UNIVERSIDADE FEDERAL DO PARÁ
CAMPUS UNIVERSITÁRIO DE CASTANHAL
FACULDADE DE MATEMÁTICA
CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

Josué Augusto Gonçalves da Silva

EXTENSÕES ALGÉBRICAS DE CORPOS

CASTANHAL-PA
2018

Josué Augusto Gonçalves da Silva

EXTENSÕES ALGÉBRICAS DE CORPOS

Trabalho de conclusão de curso apresentado na Universidade Federal do Pará-UFPA do Campus de Castanhal, como requisito parcial para obtenção do título de graduado no curso de Licenciatura Plena em Matemática, sob orientação do Professor Dr. Frayzer Lima de Almeida.

Castanhal-PA
2018

Josué Augusto Gonçalves da silva

EXTENSÕES ALGÉBRICAS DE CORPOS

Trabalho de conclusão de curso apresentado na Universidade Federal do Pará-UFPA do Campus de Castanhal, como requisito parcial para obtenção do título de graduado no curso de Licenciatura Plena em Matemática, sob orientação do Professor Dr. Frayzer Lima de Almeida.

Aprovada em: ___/___/___

Conceito:

Banca examinadora

_____

Prof. Dr. Frayzer Lima de Almeida

Orientador

_____

Prof. Dr. Edilberto Oliveira Rozal

Membro da banca

Resumo

O trabalho visa apresentar um estudo sobre extensões algébricas de corpos, mais especificamente dos racionais $\mathbb{Q}$, onde será exibida ao longo do desenvolvimento uma série de definições algébricas tais como, grupos, anéis e corpos, que contribuirão para explicar os teoremas ao longo do trabalho. A teoria de Galois nos dá uma bela resposta sobre algumas definições de construção de corpos K, onde $\mathbb{Q} \subset K \subset \mathbb{C}$, por meio de equações polinomiais através de um processo chamado de adjunção de raízes de um polinômio $P(x)$, onde $P(x) \in K[x]$ e $K \in K[x]$. Nesse contexto, daremos ênfase em demonstrar o teorema de isomorfismo de corpos K ligados a raízes algébricas e transcendente de polinômios irredutíveis, com $\alpha \in K \ P(\alpha) = 0$ e $P(\alpha) \neq 0$, respectivamente, que servirá para explicar o processo de adjunção de raízes de um polinômio para trabalhos futuros.

Palavras-chave: Grupos, anéis, corpos e extensões de corpos.

Abstract

This paper aims to present a study of the algebraic extensions of the bodies, more specifically of the rational $\mathbb{Q}$, where a series of algebraic definitions such as groups, rings and bodies will be presented throughout the development, which will contribute to explain the theorems. Galois theory gives us a nice answer about some definitions of body K, where $\mathbb{Q} \subset K \subset \mathbb{C}$, building by means of polynomials equations through a process called the adjunction of roots of a polynomial $P(x)$, where $P(x) \in K[x]$ and $K \in K[x]$. In this context, we will emphasize in demonstrating the isomorphism theorem of bodies K linked to algebriac roots and transcendent irreducible polynomials, with $\alpha \in K, P(\alpha) = 0$ and $P(\alpha) \neq 0$, respectively, which will serve to explain the process of the adjunction of roots of a polynomial to future work.

Key words: Groups, Rings, Bodies and Body Extensions

Sumário

1.INTRODUÇÃO

A obra de Galois foi importante não só por tornar a noção abstrata de grupo na teoria das equações, mas também por levar, através de contribuições de Richard Dedekind, que introduziu em 1871 a noção de ideal, Leopold Kronecker e Ernst Eduard kummer, ao que se pode chamar tratamento aritmético da álgebra, algo parecido com a aritmetização da análise.

Inspirado pela prova de Abel da irresolubilidade por radicais da equação quintica, que hoje é conhecida como teorema de Abel-Ruffini pela seguinte questão: “Porque não existe uma fórmula para raízes de uma equação polinomial de quinta ordem (ou maior) em termos de coeficientes de polinômios, usando somente as operações algébricas usuais (adição, subtração, multiplicação e divisão) e aplicação de radicais (raiz quadrada, raiz cúbica, etc.)?, Galois descobriu que uma equação algébrica irredutível é resolúvel por radicais se e só se seu grupo, isto é, grupo de permutações sobre suas raízes, é resolúvel.

De modo geral, a teoria de Galois, explorado pela primeira vez no século XIX, usa grupo de permutações para descrever como as várias raízes de uma equação polinomial estão relacionadas umas com as outras. Não irei aprofundar sobre a teoria de Galois, mas seus conceitos serão indispensáveis para o desenvolvimento do estudo de extensões algébricas.

