2	θ_2	θ_3	e	σ_1
θ_3	θ_3	θ_2	θ_1	e

Tabela 7.2: Tabela de operações de composição do subgrupo H
Fonte: elaborada pelo autor

Fazendo as identificações $(1) = e, (2,4) = \theta_1, (1,3) = \theta_2$, e $(2,4)(1,3) = \theta_3$. Então temos o subrupo $H = \{(1),(2,4),(1,3),(2,4)(1,3))\} = \{e, \theta_1, \theta_2, \theta_3\}$ de S_4. Logo, a tabela de operações de composição do subgrupo H é um isomorfismo.

Segue, pela análise das tábuas de operações do grupo $Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{p}, \sqrt{q})$ e do subgrupo H que a aplicação

$$\Psi\colon Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{p}, \sqrt{q}) \longrightarrow H$$

definida po $\iota \longrightarrow (1), \sigma_1 \longrightarrow (2,4), \sigma_2 \longrightarrow (1,3), \sigma_3 \longrightarrow (1,3)(2,4)$ é um isomorfismo.

7.2 A correspondência de Galois

Considere as seguintes definições:

Definição 7.6: Subgrupo de $Aut_F K$ associado à um corpo intermediário E:

$$\Gamma(E) = Aut_E K = \{\text{automorfismos de } K \text{ que fixam } E\}$$

Definição 7.7: Corpo intermediário associado à um subgrupo H de $Aut_F K$:

$$\Phi(H) = \{x \in K\colon \sigma(x) = x, \text{ para todo } \sigma \in H\ \}$$

De fato, temos $0, 1 \in \Phi(H)$ e mais:

1 se $x, y \in E$ então $\sigma(x - y) = \sigma(x) - \sigma(y) = x - y, \forall \sigma \in H$.

2 se $x, y \in E$ então $\sigma(xy) = \sigma(x) \cdot \sigma(y) = xy, \forall \sigma \in H$.

3 se $x \in Ex \neq 0$ então $\sigma(x^{-1}) = \sigma(x)^{-1} = x^{-1}, \forall \sigma \in H$.

Como $H \leq Aut_F K$ segue imediatamente que $\Phi(H)$ é um corpo, $F \subset \Phi(H) \subset K$. O corpo $\Phi(H)$ é chamado *corpo fixado* de H.

De acordo com as associações acima, fica bem definida a correspondência:

$$\{\text{Corpos intermediários de F} \subset K\} \longleftrightarrow \{\text{Subgrupos de } Aut_F K\}$$
$$E \xrightarrow{\Gamma} Aut_E K$$
$$\Phi(H) \xleftarrow{\Phi} H$$

A correspondência assim definida é conhecida como a *correspondência de Galois da extensão $K \mid F$.*

Observemos algumas propriedades elementares dessas correspondências.

a $\Gamma(K) = Aut_K K = \{I_K\} = \{e_K\} = \{e\}$;

b $\Phi(I_M) = \{a \in K : I_M(a) = a\} = K$;

c $\Gamma(F) = Aut_F K$;

d $\Phi(Aut_F K) = \{a \in K : \sigma(a) = a \forall \sigma \in Aut_F K\} \supseteq F$ e pelo Teorema 7.3 temos ainda que

$$\Phi(Aut_F K) = F \Leftrightarrow K \mid F \text{ é galoisiana.}$$

Proposição 7.2: Seja $E(K,F) = \{E : \text{corpo intermediário de } K \mid F\}$. Mantendo as outras notações desta seção, temos

i se $E_1, E_2 \in E(K,F)$ e $E_1 \subseteq E_2$ então $\Gamma(E_2) \leq \Gamma(E_1)$;

ii se $H_1, H_2 \in Aut_F K$ e $H_1 \leq H_2$ então $\Phi(H_1) \supseteq \Phi(H_2)$;

iii $\forall E \in E(K,F)$ tem-se $(\Phi \circ \Gamma)(E) \supseteq E$;

iv $\forall H \in Aut_F K$ tem-se $H \leq (\Gamma \circ \Phi)(H)$.

Demonstração. (a) Seja $E_1, E_2 \in E(K,F)$ e $E_1 \subset E_2$. Então, $\Gamma(E_2) = Aut_{E_2} K \leq Aut_{E_1} K = \Gamma(E_1)$.

(b) Sejam $H_1, H_2 \in Aut_F K$ e $H_1 \leq H_2$. Então,

$$\Phi(H_2) = \{a \in K : \sigma(a) = a \forall \sigma \in H_2\} \subseteq \{a \in K : \sigma(a) = a \forall \sigma \in H_1\} = \Phi(H_1).$$

(c) Seja $E \in E(K,F)$. Como $\Gamma(E) = Aut_E K$ a inclusão $E \subseteq (\Phi \circ \Gamma)(E)$ segue das definições de Γ e Φ.

(d) Seja $H \in Aut_F K$. Se $N = \Phi(H) = \{x \in K : \sigma(x) = x \forall \in \sigma \in H\}$ então segue imediatamente que $H \leq Aut_N K = \Gamma(\Phi(H))$.

Segue da proposição acima que

$$F \subseteq E_1 \subseteq E_2 \subseteq K \text{ e } I_M \leq H_2 \leq H_1 \leq G = Aut_F K.$$

□

Exemplo 7.2.1: Seja $Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \{\iota, \sigma_1, \sigma_2, \sigma_3\}$, veja Exemplo 7.1.3. Determinaremos o corpo fixado $\Phi(H)$ do subgrupo $< \sigma_1 >= \{\iota, \sigma_1\}$.

Por definição

$$\Phi(H) = \{x \in K : \sigma(x) = x, \text{ para todo } \sigma \in H \ \}.$$

Como ι é o isomorfismo identidade então fixa todo o corpo $\mathbb{Q}(\sqrt{p}, \sqrt{q})$. Assim, basta determinarmos os elementos de $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ fixados por σ_1. Seja $\{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$ uma base de $\mathbb{Q}(\sqrt{p}, \sqrt{q})$, veja Exemplo 5.1.12. Assim, todo elemento $x \in \mathbb{Q}(\sqrt{p}, \sqrt{q})$ pode ser escrito na forma:

$$x = a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq}$$

para únicos $a, b, c, d \in \mathbb{Q}$. Então $\sigma_1(x) = x$ se, e somente se,

$$\begin{aligned} a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} &= \sigma_1(a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq}) \\ &= \sigma_1(a) + \sigma_1(b)\sigma_1(\sqrt{p}) + \sigma_1(c)\sigma_1(\sqrt{q}) + \sigma_1(d)\sigma_1(\sqrt{pq}). \end{aligned}$$

Sabemos que $\sigma_1(k) = k$ para todo $k \in \mathbb{Q}$, $\sigma_1(\sqrt{p}) = \sqrt{p}$ e $\sigma_1(\sqrt{q}) = -\sqrt{q}$. Então,

$$\begin{aligned} a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} &= \sigma_1(a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq}) \\ &= \sigma_1(a) + \sigma_1(b)\sigma_1(\sqrt{p}) + \sigma_1(c)\sigma_1(\sqrt{q}) + \sigma_1(d)\sigma_1(\sqrt{pq}) \\ &= a + b\sqrt{p} - c\sqrt{q} + d\sigma_1\sqrt{p}\sigma_1\sqrt{q} \\ &= a + b\sqrt{p} - c\sqrt{q} + d\sqrt{p}(-\sqrt{q}) \\ &= a + b\sqrt{p} - c\sqrt{q} - d\sqrt{p}\sqrt{q} \end{aligned}$$

Pela unicidade da expressão de um elemento com respeito à uma base, temos $\sigma_1(x) = x$ se, e somente se, $a = a, b = b, c = -c$ e $d = -d$ se, e somente se, $c = d = 0$. Portanto, $\sigma_1(x) = x$ se, e somente se,

$$x = a + b\sqrt{p} + 0\sqrt{q} + 0\sqrt{pq} = a + b\sqrt{p}.$$

Implica que $x \in \mathbb{Q}(\sqrt{p})$. Logo, $\Phi(< \sigma_1 >) = \mathbb{Q}(\sqrt{p})$.

Para o subgrupo $< \sigma_2 >= \{\iota, \sigma_2\}$ subgrupo simples gerado por σ_2. De maneira análogo a $< \sigma_1 >$. Temos que, $b = d = 0$. Assim,

$$\Phi(< \sigma_2 >) = \{a + c\sqrt{q} : a,c \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{q}).$$

Em σ_3 temos que

$$\sigma_3(\sqrt{pq}) = \sigma_3(\sqrt{p})\sigma_3\sqrt{q} = (-\sqrt{p})(-\sqrt{q}) = \sqrt{pq}.$$

Assim, para o subgrupo $< \sigma_3 >= \{\iota, \sigma_3\}$ obtemos

$$\begin{aligned} a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} &= \sigma_3(a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq}) \\ &= \sigma_3(a) + \sigma_3(b)\sigma_3(\sqrt{p}) + \sigma_3(c)\sigma_3(\sqrt{q}) + \sigma_3(d)\sigma_3(\sqrt{pq}) \\ &= a - b\sqrt{p} - c\sqrt{q} + d\sigma_1\sqrt{p}\sigma_1\sqrt{q} \\ &= a - b\sqrt{p} - c\sqrt{q} + d\sqrt{pq} \end{aligned}$$

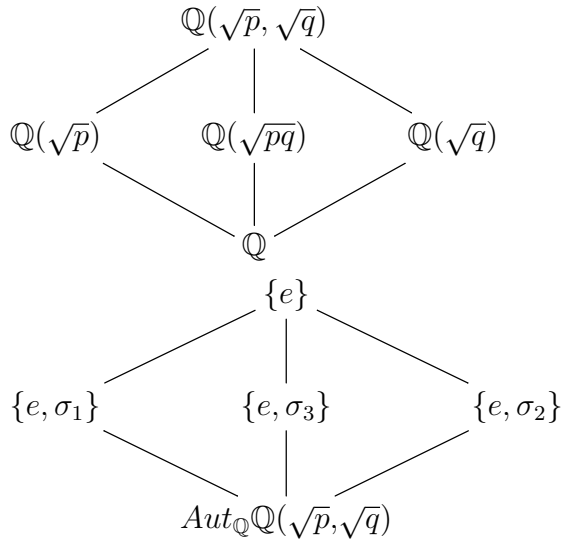
se, e somente se, $b = c = 0$. Portanto $\Phi(< \sigma_3 >) = \{a + d\sqrt{pq} : a,d \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{pq})$.

Por último, $\Phi(Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q})) = \mathbb{Q}$ já que $Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q})$ é galoisiana e por definição de grupo de Galois.

Portanto, podemos representar a seguinte correspondência

$$\begin{array}{rl} \text{Subgrupos} & \text{Corpos fixados} \\ \{e\} & \longleftrightarrow \mathbb{Q}(\sqrt{p},\sqrt{q}) \\ <\sigma_1> & \longleftrightarrow \mathbb{Q}(\sqrt{p}) \\ <\sigma_2> & \longleftrightarrow \mathbb{Q}(\sqrt{q}) \\ <\sigma_3> & \longleftrightarrow \mathbb{Q}(\sqrt{pq}) \\ Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q}) & \longleftrightarrow \mathbb{Q} \end{array}$$

Na linguagem de reticulado, no qual subcorpos e subgrupos se correspondem de acordo com suas respectivas posições.