Uma das características da matemática do último século foi a sua tendência para abstração. Das áreas da chamada Álgebra moderna, só a teoria abstrata dos anéis e ideal é puramente um produto do século XX. O primeiro matemático a dar a noção de anéis foi Adolf Fraenkel, mas foi Richard Dedekind quem introduziu o conceito de anéis através de equações polinomiais e, também de corpos.

Nesse sentido, apresentaremos no primeiro momento um estudo sobre estruturas algébricas expondo seus principais conceitos e propriedades sobre Grupos; já no segundo capitulo apresentaremos os conceitos de anéis e corpos. E por fim, estudaremos as definições de extensões algébricas dos corpos demonstrando ao final desse trabalho o teorema de isomorfismo de corpos atrelados a polinômios, com algumas aplicações sobre o tal.

1.1. Grupos

Em 1824 o matemático norueguês Niels Henrik Abel (1802-1829) provou que não há uma fórmula geral por radicais para resolver as equações polinomiais de graus maiores ou iguais a 5. Dessa maneira, surge uma questão: Por que algumas equações algébricas com graus maiores ou iguais a 5 são solúveis por radicais e outras não?". A resposta para essa pergunta foi dada pelo matemático francês Evariste Galois (1811-1832). Galois associou a cada equação um grupo formado por permutações de suas raízes e condicionou a resolubilidade por radicais a uma propriedade desse grupo. Surge assim, a teoria de Galois que, grosso modo, procura descrever as simetrias das equações satisfeitas pelas soluções de uma equação polinomial; e essa é a origem histórica do conceito de grupos.

Com o tempo, a ideia de grupos se mostrou um instrumento muito importante para a organização e o estudo de várias partes da matemática.

Definição 1.1. Um grupo é um par ordenado $(G, *)$; em que G é um conjunto não vazio, munido de uma operação denotada por $*$, tal que para todo $x, y \ e \ z \in G$, as seguintes condições são satisfeitas:

(i) $(x * y) * z = x * (y * z)$ (Associatividade);

(ii) Existe um elemento $e \in G$, tal que $e * x = x * e = x$ (Existência do elemento neutro);

(iii) Para cada elemento $x \in G$, existe $b \in G$, tal que $x * b = b * x = e$ (Existência do elemento simétrico).

(iv) Para qualquer $x \ e \ y \in G$, tal que $x * y = y * x$, dizemos que $(G, *)$ é um grupo comutativo ou abeliano.

Observação 1.1. A operação é uma função do tipo:

$$* : G \times G \longrightarrow G$$
$$(x, y) \longrightarrow x * y$$

Quando a operação do grupo é uma soma conhecida, dizemos que $(G,+)$ um grupo aditivo. O mesmo acontece quando a operação é uma multiplicação conhecida, neste caso dizemos que $(G,.)$ é um grupo multiplicativo. Quando ficar subentendida a existência da operação, vamos nos referir ao grupo $(G,*)$ simplesmente por grupo G.

Exemplo 1.1.

$M_2(\mathbb{R})$ é um grupo em que a operação $+$ é soma usual de matrizes.

Sejam $A=\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}$, $B=\begin{pmatrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{pmatrix}$ e $C=\begin{pmatrix}c_{11} & c_{12}\\ c_{21} & c_{22}\end{pmatrix} \in M_2(\mathbb{R})$

Então temos:

Associatividade.

$$A+(B+C)=\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}+\left(\begin{pmatrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{pmatrix}+\begin{pmatrix}c_{11} & c_{12}\\ c_{21} & c_{22}\end{pmatrix}\right)= =$$

$$=\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}+\left(\begin{pmatrix}b_{11}+c_{11} & b_{12}+c_{12}\\ b_{21}+c_{21} & b_{22}+c_{22}\end{pmatrix}\right)=$$

$$=\begin{pmatrix}a_{11}+(b_{11}+c_{11}) & a_{12}+(b_{12}+c_{12})\\ a_{21}+(b_{21}+c_{21}) & a_{22}+(b_{22}+c_{22})\end{pmatrix}=$$

$$=\begin{pmatrix}(a_{11}+b_{11})+c_{11} & (a_{12}+b_{12})+c_{12}\\ (a_{21}+b_{21})+c_{21} & (a_{22}+b_{22})+c_{22}\end{pmatrix}=$$

$$=\begin{pmatrix}a_{11}+b_{11} & a_{12}+b_{12}\\ a_{21}+b_{21} & a_{22}+b_{22}\end{pmatrix}+\begin{pmatrix}c_{11} & c_{12}\\ c_{21} & c_{22}\end{pmatrix}=$$

$$=\left(\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}+\begin{pmatrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{pmatrix}\right)+\begin{pmatrix}c_{11} & c_{12}\\ c_{21} & c_{22}\end{pmatrix}=(A+B)+C$$

Lembrando que a operação soma foi demonstrada com a associatividade com números reais.