7.2.1 O Teorema Fundamental da Teoria de Galois

Nesta seção continuaremos com as noções elementares da teoria de Galois. Focaremos em extensões finitas tais que $\mathbb{Q} \subset F \subset K \subset \mathbb{C}$. Todas extensões $F \subset K$ serão consideradas subcorpos de $\mathbb{C}$ contendo $\mathbb{Q}$. As propriedades e definições deste capítulo estarão em consonância com [3], [7], [14] e [19].

O teorema fundamental da teoria de Galois mostra que a correspondência de Galois, vista na Seção 7.2 é biunívoca quando a extensão é finita, normal e separável, ou seja, uma extensão galoisiana finita. Do mesmo modo que anteriormente as demonstrações omitidas encontra-se na bibliografia indicada.

Em relação a sobrejetividade temos as seguintes propriedades.

Lema 7.1: Se $F \subset K$ é finita então K é simples, normal e separável sobre o corpo fixado de qualquer subgrupo H de $Aut_F K$.

Teorema 7.4: Se $F \subset K$ é finita então $H = \Gamma(\Phi(H))$ e $|H| = [K : \Phi(H)]$ para todo subgrupo H de $Aut_F K$.

Como consequência do Teorema 7.4 temos que a correspondência de Galois é sobrejetiva para extensões finitas.

Para a injetividade temos as seguintes propriedades.

Lema 7.2: Seja $F \subset E \subset K$ extensões corpos. Se K é galoisiana sobre F então K é galoisiana sobre E.

Porém E não é necessariamente galoisiana sobre F, como mostra o exemplo $K = Gal(x^3 - 2,\mathbb{Q})$, $E = \mathbb{Q}[\sqrt[3]{2}]$ e $F = \mathbb{Q}$.

Teorema 7.5: Se $F \subset K$ é uma extensão galoisiana, então $E = \Phi(\Gamma(E))$ para todo corpo intermediário E.

Como consequência do Teorema 7.5, temos que correspondência de Galois é injetiva para extensões de galoisianas.

Corolário 7.5: Seja K uma extensão finita sobre F. Então,

$$K \text{ é galosiana sobre } F \Leftrightarrow F = \Phi(Aut_F K)$$

A demonstração do teorema abaixo encontra-se em [7].

Teorema 7.6: Se $F \subset L \subset K$ são extensões finitas e $F \subset K$ é Galoisiana, então as seguintes afirmações são equivalentes:

(a) $K \supset L$ galoisiana

(b) $\sigma(L) \subseteq L \forall \sigma \in Aut_F K$

(c) $Aut_L K \trianglelefteq Aut_F K$.

Para a proposição abaixo considere as notações $F \subset L \subset K$, $\mathcal{E}(K,F) = \{L :$ corpo intermediário de $K \mid F\}$ e $\mathcal{S}(G) = \{H : H$ subgrupo de $G\}$.

Proposição 7.3: Temos:

a) Se $L_1, L_2 \in \mathcal{E}(K,F)$ e $L_1 \subseteq L_2$ então $\Gamma(L_1) \geq \Gamma(L_2)$.

b) Se H_1, $H_2 \in \mathcal{S}(G)$ e $H_1 \leq H_2$, então $\varphi(H_1) \supseteq \varphi(H_2)$.

c) Para todo $L \in \mathcal{E}(K,F)$ tem-se $(\varphi \circ \Gamma)(L) \supseteq L$.

d) Para todo $H \in \mathcal{S}(G)$ tem-se $(\Gamma \circ \varphi)(H) \geq H$.

Demonstração. Para provar o item (a), sejam $L_1, L_2 \in \mathcal{E}(K,F)$ e $L_1 \subset L_2$. Então

$$\Gamma(L_1) \;=\; Gal_{L_1}K \geq Gal_{L_2}K \;=\; \Gamma(L_2).$$

Já para o item (b), sejam $H_1, H_2 \in \mathcal{S}(G)$ e $H_1 \leq H_2$. Então

$$\begin{aligned} \varphi(H_2) &= \{a \in M \mid \sigma(a) = a \;\forall\; \sigma \;\in H_2\} \\ &\subseteq \{a \in M \mid \sigma(a) = a \;\forall\; \sigma \;\in H_1\} \\ &= \varphi(H_1) \end{aligned}$$

Tomando $L \in \mathcal{E}(K,F)$, temos $\Gamma(L) = Gal_L K$ e o item (c) segue imediatamente das definições.

Agora, para o item (d) tome $H \in \mathcal{S}(G)$. Chamado $N = \varphi(H) = \{a \in M \mid \sigma(a) = a \ \forall \ \sigma \in H\}$, segue imediatamente que $H \leq Gal_N K = \Gamma(\varphi(H))$. $\square$

Teorema 7.7: *(Teorema Fundamental de Galois).* Se $K \mid F$ é uma extensão galoisiana, $Aut_F K = G$, $\mathcal{E}(K,F) = \{L :$ corpo intermediário de $K \mid F\}$ e $\mathcal{S}(G) = \{H : H$ subgrupo de $G\}$ então:

(a) $\forall\ L \in E(K,F)$ tem-se $[K : L] = |\Gamma(L)|$ e $[L : F] = [G : \Gamma(L)]$(o índice de $\Gamma(L)$ em G);

(b) $\forall H \in \mathcal{S}(G)$ tem-se $[K : \Phi(H)] = |H|$ e $[\Phi(H) : E] = [G : H]$ (o índice de H em G);

(c) $\Gamma \circ \Phi = I_{\mathcal{S}(G)}$ e $\Phi \circ \Gamma = I_{\mathcal{E}(K,F)}$

(d) $\forall\ L \in E(K,F), L \mid F$ galoisiana $\Leftrightarrow \Gamma(L) = Aut_L K \trianglelefteq G$.

(e) Seja $L \in E(K,F)$. Se $L \mid F$ galoisiana então $[L : F] = |Aut_F L|$ e $G/\Gamma(L) \approx Aut_K L$

Demonstração. No item (a). Seja $L \in \mathcal{E}(K,F)$, $F \subset L \subset K$. Mas, $K \supset F$ implica que $K \mid F$ é galoisiana pelo Teorema 7.3 segue que:

$$[K : L] = |Aut_L K| = |\Gamma(L)|$$

e como $[K : F] = |Aut_F K| = [K : L] \cdot [L : F]$ temos que :

$$|G| = [K : L] \cdot [L : F] = |\Gamma(L)| \cdot [L : F]$$

e daí vem que $[L : F] = [G : \Gamma(L)]$.

Em (b) provaremos primeiro a segunda parte, que segue imediatamente da primeira parte, pois dado $H \leq G$ e $L = \varphi(H)$ e por $|G| = [K : F] = [K : \varphi(H)][\varphi(H) : F]$, temos que

$$[\varphi(H) : F] = [G : H]$$

segue do Teorema de Lagrange (já que $[K : \varphi(H)] = |H|$).

Agora, para provar que $[K : \varphi(H)] = |H|$, seguiremos o mesmo argumento utilizado no Teorema 7.3 item 4. Pelo item (a) temos que

$$[[K : L] = |\Gamma(L)| \text{ em que } L = \varphi(H)]$$

dessa forma $[K : \varphi(H)] = |\Gamma(\varphi(H))|$ que sabemos, pela Proposição 7.3, $[M : \phi(H)] \geq |H|$. Suponhamos por absurdo que

$$[[K : \varphi(H)] > |H|]$$

e suponhamos que H tenha n elementos, $H = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$. Como $[K : \varphi(H)] = [K : L] > |H|$, a dimensão de K como espaço vetorial sobre L é maior que n, logo existem $(n+1)$ vetores $u_1, u_2, \ldots, u_n, u_{n+1}$ vetores LI sobre $L = \varphi(H)$.

De modo totalmente análogo ao que fizemos no Teorema 7.3 item 4, temos uma contradição e concluímos que

$$[K : \phi(H)] = |H|.$$

Em (c)temos, seja $H \in Aut_F K$ e $L \in E[K,F]$. Sabemos da proposição pela Proposição 7.2 que:

$$H \leq \Gamma(\Phi(H)) \text{ e } L \leq \Phi(\Gamma(L)).$$

Pelo item (a), temos: $[G\colon \Gamma(\Phi(H))] = [\Phi(H)\colon F]$ e pelo item (b), temos: $[\Phi(H)\colon F] = [G\colon H]$. Daí segue imediatamente que

$$[G\colon \Gamma(\Phi(H))] = [G\colon H] \text{ e } \Gamma(\Phi(H)) = H.$$

Analogamente, pelo item (b): $[K\colon \Phi(\Gamma(L))] = |\Gamma(L)|$ e pelo item (a) temos $|\Gamma(L)| = [K\colon L]$. Logo,

$$[K\colon \Phi(\Gamma(L))] = [K\colon L] \text{ e } \Phi \circ (\Gamma(L)) = L.$$

O item (d) é consequência imediata do Teorema 7.6.

Em (e) temos, pelo item (a) sabemos que $[G\colon \Gamma(L)] = [L\colon F]$ portanto é suficiente provarmos que: $\forall L \in E[K,F], L \mid F$ galoisiana implica que:

$$G/\Gamma(L) \approx Aut_F L$$

De fato, com $L \mid F$ galoisiana sabemos do Teorema 7.6 que, $\forall\ \sigma \in G$ tem-se $\sigma_0 = \sigma_{|_L} \in Aut_F L$, portanto podemos definir a seguinte função:

$$\begin{aligned} \xi : G &\longrightarrow Aut_F L \\ \sigma &\longrightarrow \sigma_0 = \sigma_{|_L} \end{aligned}$$

como ξ é um homomorfismo de grupos, cujo núcleo $N(\xi) = \{\sigma \in G\colon \sigma_0 = \sigma_{|_L} = I_L\} = Aut_L K = \Gamma(L)$.

□

7.3 Solubilidade por meio de radicais

Nesta seção definiremos a noção de polinômio solúvel por meio de radicais, e daremos um critério (por meio dos grupos de automorfismos) para que as raízes de um polinômio sejam expressas por meio de radicais. Vejamos um exemplo.

Exemplo 7.3.1: Suponhamos que uma raiz α de $f(x) \in \mathbb{Q}[x]$ seja expressa por meio dos seguintes radicais:

$$\alpha = \frac{\sqrt[5]{2-\sqrt[3]{2}}+\sqrt{3}}{\sqrt[7]{1-\sqrt[4]{5}}}.$$

Se denotarmos $a_1 = \sqrt[4]{5} a_2 = \sqrt[7]{1-a_1}, a_3 = \sqrt[3]{2}, a_4 = \sqrt[5]{2-a_3}$ e $a_5 = \sqrt{3}$, teremos:

$$\mathbb{Q} = F_0 \subseteq F_0[a_1] = F_1 \subseteq F_1[a_2] = F_2 \subseteq F_2[a_3] = \ = F_3 \subseteq F_3[a_4] = F_4 \subseteq F_4[a_5] = F_5.$$

E, ainda, $a_1^4 \in F_0, a_2^7 \in F_1, a_3^3 \in F_2, a_4^5 \in F_3, a_5^2 \in F_4, \alpha \in F_5 = \mathbb{Q}[a_1,a_2,a_3,a_4,a_5]$.

Portanto. dada a expressão radical acima conseguimos uma extensão F_5, contendo α.

Definiremos a noção de extensão radical.

Definição 7.8: Dizemos que $K \mid F$ finita é um *extensão radical* sobre F se $\exists a_1, a_2, \ldots, a_r \in K$ tais que:

$$\begin{aligned}(a) & F = F_0 \subseteq F_0[a_1] = F_1 \subseteq F_1[a_2] = F_2 \subseteq F_2[a_3] = \\ & = F_3 \subseteq F_3[a_4] = F_4 \subseteq F_4[a_5] \subseteq \ldots \subseteq F_i = \\ & = F_{i-1}[a_i] \subseteq \ldots \subseteq F_r = K. \\ (b) \ & \forall i \in \{1,2,\ldots,r\}, \exists n_i \mathbb{N} \text{ tais que } a_i^{n_1} \in F_{i-1}.\end{aligned}$$

Observe que como $a_i^{n_i} = b_{i-1} \in F_{i-1}$ podemos também denotar $F_i = F_{i-1}[\sqrt[n_i]{b_{i-1}}]$ ou seja F_i é obtido de F_{i-1} por adjunção de um raiz do polinômio

$$x^{n_i} - b_{i-1} \in F_{i-1}[x].$$

Agora, se $f(x) \in F[x]$ é uma raiz α de $f(x)$ está numa extensão radical $K = F[a_1,a_2,\ldots,a_r]$ com anteriormente, então α pode ser expresso como uma expressão polinomial $p(a_1,a_2,\ldots,a_r)$ com coeficientes em F, isto é,

$$\alpha = p(a_1,a_2,\ldots,a_r) \in F[a_1,a_2,\ldots,a_r].$$

Então, $a_1 = \sqrt[n_1]{b_0}, a_2 = \sqrt[n_2]{b_1} \ldots a_r = \sqrt[n_r]{b_{r-1}}$ em que $b_j \in F_j$, $j = 0,1,\ldots,r-1$ e teremos também:

$$\alpha = p(\sqrt[n_1]{b_0}, \sqrt[n_2]{b_1}, \ldots, \sqrt[n_r]{b_{r-1}}),$$

que é um expressão polinomial radical. Note ainda que,

$$a_1 = \sqrt[n_1]{b_0}, a_2 = \sqrt[n_2]{q_1(\sqrt[n_1]{b_0})}, a_3 = \sqrt[n_3]{q_2(\sqrt[n_2]{q_1(\sqrt[n_1]{b_0})})},$$

e, assim, sucessivamente, em que $q_1,q_2,\ldots,$ são polinômios em F, e assim α poderia se reduzir a um expressão radical envolvendo polinômios e raízes de $b_0 \in F$.

Definiremos a noção de polinômio solúvel por meio de radical.

Definição 7.9: Sejam $f(x) \in F[x]$ e $L = Gal(f,F)$. Dizemos que $f(x)$ é um *polinômio solúvel* por meio de radicais sobre F se $\exists$ uma extensão radical $K \mid L$ tal que $F \subset L \subset K$.

Finalizaremos este capítulo com algumas importantes propriedades.

Proposição 7.4: Seja $\mathbb{Q} \subset F \subset L$ uma extensão radical sobre F. Então existe um extensão K, tal que $F \subset L \subset K$ em que K é radical e galoisiana sobre F.

Teorema 7.8: Sejam $F \mid \mathbb{Q}$, $f(x) \in F[x]$ e $L = Gal(f,F)$. Se $f(x)$ é solúvel por meio de radicais sobre F, então o grupo $G = Aut_F L$ é solúvel.

O teorema acima nos dá condições para a solubilidade de $f(x)$.

Exemplo 7.3.2: O polinômio $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ não é solúvel por meio de radicais sobre $\mathbb{Q}$.

Como $Aut_{\mathbb{Q}} L \approx S_5$ não solúvel, no qual $L = Gal(f,F)$, segue o resultado imediatamente pelo Teorema 7.8.

Já vimos que se $K \mid F$ é uma extensão galoisiana de grau n, então $G = Aut_F K$ é isomorfo a um subgrupo de S_n, veja a Proposição 7.1. Então, para determinarmos a solubilidade por meio de radicais podemos verificar se S_n é solúvel, como no exemplo anterior, já sabendo que pela Proposição 6.10, S_n não é solúvel para $n \geq 5$.

Deste modo temos o seguinte fato: não existe uma fórmula envolvendo somente as operações definidas no corpo e extração de raízes para a solução de uma equação algébrica geral de grau ≥ 5.

O exemplo a seguir nos dirá sobre a solubilidade por radicais de um polinômio geral de grau n.

Exemplo 7.3.3: Seja $L = \mathbb{Q}(x_1, x_2,..., x_n)$ o corpo das funções racionais com coeficientes sobre $\mathbb{Q}$ nas "variáveis independentes $x_1, x_2,..., x_n$".

Se definimos:

$$\begin{aligned} s_1 &= x_1 + x_2 + ... + x_n \\ s_2 &= x_1x_2 + x_1x_3 + ... + x_1x_n + ... + x_{n-1}x_n \\ &\vdots \\ s_n &= x_1x_2...x_n \end{aligned}$$

então $K = \mathbb{Q}(s_1, s_2, \ldots, s_n)$ é chamado o corpo das funções racionais simétricas sobre $\mathbb{Q}$.

Veja que $x_1, x_2,...x_n$ são elementos algébricos sobre K (embora transcendentes sobre $\mathbb{Q}$) pois $L = Gal(f, K)$ no qual

$$f(t) = t^n - s_1t^{n-1} + s_2t^{n-2} + ... + (-1)^n s_n \ \in \ K[t].$$

Assim, $x_1,..., x_n$ são as n raízes de $f(t)$ e mais, $L = K[x_1,x_2,...,x_n] = Gal(f, K)$.

Pode-se provar que cada permutação σ_0 do conjunto $\Omega = \{x_1, x_2, \ldots, x_n\}$ das raízes de f dá origem a um elemento $\sigma \in Aut_K L$, ou seja, $[L : K] = n!$ e $Aut_K L \approx S_n$.

O polinômio $t^n - s_1 t^{n-1} + ... + (-1)^n s_n = f(t)$ chama-se o *polinômio geral de grau n* sobre $\mathbb{Q}$ e portanto:

O polinômio geral de grau n sobre $\mathbb{Q}$, $n \geq 5$, não é solúvel por meio de radicais sobre o corpo das funções racionais simétricas.

Apresentaremos no próximo capítulo três atividades para serem aplicadas em alunos de turmas do 3º ano do ensino médio. Essas atividades serão apresentadas com os respectivos roteiros em concomitância com o software *GeoGebra* tendo em vista um estudo diferenciado de equações algébrica. Neste caso, o aluno terá a oportunidade de ampliar o seu conhecimento por meio de um processo investigativo proporcionando a consolidação de conceitos matemáticos.

8

Atividades Propostas

Neste capítulo o trabalho desenvolvido está relacionado com as equações do 2º, 3º e 5º graus com foco na solubilidade por radicais, ou seja, por meio de fórmulas envolvendo radicais e operações elementares no corpo. O objetivo geral destas atividades é compreender as propriedades básicas dos números complexos e a sua história, a resolução das equações algébricas por meio de fórmulas envolvendo radicais, as diferenças das raízes complexas e reais, e se uma equação é ou não solúvel por radicais. O trabalho aqui proposto tem como objetivo a contextualização e estarão em consonância com [16] e [17].

Nestas atividades o professor deve focar a metodologia de resolução de problemas. Essa metodologia busca primeiro compreender o problema, estabelecer um plano, executar o plano e fazer o retrospecto. Na etapa de compreender o problema o professor deve orientar o aluno a identificar a incógnita, os dados, a condicionante e traçar um figura. No estabelecimento de um plano deve-se encontrar a conexão entre os dados e a incógnita, verificar se existe um problema correlato para facilitar a compreensão, retomar definições ou qualquer outro estratégia que facilite a construção do plano. Ao executar o plano, a verificação de cada passo é essencial para construção do resultado correto. Por último, o retrospecto, examinar a solução obtida para verificar o resultado, possibilita a compreensão dos conceitos abordados no problema. Durante todos as etapas, o professor orienta os alunos como mediador do processo de aprendizagem para não interferir no protagonismo do aluno.

No processo de investigativo temos a exploração e formulação de questões como, reconhecer uma situação problema, explorar a situação problemática e formular questões. Outros momentos importantes na realização de uma investigação são as conjecturas, os testes e reformulações, a justificação e avaliação. Conjecturar é essencial para organizar dados e formular conjecturas. Nos testes e reformulações é possível refinar uma conjectura. E na justificação e avaliação, pode-se justificar uma conjectura e avaliar o raciocínio ou resultado do raciocínio.

Ressalta-se que o *GeoGebra* como ferramenta de ensino/aprendizagem pode ser benquisto pelos educandos, por ser de fácil entendimento e ter layout favorável para o aprendizado, proporcionando a consolidação dos diversos conceitos geométricos no contexto da resolução de problemas. Destaca-se que, ao utilizar este recurso

tecnológico para aperfeiçoar um dado conceito, pode-se aprimorar a didática do educador e permitir ao estudante aprender por meio da dedução, teste e verificação de suas hipóteses. O *GeoGebro* promove uma didática aprimorada do professor, e possibilita ao aprendiz um ambiente desafiador e interessante. E ainda, desenvolve nos estudantes a capacidade de abstração, verificação, construção e consolidação do conhecimento de forma motivadora.

Percebe-se que uma didática diferenciada e inovadora que possibilite ao professor explorar ainda mais as habilidades dos estudantes e os instigue à prática da investigação, pode levá-los a tornarem-se sujeitos argumentativos e reflexivos na busca de um conhecimento adequado e prazeroso.

Foi feito no final deste capítulo uma breve análise dos resultados alcançados por parte dos alunos tendo em vista o conhecimento adquirido, a expectativa em relação a metodologia adotada e se foi despertado o espírito científico no alunos.

8.1 Atividade I - Soluções das equações de segundo e terceiro Graus

Tema:

Determinando as raízes de um tipo equação do terceiro grau através das equações do primeiro e segundo graus.

Objetivos:

- Investigar a solução de uma situação-problema envolvendo cálculo de máximos ou mínimos de uma função do segundo grau;
- Explorar a metodologia de resolução de problemas com auxílio do *GeoGebra*;
- Alterar hipóteses de um problema para obter problemas correlatos e resolvê-los.