Existência do elemento neutro. Seja a matriz nula $E=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix} \in M_2(\mathbb{R})$

Assim temos:

$$A+E=\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}+\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}=\begin{pmatrix}a_{11}+0 & a_{12}+0\\ a_{21}+0 & a_{22}+0\end{pmatrix}=$$

$$=\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}=A=\begin{pmatrix}0+a_{11} & 0+a_{12}\\ 0+a_{21} & 0+a_{22}\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}+\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}=E+A$$

Logo E é o elemento neutro

Existência do elemento simétrico. Seja $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_2(\mathbb{R})$ qualquer e use $A' = \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}$. Então temos:

$$A + A' = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} - a_{11} & a_{12} - a_{12} \\ a_{21} - a_{21} & a_{22} - a_{22} \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = E \text{ e}$$

$$A' + A = \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix} + \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} -a_{11} + a_{11} & -a_{12} + a_{12} \\ -a_{21} + a_{21} & -a_{22} + a_{22} \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = E$$

Portanto A' é simétrico de A, logo $M_2(\mathbb{R})$ é um grupo.

Grupo abeliano. Sejam $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ e $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in M_2(\mathbb{R})$

Então temos:

$$A + B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix} =$$

$$\begin{pmatrix} b_{11} + a_{11} & b_{12} + a_{12} \\ b_{21} + a_{21} & b_{22} + a_{22} \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} + \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = B + A$$

Com isso $M_2(\mathbb{R})$ é um grupo abeliano

Exemplos de grupos: O conjunto dos inteiros $(\mathbb{Z}, +)$ com a adição usual é um Grupo.

O conjunto dos números reais não nulos $(\mathbb{R}^*, .)$ com a operação multiplicação usual é Grupo.

O conjunto dos números complexos $(\mathbb{C}^*, .)$ é um grupo multiplicativo comutativo, pois o produto de dois números complexos $z = a + bi$ e $w = c + di$ é definido por $zw = (ac - bd) + (ad + bc)i$. Se verificarmos por cálculos algébricos observar-se que $(\mathbb{C}^*, .)$ a operação é associativo e o elemento neutro é $1 = 1 + 0i$, e o inverso de um elemento $z = a + bi$, não nulo, é $z^{-1} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2} i$

1.2. Subgrupos

Definição 1.2. Sejam (G,$*$) Grupo e $H \subseteq G$ não vazio. Dizemos que H é subgrupo de G se:

(i) H é fechado com relação à operação $*$, ou seja, se $x, y \in H$ tem-se $x * y \in H$;
(ii) (H ,$*$) é Grupo

Lema 1.1. Sejam (G,$*$) um grupo, (H,$*$) um subgrupo de (G ,$*$) e $y \in H$ qualquer. Então o inverso de y em H é o mesmo inverso de y em G e o elemento neutro de H é o mesmo elemento neutro de G.

Demonstração: Seja $y \in H$ qualquer e denote y'' o inverso de y em H e por y' o inverso de y em G. Devemos mostrar que $y'' = y'$. E seja e_h o elemento neutro de H e e_g o elemento neutro de G. Então temos:

$$\begin{aligned} y * y" = e_h = e_h * e_g = e_h * (y * y') = (e_h * y) * y' \\ = y * y' \Rightarrow y' * (y * y") = y' * (y * y') \\ \Rightarrow (y' * y) * y" = (y' * y) * y' \Rightarrow e_g * y" \\ = e_g * y' \end{aligned}$$

Logo, $y'' = y'$

Também temos:

$$e_h = y * y" = y * y' = e_g \Rightarrow e_h = e_g$$

Como queríamos demonstrar.

■

Proposição 1.2. Sejam (G,$*$) grupo e $H \subseteq G$ não vazio. H é subgrupo de G se, e somente se, para qualquer $x, y \in H$ tem-se $x * y' \in H$, em que y' é o simétrico de y.