Pré-requisitos:

- Reconhecer o gráfico de uma função do segundo grau;
- Reconhecer que o sinal do coeficiente de x^2 é que determina a existência de máximo ou de mínimo de uma função do segundo grau;
- Identificar o valor máximo (ou mínimo) de uma função do segundo grau e quando ele ocorre, respectivamente, com a ordenada e a abscissa do vértice da parábola;
- Calcular as coordenadas do vértice;
- Identificar os intervalos de crescimento e decrescimento da função do segundo grau;

- Calcular o máximo ou o mínimo de uma função do segundo grau;
- Construção do gráfico de função do segundo grau no *GeoGebra*.

Metodologia adotada:

Lista de atividades, lápis, régua, borracha, caneta, quadro, pincel para quadro, apagador, computadores com o software *GeoGebra*.

Orientações didáticas:

Para otimizar o processo de aprendizagem, os alunos deverão sentar-se em dupla ou trio, adotando critérios de afinidade, aptidão matemática e conhecimento em informática. Proporcionando, deste modo, debates sobre as possíveis resoluções e dúvidas a respeito das questões propostas.

O professor deverá prever os possíveis problemas técnicos e a melhor proporção entre números de alunos e computadores. Durante todo o processo de aprendizagem o professor deverá sanar as dúvidas, seguindo pausadamente o roteiro, observando se todos estão compreendendo os conceitos abordados.

Dificuldades Previstas:

Problemas técnicos, conhecimentos sobre o uso de computadores, compreensão dos conceitos abordados e ansiedade dos alunos para conclusão das atividades.

Tempo Estimado

Tempo previsto para a execução desta atividade é de 2 aulas de 50 minuto cada.

Atividade I
Resolva a equação $x^3 - 8x^2 + 12x = 0$

Roteiro da Atividade I:

1. A equação possui no máximo quantas raízes?
2. Fatore, se possível, a equação.
3. Note que determinamos dois fatores, e já podemos determinar uma raiz. Qual é esse valor?
4. O outro fator é um trinômio do 2° grau. Determine as raízes usando a fórmula resolvente da equação do segundo grau que leva o nome de *fórmula de Bhaskara*.
5. Determine as coordenadas do vértice da equação do 2°grau do item anterior.

6. Com o uso do *GeoGebra* faça o gráficos das funções $f(x) = x$ e $g(x) = x^2 - 8x + 12$.

7. Encontre no mínimo 5 pontos no *GeoGeobra*, tal que, $(x, x \cdot (x^2 - 8x + 12))$

8. Faça o gráfico da função $h(x) = x \cdot (x^2 - 8x + 12) = x^3 - 8x^2 + 12x = 0$

9. Faça um análise entre os itens 6,7 e 8. O que podemos concluir sobre a construção do gráfico da função $h(x)$ em relação as funções $f(x) = x$, $g(x) = x^2 - 8x + 12$?

Resolução:
Gráfico das funções $f(x) = x$, $g(x) = x^2 - 8x + 12$ e $h(x) = x^3 - 8x^2 + 12x = 0$

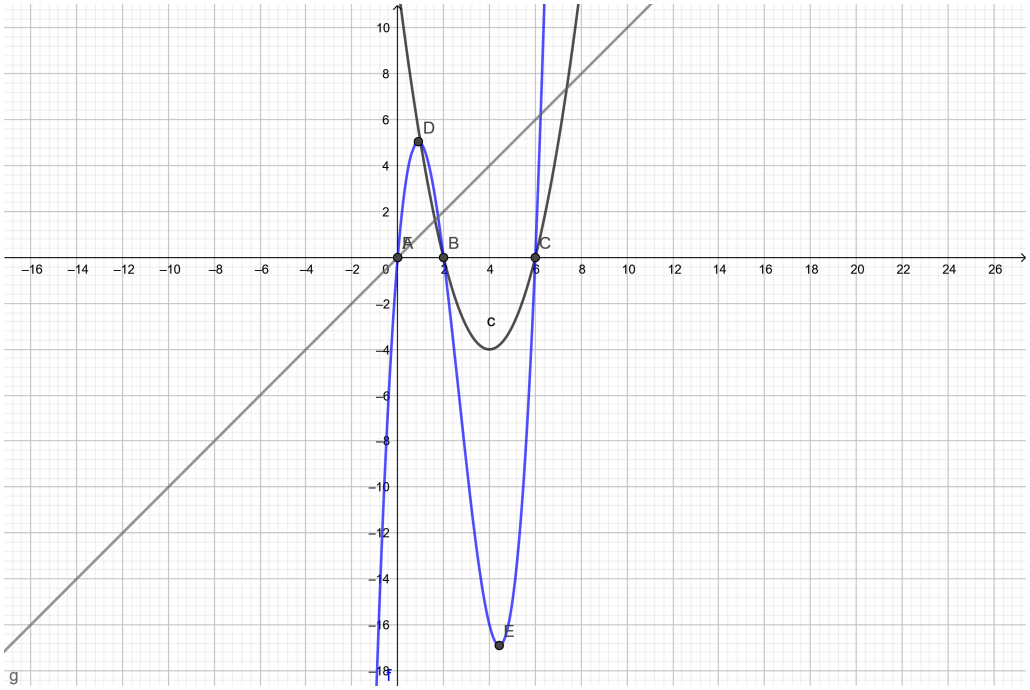


Figura 8.1: Gráfico das funções $f(x) = x$, $g(x) = x^2 - 8x + 12$ e $h(x) = x^3 - 8x^2 + 12x$ da Atividade I
Fonte: Elaborado pelo Autor

Seja $x^3 - 8x^2 + 12x = 0$. Sabemos que um polinômio de grau três possui no máximo três raízes. Se fatorarmos a equação obtemos $x(x^2 - 8x + 12) = 0$. Logo, para esse produto ser igual a zero devemos ter $x = 0$ ou $x^2 - 8x + 12 = 0$. Assim,

$$x^2 - 8x + 12 = 0 \Rightarrow$$

$$x = \frac{-b \pm \sqrt{\triangle}}{2a}$$

$$= \frac{8 \pm \sqrt{16}}{2}$$

Obtemos dois valores $x_1 = 6$ e $x_2 = 2$.

Para os vértices obtemos,

$$x_v = \frac{-b}{2a} = \frac{8}{2} = 4$$
$$y_v = \frac{-\triangle}{4a} = \frac{-16}{4} = -4$$

Note que $h(x)$ é determinado pelo produto de $f(x)$ e $g(x)$. Isto é, seja $y = h(x), m = f(x)$ e $n = g(x)$ temos $y = m \cdot n$

8.2 Atividade II - Solução da equação do terceiro grau por meio das *fórmulas de Cardan*

Tema:
O uso das *fórmulas de Cardan* para solução de uma equação do terceiro grau.

Objetivos:

- Investigar a solução de uma situação-problema por meio de fórmulas;
- Explorar a metodologia de resolução de problemas com auxílio do *GeoGebra*;
- Ampliar o conhecimento sobre números complexos.

Pré-requisitos:

- Reconhecer o gráfico de uma função do terceiro grau do tipo $f(x) = x^3$ em $\mathbb{R}$;
- Conhecer os conceitos básicos de números complexos e raízes da unidade;
- Identificar os intervalos de crescimento e decrescimento da função do terceiro grau em $\mathbb{R}$;
- Construção do gráfico da função do terceiro grau em $\mathbb{R}$ do tipo $f(x) = x^3 + ax^2 + bx + c$ no *GeoGebra* para a, b e c reais;
- Determinar as raízes usando as *fórmulas de Cardan*.

Metodologia adotada:

Lista de atividades, lápis, régua, borracha, caneta, quadro, pincel para quadro, apagador, computadores com o software *GeoGebra* e calculadora científica.

Orientações didáticas:

Para otimizar o processo de aprendizagem, os alunos deverão sentar-se em dupla ou trio, adotando critérios de afinidade, aptidão matemática e conhecimento em

informática. Proporcionando, deste modo, debates sobre as possíveis resoluções e dúvidas a respeito das questões propostas.

O professor deverá prever os possíveis problemas técnicos e a melhor proporção entre números de alunos e computadores. Durante todo o processo de aprendizagem o professor deverá sanar as dúvidas, seguindo pausadamente o roteiro, observando se todos estão compreendendo os conceitos abordados.

Dificuldades Previstas:

Problemas técnicos, conhecimentos sobre o uso de computadores, compreensão dos conceitos abordados e ansiedade dos alunos para conclusão das atividades.

Tempo Estimado

Tempo previsto para a execução desta atividade é de 2 aulas de 50 minuto cada.

Atividade II

Resolva a equação $x^3 + 6x^2 + 21x + 14 = 0$ em $\mathbb{C}$.

Roteiro da Atividade II:

1. A equação possui no máximo quantas raízes?
2. É possível utilizar o método da Atividade I?
3. Determine os valores de p e q.
4. Encontre a raiz real usando as fórmulas de Cardan.
5. Com o uso do *GeoGebra* faça o gráfico da função $f(x) = x^3 + 6x^2 + 21x + 14$.
6. Determine as raízes complexas da função.
7. O *GeoGebra* fornece as raízes complexas da função?
8. Repita o processo para a equação $x^3 - 3x - 18 = 0$
9. Verifique se 3 é raiz da equação do item 8.
10. Se o item 9 for verdadeiro, então nós temos quatro raízes para equação do item 8? Justifique a sua resposta.

Resolução:

Determinemos inicialmente os valores de de p e q.

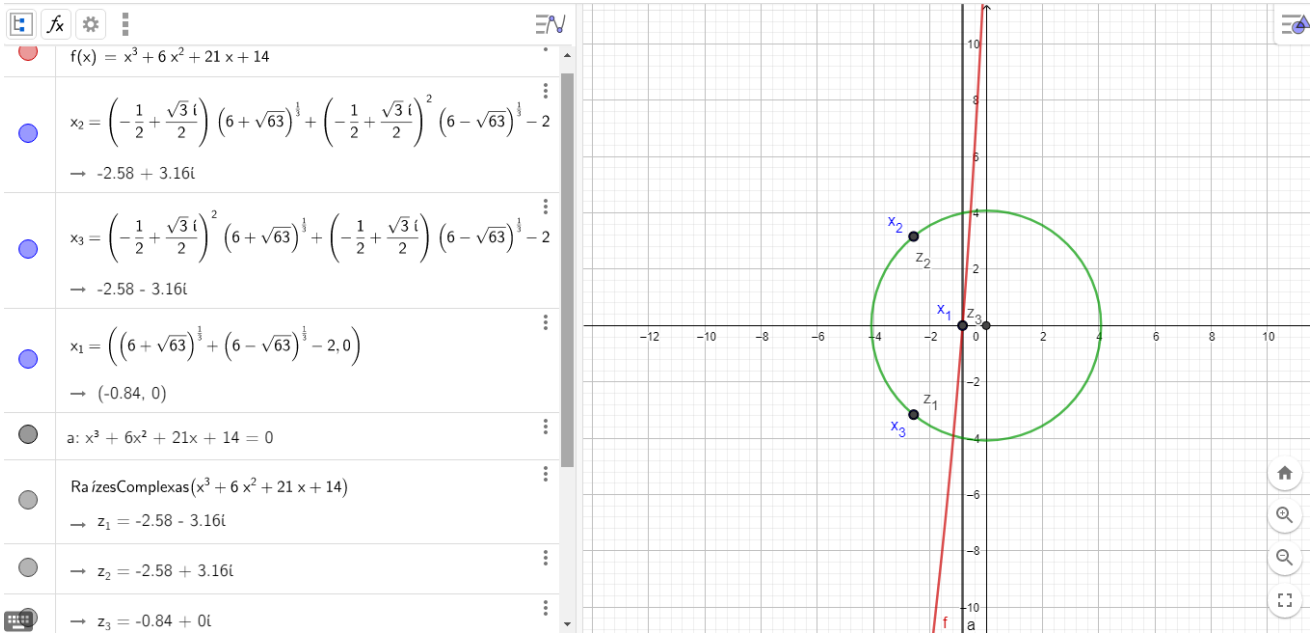


Figura 8.2: Gráfico da função $f(x) = x^3 + 6x^2 + 21x + 14$ da Atividade II
Fonte: Elaborado pelo autor

$$x = y - \frac{6}{3} = y - 2,\ p = 21 - \frac{6^2}{3} = 9,\ q = \frac{2(6^3)}{27} - \frac{21 \cdot 6}{3} + 14 = -12.$$

Para eliminarmos o termo do segundo grau, efetuamos a substituição $x = y - 2$, obtendo a equação $y^3 + 9y - 12 = 0$, cujas raízes são:

$$\begin{aligned} y_1 &= \sqrt[3]{6 + \sqrt{63}} + \sqrt[3]{6 - \sqrt{63}}; \\ y_2 &= w\sqrt[3]{6 + \sqrt{63}} + w^2\sqrt[3]{6 - \sqrt{63}}; \\ y_3 &= w^2\sqrt[3]{6 + \sqrt{63}} + w\sqrt[3]{6 - \sqrt{63}}. \end{aligned}$$

Portanto, as raízes da equação original, veja o Gráfico 8.2, são:

$$\begin{aligned} x_1 &= y_1 - 2; \\ x_2 &= y_2 - 2; \\ x_3 &= y_3 - 2. \end{aligned}$$

No caso da equação $x^3 - 3x - 18 = 0$ temos por inspeção que 3 é raiz da equação, resolvendo de forma análoga obtemos,

$$3 = \sqrt[3]{9 + 4\sqrt{5}} + \sqrt[3]{9 - 4\sqrt{5}}$$

Logo, não temos quatros raízes complexas, veja Gráfico 8.3.

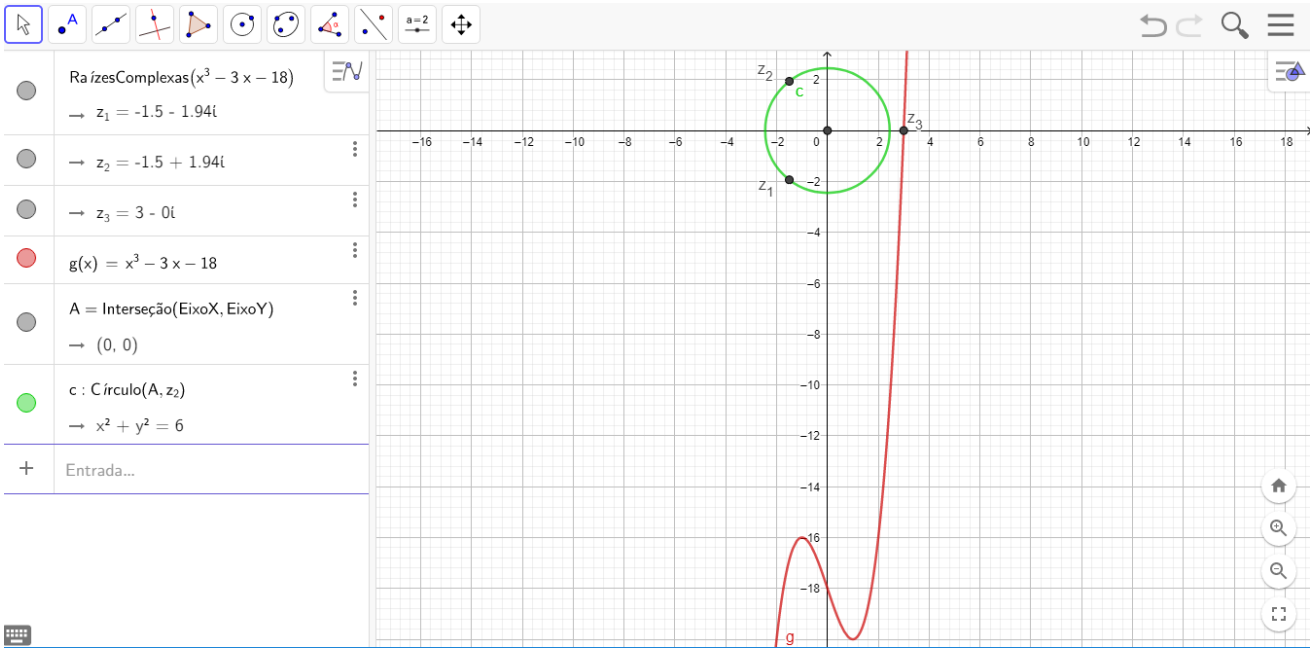


Figura 8.3: Gráfico da função $f(x) = x^3 - 3x - 18$ da Atividade II
Fonte: Elaborado pelo autor

8.3 Atividade III - Solução da equação do quinto grau

Tema:

Uma quíntica não solúvel por radicais

Objetivos:

- Investigar a solução de uma situação-problema por meio de fórmulas;
- Explorar a metodologia de resolução de problemas com auxílio do *GeoGebra*;
- Determinar valores aproximados de raízes por inspeção.

Pré-requisitos:

- Reconhecer o gráfico de uma função do quinto grau do tipo $ax^5 + bx + c$ para a, b e c racionais;
- Identificar os intervalos de crescimento e decrescimento da função do quinto grau em $\mathbb{R}$;
- Construção do gráfico da função do quinto grau no *GeoGebra* para a, b e c racionais;

Metodologia adotada:

Lista de atividades, lápis, régua, borracha, caneta, quadro, pincel para quadro, apagador, computadores com o software *GeoGebra* e calculadora científica.

Orientações didáticas:

Para otimizar o processo de aprendizagem os alunos deverão sentar-se em dupla ou trio, adotando critérios de afinidade, aptidão matemática e conhecimento em informática. Proporcionando, deste modo, debates sobre as possíveis resoluções e dúvidas a respeito das questões propostas.

O professor deverá prever os possíveis problemas técnicos e a melhor proporção entre números de alunos e computadores. Durante todo o processo de aprendizagem o professor deverá sanar as dúvidas, seguindo pausadamente o roteiro, observando se todos estão compreendendo os conceitos abordados.

Dificuldades Previstas:

Problemas técnicos, o conhecimento sobre o uso de computadores, compreensão dos conceitos abordados e ansiedade dos alunos para conclusão das atividades.

Tempo Estimado

Tempo previsto para a execução dessa atividade é de 1 aula de 50 min.

Atividade III

Determine por inspeção um valor aproximado das raízes reais da equação $2x^5 - 10x + 5 = 0$. Sugestão: utilize valores reais dentro do intervalo $[-2,2]$ e pesquise se existe alguma fórmula envolvendo somente as operações definidas em $\mathbb{C}$ e extração de raízes para a solução de uma equação algébrica geral de grau 5.

Roteiro da Atividade III:

1. A equação possui no máximo quantas raízes?
2. Utilize a calculadora para determinar os valores aproximados das raízes. Compare seu resultado com os outros grupos.
3. Com o uso do *GeoGebra* faça o gráfico da função $f(x) = 2x^5 - 10x + 5 = 0$
4. Compare o seu resultado com as raízes determinadas pelo *GeoGebra*.
5. Pesquise uma solução que utilize fórmulas correspondentes com a Atividade II.

Resolução:

Por inspeção podemos determinar alguns valores aproximados para as raízes. Vejamos alguns valores:

$$
\begin{aligned}
f(2) &= 2(2)^5 - 10(2) + 5 = 49 \\
f(1{,}5) &= 2(1{,}5)^5 - 10(1{,}5) + 5 = 5{,}188 \\
f(1{,}4) &= 2(1{,}4)^5 - 10(1{,}4) + 5 = 1{,}756 \\
f(1{,}3) &= 2(1{,}3)^5 - 10(1{,}3) + 5 = -0{,}574 \\
f(1{,}33) &= 2(1{,}33)^5 - 10(1{,}33) + 5 = 0{,}0231
\end{aligned}
$$

Gráfico das função $f(x) = 2x^5 - 10x + 5 = 0$.

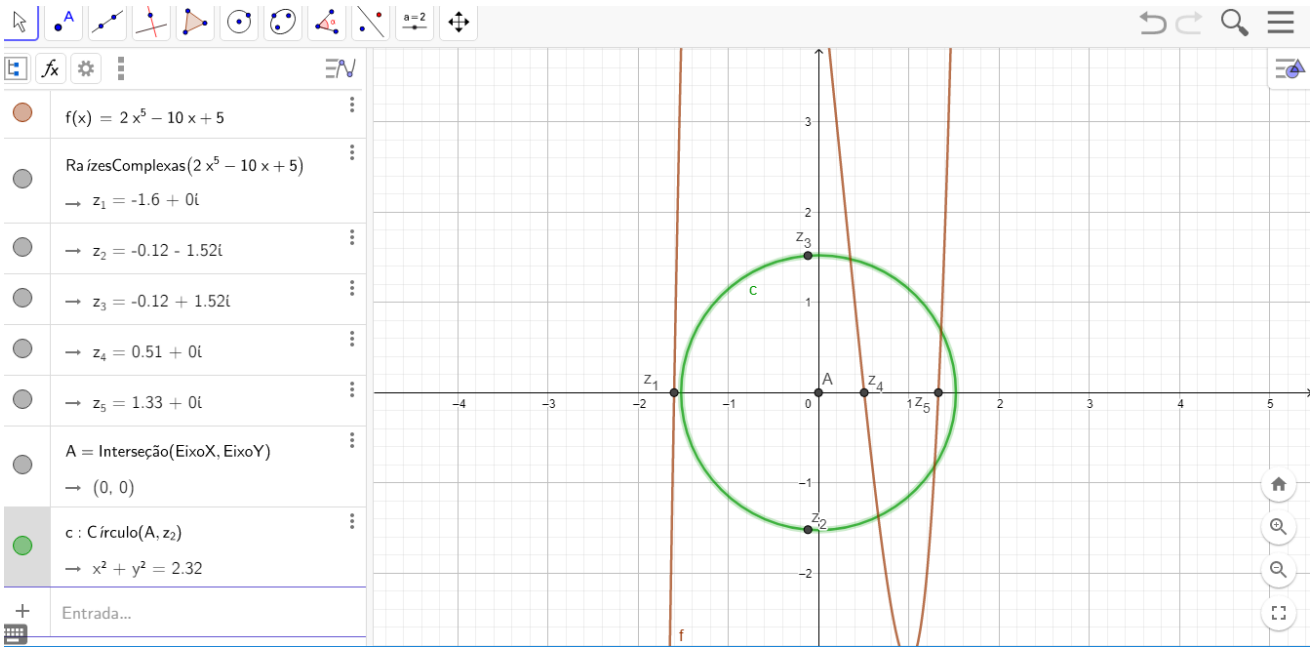


Figura 8.4: Gráfico das função $f(x) = 2x^5 - 10x + 5 = 0$ da Atividade III
Fonte: Elaborado pelo autor

Note que o *GeoGebra* determinou $z_5 = 1{,}33$ como a raiz da função. Mas quando utilizamos este valor na função $f(x) = 2x^5 - 10x + 5$ encontra-se $f(1{,}33) \neq 0$. Isto ocorre devido aos critérios arredondamentos do programa.

Por último, o grupo de galois do polinômio $f(x) = 2x^5 - 10x + 5 = 0 \in \mathbb{Q}$ é isomorfo à S_5, não solúvel. Consequentemente, a equação $f(x) = 2x^5 - 10x + 5 = 0$ não é solúvel por radicais.

8.4 Avaliação das aulas ministradas

Em parceria com a equipe pedagógica na unidade escolar, foi estabelecido que selecionaríamos 18 alunos do 3° ano do Ensino Médio. Esta amostragem foi estabelecida de acordo com os critérios de interesse, disponibilidade de horário, vocação matemática. Esses alunos pertencem a várias unidades escolares do Município de Contagem/MG, Brasil. Todas as aulas foram ministradas no laboratório de informática e ministrada pelo o autor. O período previsto de trabalho era de 3 dias no turno da tarde das 13 horas as 17 horas.

Devido a dinâmica da aulas, o período de trabalho foi concluído em 4 dias, um dia além do previsto. Inicialmente foi necessário ministrar 3 aulas de 50 minutos referentes ao conteúdo dos números complexos e 1 aula de 50 minutos, sobre as ferramentas básicas do *GeoGebra*.

Na primeira aula, relatou-se sobre a importância dos números complexos nas ciências e um pouco da história. Posteriormente, no intuito compreender a ideia $\sqrt{-1} = i$ iniciou-se com uma situação-problema mais simples, e aguardou-se a reação dos alunos. Segue esse primeiro Exemplo 8.4.1 trabalhado em sala.

Exemplo 8.4.1: Faça conforme o exemplo abaixo.
$\sqrt{-3} = \sqrt{3(-1)} = \sqrt{3} \cdot \sqrt{-1}$

a) $\sqrt{-5}$

b) $\sqrt{-6}$

Neste momento os alunos indagaram que "não existe raiz quadrada de -1". Houve a seguinte intervenção. "Temos um problema, $\sqrt{-1} \notin \mathbb{R}$ e não podemos resolver o exemplo em $\mathbb{R}$. O que podemos fazer? Será podemos criar um conjunto no qual resolveremos o exemplo?".

Após uma explanação sobre a possibilidade de criarmos um conjunto no qual existe $\sqrt{-1}$ e tomando o devido cuidado para não desvincular das propriedades do conjunto $\mathbb{C}$ visto no Capítulo 4, Seção 4.2 trabalhou-se a seguinte estratégia. "Portanto, façamos a adjunção de $\sqrt{-1}$ com $\mathbb{R}$, ou seja, $\mathbb{R} \cup \{\sqrt{-1}\}$, e ainda, $\sqrt{-1} = i$ e $\mathbb{R} \cup \{\sqrt{-1}\} = R(i) = \mathbb{C}$. Chamamos $\mathbb{C}$ de conjuntos dos complexos". Sugerimos ao leitor a releitura da Definição 5.2 e o Exemplo 5.1.7.

Posteriormente os alunos foram direcionados a refazerem Exemplo 8.4.1 em $\mathbb{C}$. Com objetivo de levar os alunos à definição dos números complexos foi descrito no quadro branco alguns exemplos de números complexos como, $10i, 5 + 7i, -i, 20$, e $7 - 9i$. E feita a seguinte pergunta, "Por quê esses números pertencem ao conjunto $\mathbb{C}$? Houve diversas respostas, "Porque tem o i", "O número real está dentro do complexo", "Quando soma, não deixa de ser complexo". E claro que as respostas não foram instantâneas, sempre houve a necessidade de direcionar os alunos.

Após outras orientações sobre os números complexos percebeu-se que os alunos compreenderam o porquê dos exemplos apresentados eram números complexos. Logo, antes de introduzir a definição de números complexos, apresentou-se o seguinte exemplo.

Exemplo 8.4.2: Represente os números complexos $1 + 5i$, $9 - 7i$, 5 e $8i$ no plano cartesiano usando *GeoGebra*.

O exemplo 8.4.2 foi descrito no quadro branco e orientou-se os alunos a fazerem; sem mais explicações. Essa estratégia de não explicar foi intencional para analisar as reações e indagações dos alunos, o objetivo era que eles percebesse quais números estavam no eixo vertical e no eixo horizontal. A surpresa é que eles, simplesmente, abriram o *GeoGebra* e fizeram o que foi pedido, e ficaram aguardando novas orientações. Esperava-se que ficassem surpresos com a ideia números complexos serem representados como par ordenado, mas, não houve essa assimilação.

Então, após algumas falas sobre a relação dos números complexos e os pares ordenados, explicou-se a definição de números complexos, Definição 4.1, a forma algébrica do complexo z, as propriedades do módulo de z, o conjugado e a aritmética dos números complexos do Seção 4.2.

Os alunos conseguiram compreender que $z = a + bi$ em que a e b são reais (a é chamado *parte real* e b a *parte imaginária* (O aluno P.L.F relatou "Imaginário, porque imaginamos que $i = \sqrt{-1}$".) do complexo, mas, a relação dos números complexos com os pares ordenadas não foram compreendidas por todos, 3 alunos afirmaram que entenderam parcialmente e outros 15 alunos afirmaram que compreenderam.

Assim para trabalhar os conceitos apresentados foram feitos alguns exercícios com os alunos. São eles,

No caso da aritmética dos números complexos foi proposto os exemplos 8.4.3, 8.4.4, 8.4.5, 8.4.6 e 8.4.7.

Exemplo 8.4.3: Dados os números complexos $z_1 = (x - 1, y + 2)$ e $z_2 = (-4, 3)$, determine os números reais x e y para que se tenha $z_1 = z_2$.

Exemplo 8.4.4: Dados os complexos $z_1 = (2, 4)$ e $z_2 = (3, -1)$, determine os complexos v e w, tais que $v = z_1 + z_2$ e $w = z_1 \cdot z_2$.

Exemplo 8.4.5: Dados os complexos $z_1 = (1, 2)$ e $z =_2 (3, 4)$ cada caso determine o complexo z que satisfaz a condição indicada:

a $z_2 + z = z_1$

a $z_2 \cdot z = z_1$

Exemplo 8.4.6: Calcule:

a) i^2

b) i^3

c) i^4

d) i^5

e) $i^5 4$

f) $i^9 5$

Exemplo 8.4.7: Dados os complexos $v = 1+2i$ e $w = 2-2i$, calcule $v+w, v \cdot w, w^2$ e $w - v$

O exemplo 8.4.8 foi proposto no intuito de melhorar a compreensão das *fórmulas de Cardan*. As quais foram utilizadas na Atividade II.

Exemplo 8.4.8: Dado o número complexo $w = \frac{-1}{2} + \frac{i\sqrt{3}}{2}$, calcule w^2 e w^3.

O exemplo 8.4.9 foi proposto para trabalhar os conceitos de módulo e conjugado.

Exemplo 8.4.9: Dado o complexo $z = 2 - 4i$, determine:

a) o inverso de z;

b) o conjugado do inverso de z^2;

c) o inverso de $z \cdot i$

d) o módulo de z e $\bar{z}$

Concluímos desta forma o primeiro dia de estudo. Essa metodologia de construir um trabalho investigativa sobre um determinado conceito antes de apresentá-lo, contribui para desenvolvimento da autonomia do aluno e promove a consolidação do conhecimento.

No segundo dia de trabalho a proposta era trabalhar as atividades I e II em 4 aulas de 50 minutos. Os conceitos abordados na Atividade I e II estão relacionados com Capítulo 4 Seção 4.3.

Na Atividades I, Resolva a equação $x^3 - 8x^2 + 12x = 0$, os alunos sentaram em duplas nos computadores nos quais foram disponibilizado o *GeoGeobra*. Também foram entregues para os alunos material escolar básico (lápis, borracha, canetas azul e vermelha, régua) e calculadora científica. Cada dupla recebeu o roteiro e aguardou-se um tempo para eles o lerem. Rapidamente, sem qualquer explicação notou-se algumas duplas responderem as perguntas corretamente, sem qualquer auxílio do professor. Com auxílio do professor, todos os alunos participaram da atividade, esta primeira atividade transcorreu tranquilamente. Importante relatar que o professor não pode ser o agente principal da resolução da atividade, e sim, o aluno. A dificuldade por parte dos alunos que se destacou nesta atividade foi a de encontrar a relação entre os três gráficos $f(x) = x, g(x) = x^2 - 8x + 12$ e $h(x) = x(x^2 - 8x + 12) = x^3 - 8x^2 + 12x$.

A proposta de apresentar a turma os três gráficos no mesmo plano cartesiano, para entenderem que $h(x) = f(x) \cdot g(x)$, foi um dificultador do aprendizado. Seria mais interessante explicar separadamente os três gráficos e somente posteriormente a explicação deles juntos. Assim, foi necessário retornar no item 7 com uma estratégia diferente, Exemplo 8.4.10.

Exemplo 8.4.10: Determine pontos no plano cartesiano, para $x = 2, 4, 6, 8$ tal que as coordenadas sejam determinadas por (x,x), $(x, x^2-8x+12)$ e $(x, x\cdot(x^2-8x^2+12x))$.

Neste caso, a determinação desses pontos foram feitas em concomitância com o professor, da seguinte forma:

1. $A = (3, 3)$ e $E = (3, -3)$. Determina $I = (3, 3 \cdot -3) = (3, -9)$;
2. $B = (4, 4)$ e $F = (4, -4)$. Determina $J = (4, 4 \cdot -4) = (4, -16)$;
3. $C = (5, 5)$ e $G = (5, -3)$. Determina $K = (5, 5 \cdot -3) = (5, -15)$;
4. $D = (8, 8)$ e $H = (8, 12)$. Determina $L = (8, 8 \cdot 12) = (8, 96)$.

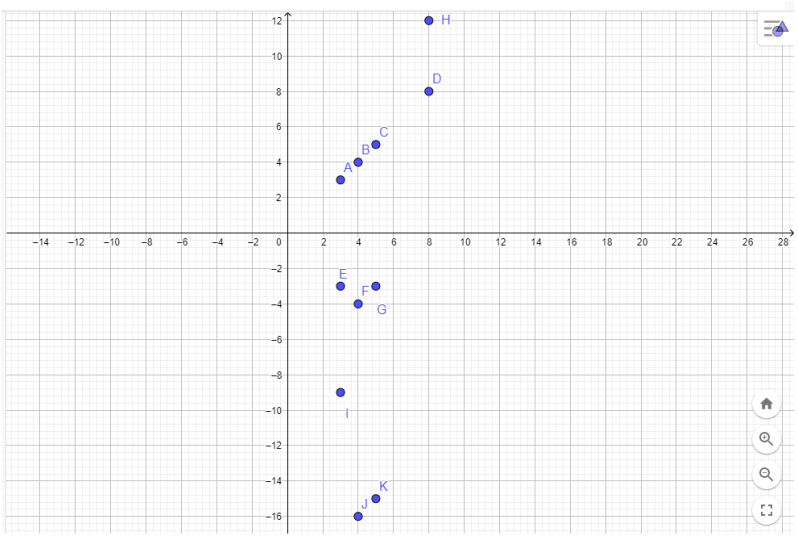


Figura 8.5: Exemplo 8.4.10 da Atividade I
Fonte: Elaborado pelo autor

A medida que os alunos determinavam a construção dos pontos, havia a explicação de cada passo. Em seguida foi feito o Gráfico 8.6 da função $h(x) = x^3 - 8x^2 + 12x$ e explicou-se novamente a igualdade $h(x) = f(x) \cdot g(x)$.

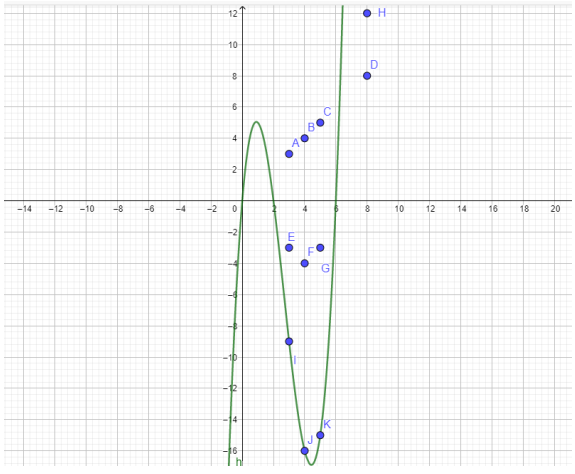


Figura 8.6: Exemplo 8.4.10 da Atividade I
Fonte: Elaborado pelo autor

No terceiro dia a expectativa era concluir as Atividades II e III em 4 aulas de 50 minutos.

Na Atividade II, "Resolva a equação $x^3 + 6x^2 + 21x + 14 = 0$ em $\mathbb{C}$", os alunos continuaram em duplas, necessitou retomar sobre o conteúdo de números complexos e escrever no quadro branco as fórmulas, da Seção 4.3.2, necessária para o desenvolvimento da atividade. São elas:

Obter a igualdade,

$$x^3 + a_2x^2 + a_1x + a_0 = y^3 + py + q = 0,$$

para

$$x = y + d \Rightarrow x = y - \frac{a_2}{3},\ p = a_1 - \frac{a_2^2}{3},\ q = \frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0.$$

Finalizar com as

Fórmulas de Cardan

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

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

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

Quando foi escrito essas fórmulas no quadro branco, surgiu todo tipo de adjetivos, mas, não houve desânimo por parte dos alunos já que podia usar a calculadora. Esse é importante instrumento para motivação e conferência de resultados. A primeira pergunta feita pelos alunos foi: "Como escreve essa fórmula na calculadora?"Então, eles foram orientados a seguir o roteiro e o uso das *fórmulas de Cardan* seria para o para o item 6 do roteiro.

O interessante que vários alunos, sem intervenção do professor, responderam corretamente a primeira pergunta, "A equação possui no máximo quantas raízes?". Conseguiram relacionar o grau do polinômio $f(x) = x^3 + 6x^2 + 21x + 14$ com o número de raízes, veja a Proposição 3.4.

Antes de responderem o item 3, foram feitas explicações sobre a origem, do ponto de vista histórico, das *fórmulas de Cardan*, veja Seção 4.1, e o modo usar as fórmulas, principalmente a importância de eliminar o termo de segundo grau. Mas, o maior desafio foi explicar o porquê do $w = \dfrac{-1 + i\sqrt{3}}{2}$ nas *fórmulas de Cardan*, que é uma das raízes cúbicas da unidade (veja Corolário 4.3), já que, a explicação feita na Seção 4.3.2 não está direcionada para o Ensino Médio. Após algumas explicações, houve mais aceitação que compreensão do assunto, mas, não impediu de usá-las.

Transcorreu tranquilamente a determinação dos valores de p e q. No entanto, na eliminação do termo de segundo grau foi necessário algumas intervenções individuais e coletivas. Somente um aluno, sem auxilio do professor, conseguiu efetuar a

substituição $x = y - 2$ e obteve corretamente a equação $y^3 + 9y - 12 = 0$. A maior dificuldades dos alunos na eliminação do termo do segundo grau foi a manipulação dos fatores. Os erros eram mais falta de atenção que falta de conhecimento.

No item 4, foi recomendado aos alunos fazerem primeiramente no caderno as devidas substituições e simplificações para posteriormente usarem a calculadora. Desta forma o uso da calculadora fica simplificado. A dificuldade identificada foi escrever a expressão $\sqrt[3]{6+\sqrt{63}} + \sqrt[3]{6-\sqrt{63}}$ na calculadora mas todos conseguiram após as orientações. Até a esse item foram usadas 2 aulas de 50 minutos.

No item 5 não foi falado, intencionalmente, que quando encontrassem o gráfico da função $f(x) = x^3 + 6x^2 + 21x + 14$ o *GeoGebra* apenas identificaria a raiz real. No intuito de verificar a reação dos alunos. E realmente aconteceu o esperado, rapidamente perguntaram sobre as outras duas raízes complexa. Foi explicado aos alunos que quando digitamos uma função no *GeoGebra* o gráfico exibido está em $\mathbb{R}$. Então eles foram orientados a fazerem uma pequisa na internet sobre como determinar as raízes complexas usando o *GeoGebra*. Verificou-se que existe o comando *RaízesComplexa(*$f(x)$*)*, o que satisfaz o item 7.

No item 6, usou-se as *fórmulas de Cardan*. Como foi determinado os valores de p e q anteriormente, a aplicação da fórmula transcorreu tranquilamente. Em seguida, determinou-se as raízes complexas usando o comando *RaízesComplexa(*$x^3 + 6x^2 + 21x + 14$*)* para verificação do resultado, veja Gráfico 8.2. Nesse gráfico é importante traçarmos a circunferência de raio $|x_2|$ ou $|x_3|$ para alunos compreenderem as diferenças da raiz real e as complexas.

Importante relatar que devido ao uso da calculadora e do *GeoGebra* os alunos não ficaram desanimados com o desenvolvimento da aula. Mesmo com uma maior intervenção do professor o trabalho investigativo por parte dos alunos foi surpreendente, e todos conseguiram encontrar o resultado esperado. Na Atividade II foi necessário quase as 4 aulas de 50 minutos. Um fato interessante que ocorreu, foi na resposta da pergunta (10), quando neste momento após a explicação da mesma no quadro branco, o aluno M.A.S fez a seguinte indagação sobre o fato que $3 = \sqrt[3]{9+4\sqrt{5}} + \sqrt[3]{9-4\sqrt{5}}$: "Professor, você está errado! Isso não é possível! A calculadora deve estar com erro de arredondamento!" Note que a pergunta sobre arredondamento é prudente e interessante. Então foi esclarecido para o aluno o fato, mas, ele não acreditou e relatou que levaria para outro professor. Tudo isso ocorreu de forma tranquila e respeitosa. Posteriormente o aluno comunicou a escola que informou o autor deste trabalho, que a questão estava correta.

Por último a Atividade III que ocorreu no quarto dia, o qual não estava previsto no cronograma. "Determine por inspeção um valor aproximado das raízes reais da equação $2x^5 - 10x + 5 = 0$. Sugestão: utilize valores reais dentro do intervalo $[-2{,}2]$. E pesquise se existe alguma fórmula envolvendo somente as operações definidas em $\mathbb{C}$ e extração de raízes para a solução de uma equação algébrica geral de grau 5", foi impossível controlar a ansiedade dos alunos em relação a pesquisa, porque rapidamente eles vincularam a pesquisa com a *internet*. Então, o cronograma da aula foi modificado e os alunos fizeram diversas pesquisas direcionada pelo professor para responder a pergunta (5) do roteiro. Esse trabalho investigativo em nenhum

momento pode ser desmotivado, e sim, direcionado e incentivado. Encontraram nas suas pesquisas que não é possível determinar uma fórmula envolvendo radicais para uma equação de 5° grau. Mas eles não compreenderam o motivo. A explicação sobre a solubilidade de radicais, foi um desafio. E após diversas tentativas de esclarecimento, concordamos em apenas aceitar o fato. Fica então a pergunta: É possível ensinar a solubilidade de radicais para os alunos da educação básica na rede pública?

Na Atividade III, os alunos ficaram interessados em como descobrir as raízes de equações de grau n sem o *GeoGebra*. Então, citou-se a eles os seguintes métodos: *Método de Newton*, *Método da Secante* e o *Método da Posição Falsa* que são métodos de aproximações numéricas e estão fora do contexto desta atividade.

Importante ressaltar que foi feita, pelo autor deste trabalho, uma avaliação contínua por meio de relatórios e uma autoavaliação por parte dos alunos no último dia. Esses relatórios continham as seguintes indagações com algumas respostas,

1. Os alunos se interessaram pela atividade proposta?

   "O nível de interesse estava bom, talvez os recursos didáticos e os fatos históricos contribuíram. Mas, todos alunos presentes tinham vocação matemática. E se não tivessem, será que o nível de interesse seria o mesmo?"

2. Quais foram as dificuldades apresentadas?

   "Na Atividade I a maior dificuldade foi compreender o item 9, necessitando uma maior intervenção. Na Atividade II foi o uso das *fórmulas de Cardan*, compreender que $3 = \sqrt[3]{9+4\sqrt{5}} + \sqrt[3]{9-4\sqrt{5}}$ e o uso da calculadora e do *GeoGebra* para conferência dos resultados. Por último, na Atividade III foi a compreensão sobre a solubilidade por meio de radicais".

3. Quais foram os objetivos alcançados?

   "Compreenderam, as propriedades básicas dos números complexos, a importância das equações algébricas nas ciências, os métodos para solucionar as equações algébricas e as diferenças das raízes complexas e reais. No entanto, não foi compreendido de maneira plena o porque do $w = \dfrac{-1+i\sqrt{3}}{2}$ nas *fórmulas de Cardan* e se uma equação é ou não solúvel por radicais."

4. Qual outro recursos didático poderia ser empregado nas aulas?

   "Não foi identificado outro recurso"

5. Em qual momento houve maior interação entre as pessoas envolvidas no trabalho?

   "No momento que o aluno M.A.S relatou que estaria errado a igualdade

$3 = \sqrt[3]{9+4\sqrt{5}} + \sqrt[3]{9-4\sqrt{5}}$ por causa do erro de arredondamento da calculadora e do *GeoGebra*. Houve um debate intenso entre os alunos, mas, sem indisciplina".

Em relação a autoavaliação, foram feitas as seguintes perguntas aos alunos para responderem sem identificação:

1. Em relação ao aprendizado dos conteúdos apresentados, marque uma das opções abaixo:

a) **Uso do *GeoGebra*:**

( ) Bom

( ) Regular

( ) Ruim

b) **Números complexos:**

( ) Bom

( ) Regular

( ) Ruim

c) **Resolução das equações algébricas de 2° e 3° grau usando as fórmulas:**

( ) Bom

( ) Regular

( ) Ruim

d) **Resolução de equações algébricas de grau maior que 3 usando o *GeoGebra***

( ) Bom

( ) Regular

( ) Ruim

e) **Diferença entre as raízes reais e complexas:**

( ) Bom

( ) Regular

( ) Ruim

f) **Solubilidade por meio de radicais**

( ) Bom

( ) Regular

( ) Ruim

Na autoavaliação dos 18 alunos, temos,

- Na letra (a) 16 alunos responderam “Bom”e 2 “Regular”e 0 “Ruim”;
- Na letra (b) 13 alunos responderam “Bom”e 3 “Regular”e 2 “Ruim”;
- Na letra (c) 16 alunos responderam “Bom”e 0 “Regular”e 2 “Ruim”;
- Na letra (d) 18 alunos responderam “Bom”e 0 “Regular”e 0 “Ruim”;
- Na letra (e) 12 alunos responderam “Bom”e 2 “Regular”e 4 “Ruim”;
- Na letra (f) alunos responderam 0 “Bom”e 3 “Regular”e 15 “Ruim”.

O fato dos alunos não compreenderem plenamente o porque do $w = \dfrac{-1 + i\sqrt{3}}{2}$ nas *fórmulas de Cardan* e se uma equação é ou não solúvel por radicais, não indica que o trabalho foi ineficiente já que a demonstração desses dois assuntos estão fora do contexto do ensino médio. E também, os outros objetivos foram alcançados, são eles, as propriedades básicas dos números complexos, a importância das equações algébricas nas ciências, os métodos para resolver as equações algébricas e as diferenças das raízes complexas e reais. Com base na participação dos alunos em todo o processo, das respostas corretas e a conclusão das atividades.

Enfim, as atividades propostas no Capítulo 8, seria recomendado aplicá-las nas escolas como um projeto de trabalho anual e em pequenos grupos, devido aos conteúdos abordados. Assim, a importância de abordar esse tipo de trabalho é desenvolvimento do espírito cientifico nos estudantes.

9

Conclusão

O estudo das equações algébricas demonstrou a importância de trabalharmos esse assunto na educação básica, já que as equações algébricas estão presentes nas diversas áreas do conhecimento científico. E a descoberta por Galois que não existe uma fórmula envolvendo somente operações definidas no corpo e extração de raízes para a solução de uma equação algébrica de grau ≥ 5, direciona o professor de educação básica a usar meios computacionais na busca da solução de uma equação algébrica de grau ≥ 5, semelhante ao usado no Capítulo 8. Nesse caso o *GeoGebra* é um ótimo recurso computacional, visto que, é gratuito, de fácil aprendizado e pode ser usado em *smartphones*.

Os professores devem aprofundar no estudo das equações algébricas no intuito de aperfeiçoar a metodologia de ensino, não esquecendo da importância de trabalharmos fatos históricos que incentivará os alunos a ficarem motivados no estudo das equações. Nas Atividades Propostas, Capítulo 8, foi essencial explicar a história das *fórmulas de Cardan* na intenção de compreenderem a importância do desenvolvimento científico.

Anéis e corpos estão inseridos em todas as propriedades da matemática, sendo necessário defini-los antes de iniciarmos o estudo das diversas propriedades e definição matemáticas da educação básica e superior. Na educação básica brasileira a tendência é nos limitarmos, no corpo dos reais, sendo um erro, já que o corpo dos complexos proporciona novas propriedades e facilita a determinação de raízes das equações algébricas, como vimos neste trabalho.

Os polinômios perpassa por quase todo o trabalho, Capítulos 3, 4, 5 e 7, visto que determina diversas relações na teoria de corpos e equações algébricas. Por isso, a necessidade de aprofundar de forma sistemática na determinação de raízes e conceitos de irredutibilidade de polinômios. As soluções de equações algébricas por meio de fórmulas envolvendo radicais e as operações básicas de um corpo contribui para uma metodologia de ensino focado no aluno, já que, facilita a obtenção de resultados e o estudo de novos conceitos matemáticas. Mas, sabemos que não são todas equações de grau ≥ 5 que é solúvel por radicais, então, as aproximações numéricas para o valor da raiz por meio da inspeção contribuirá para um melhor entendimento para o assunto nesse caso, conforme feito na Atividade III.

Portanto, é necessário uma mudança de perspectiva no estudo de equações

algébricas. Visto que a matemática moderna está vinculada ao progresso da sociedade contemporânea.

Bibliografia

[1] Alves, M. M. S. *Teoria de Aneis*. Ed. por UFP. 2013.

[2] Anyah, J. N. *Álgebra II*. Ed. por UFBA. 2017, p. 244.

[3] Araujo, K. V. de. *Estruturas Algebricas II*. Ed. por UFS. 2ª ed. 2009.

[4] Bedoya, H. e Camelier, R. *Álgebra II*. Ed. por CECIERJ. 2010, p. 264.

[5] Boyer, C. B. *História da Matemática*. Ed. por Blucher, E. 1996.

[6] Ferreira, J. *A construção dos Números*. Ed. por SBM. 3ª ed. 2013, p. 133.

[7] Gonçalves, A. *Introdução à álgebra*. Ed. por IMPA. 5ª Ed. 2015, p. 194.

[8] Gonçalves, A. e Figuereido, L. M. *Álgebra I*. Ed. por CECIERJ, F. Vol. 2. 2010, p. 60.

[9] Hefez, A. *Curso de Álgebra*. Ed. por IMPA. 1ª Ed. Vol. 1. 2014, p. 213.

[10] Hefez, A. e Villela, M. L. T. *Polinômios e Equações Algébricas*. Ed. por SBM. 1ª Ed. Coleção Profmat. SBM, 2012, p. 269.

[11] Lima, E. L. et al. *A Matemática do Ensino Médio*. Ed. por SBM. 6ª ed. Vol. 3. 2006.

[12] Marques, C. M. *Introdução à Teoria de Anéis*. Ed. por UFMG. 2005.

[13] Ohse, M. L. *A Matemática na Idade Moderna do Renascimento à Revolução Industrial*. URL: https://pt.scribd.com/document/2972265/Historia-da-Matematica-Renascimento.

[14] Picado, J. *Apontamentos de Álgebra II*. Ed. por Coimbra, U. de. 2006, p. 149.

[15] Pitombeira, J. B. e Roque, T. M. *Tópicos de História da Matemática*. 1ª Ed. Coleção Profmat. SBM, 2012, p. 269.

[16] Polya, G. *A arte de resolver problemas*. Ed. por Interciência. 2006, p. 203.

[17] Ponte, J. P. da, Brocardo, J. e Oliveira, H. *Investigações Matemátias na Saula de Aula*. Ed. por Autêntica. 1ª ed. 2005, p. 152.

[18] VIDIGAL, A. e. a. *Fundamentos de Álgebra*. Ed. por UFMG. 1ª Ed. 2009.

[19] Villela, M. L. T. *Teoria Galois*. Ed. por UFF. 2017. URL: http://www.professores.uff.br/marco/wp-content/uploads/sites/37/2017/08/corpos-mod2.pdf.

10

Apêndice

10.1 Apêndice A - Atividade I

	Mestrado Profissional em Matemática em Rede Nacional Mestrando: Cristiano Gonçalves Augusto Orientadora: Danielle Franco Nicolau Lara Aluno: _____ Grupo: __ Data: ____	PROFMAT

Atividade I

Resolva a equação $x^3 - 8x^2 + 12x = 0$

Roteiro da Atividade I:

1. A equação possui no máximo quantas raízes?
2. Fatore, se possível, a equação.
3. Note que determinamos dois fatores, e já podemos determinar uma raiz. Qual é esse valor?
4. O outro fator é um trinômio do 2° grau, determine as raízes usando a fórmula resolvente da equação do segundo grau que leva o nome de *fórmula de Bhaskara*.
5. Determine as coordenadas do vértice da equação do 2°grau do item anterior.
6. Com o uso do *GeoGebra* faça o gráficos das funções $f(x) = x$ e $g(x) = x^2 - 8x + 12$.
7. Encontre no mínimo 5 pontos no *GeoGeobra*, tal que, $(x, x \cdot (x^2 - 8x + 12))$
8. Faça o gráfico da função $h(x) = x \cdot (x^2 - 8x + 12) = x^3 - 8x^2 + 12x = 0$
9. Faça um análise entre os itens 6,7 e 8. O que podemos concluir sobre a construção do gráfico da função $h(x)$ em relação as funções $f(x) = x$, $g(x) = x^2 - 8x + 12$?

10.2 Apêndice B - Atividade II

	Mestrado Profissional em Matemática em Rede Nacional Mestrando: Cristiano Gonçalves Augusto Orientadora: Danielle Franco Nicolau Lara Aluno: _____ Grupo: ___ Data: _____	PROFMAT

Atividade II

Resolva a equação $x^3 + 6x^2 + 21x + 14 = 0$ em $\mathbb{C}$

Roteiro da Atividade II:

1. A equação possui no máximo quantas raízes?

2. É possível utilizar o método da Atividade I?

3. Determine os valores de p e q.

4. Encontre a raiz real usando as fórmulas de Cardan?

5. Com o uso do *GeoGebra* faça o gráfico da função $f(x) = x^3 + 6x^2 + 21x + 14$.

6. Determine as raízes complexa da função.

7. O *GeoGebra* fornece as raízes complexa da função?

8. Repita o processo para a equação $x^3 - 3x - 18 = 0$.

9. Verifique se 3 é raiz da equação do item 8.

10 Se o item 9 for verdadeiro, então nós temos quatro raízes para equação do item 8? Justifique a sua resposta.

	Mestrado Profissional em Matemática em Rede Nacional Mestrando: Cristiano Gonçalves Augusto Orientadora: Danielle Franco Nicolau Lara Aluno: _____ Grupo: ___ Data: _____	PROFMAT

10.3 Apêndice C - Atividade III

Atividade III

Determine por inspeção um valor aproximado das raízes reais da equação $2x^5 - 10x + 5 = 0$. Sugestão: utilize valores reais dentro do intervalo $[-2,2]$. E pesquise se existe alguma fórmula envolvendo somente as operações definidas em $\mathbb{C}$ e extração de raízes para a solução de uma equação algébrica geral de grau 5.

Roteiro da Atividade III:

1. A equação possui no máximo quantas raízes?
2. Utilize a calculadora para determinar os valores aproximados das raízes. Compare seu resultado com os outros grupos.
3. Com o uso do *GeoGebra* faça o gráfico da função $f(x) = 2x^5 - 10x + 5 = 0$
4. Compare o seu resultado com as raízes determinada pelo *GeoGebra*.
5. Pesquise uma solução que utilize fórmulas correspondentes com Atividade II.