Exemplo 1.2. Considere o grupo aditivo M_2 ($\mathbb{R}$). Vamos mostrar que o conjunto $Sl_2(\mathbb{R}) = \left\{ \begin{pmatrix} x & y \\ z & -x \end{pmatrix} ; x, y \, e \, z \in \mathbb{R} \right\}$ é um subgrupo de $M_2(\mathbb{R})$

i) Verifica-se que $Sl_2(\mathbb{R})$ não é vazio. De fato, não é, pois $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ pertence $Sl_2(\mathbb{R})$

i) Sejam $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & -a_{22} \end{pmatrix}$, B= $\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & -b_{22} \end{pmatrix} \in Sl_2(\mathbb{R})$ quaisquer, assim temos:

$$A + (-B) = \begin{pmatrix} a_{11} - b_{11} & a_{12} - b_{12} \\ a_{21} - b_{21} & -a_{22} + b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} - b_{11} & a_{12} - b_{12} \\ a_{21} - b_{21} & -(a_{22} - b_{22}) \end{pmatrix}$$
$$\in Sl_2(\mathbb{R})$$

Portanto $Sl_2(\mathbb{R})$ é subgrupo de $M_2(\mathbb{R})$.

1.3. Homomorfismo de Grupos

Agora falaremos sobre homomorfismo de grupos, em que nada mais é uma correspondência entre dois Grupos, sujeita a algumas regras.

Definição 1.3. Seja $(G,*)$ um grupo munido da operação $*$ e $(H,.)$ um grupo munido da operação . , e seja f uma aplicação de G em H, definimos homomorfismo de grupos toda aplicação $f: G \longrightarrow H$, tal que, quaisquer que sejam $x, y \in G$ tem-se:

$$f(x * y) = f(x).f(y)$$

Observação 1.2. Dizemos que uma aplicação $f: G \longrightarrow H$ é chamado de homomorfismo nulo, se para todo $x \in G$ tem-se $f(x) = e_h$ em que, e_h é o elemento neutro de H.. Sejam $x, y \in G$ quaisquer, então temos:

$$f(x * y) = e_h = e_h.e_h = f(x).f(y)$$

Exemplo 1.3. A aplicação $f: \mathbb{Z} \longrightarrow \mathbb{C}^*$ definida por $f(m) = i^m$ é um homomorfismo de grupos. É preciso notar, primeiro que em casos como esses as operações são usuais e devem ser pressupostas. Portanto, $\mathbb{Z}$ é um grupo aditivo e $\mathbb{C}^*$ grupo multiplicativo. Então temos:

$$f(m + n) = i^{m+n} = i^m.i^n = f(m).f(n)$$

Logo fica provado que se trata de homomorfismo

Também pode-se observar que f não é homomorfismo injetor. Para isso tem-se um contraexemplo. De fato, $f(4) = i^4 = 1$ e $f(0) = i^0 = 1$, ou seja, $4 \neq 0$ e $f(4) \neq f(0)$. Ainda mais, podemos verificar que f não é homomorfismo sobrejetor, pois $Im(f) = \{1, i, -1, -i\}$ e o contradomínio é $\mathbb{C}^*$, ou seja, $Im(f) \neq \mathbb{C}^*$

Definição 1.4. Um homomorfismo injetor é chamado de momorfismo. Um homomorfismo sobrejetor é chamado de epimorfismo. Um homomorfismo bijetor é chamado de isomorfismo. Um homomorfismo $f: G \longrightarrow G$ é chamado de endomorfismo. Um isomorfismo $f: G \longrightarrow G$ é chamado de automorfismo.

Proposição 1.3. Sejam G, J grupos multiplicativos cujos elementos neutros indicaremos por e_g, e_J, respectivamente, e $f: G \longrightarrow J$ um homomorfismo de grupos. Então $f(e_g) = e_J$ e para qualquer $x \in G$ tem-se $f(x^{-1}) = f(x)^{-1}$

Demonstração: De forma bem clara $e_g \,.\, e_g = e_g$ (pois e_g é o elemento neutro de G) e $e_J . f(e_g) = f(e_g)$ (pois $f(e_g) \in J$ e e_J é o elemento de neutro de J). Levando-se em conta isso e a hipótese de que f é um homomorfismo:

$$f(e_g).f(e_g) = f(e_g \,.\, e_g) = f(e_g) = e_J.f(e_g)$$
$$\Longrightarrow f(e_g).f(e_g) = e_J.f(e_g)$$
$$\Longrightarrow f(e_g).f(e_g).f(e_g)^{-1} = e_J.f(e_g).f(e_g)^{-1}$$
$$\Longrightarrow f(e_g) = e_J$$

Agora seja $x \in G$ qualquer. Da proposição anterior assim temos,

$$f(x).f(x^{-1}) = f(x.x^{-1}) = f(e_g) = e_J = f(x).f(x)^{-1}$$
$$\Longrightarrow f(x).f(x^{-1}) = f(x).f(x)^{-1}$$
$$\Longrightarrow f(x)^{-1}.f(x).f(x^{-1}) = f(x)^{-1}.f(x).f(x)^{-1}$$
$$\Longrightarrow f(x^{-1}) = f(x)^{-1}$$

Portanto está provado que $f(e_g) = e_J$ e $f(x^{-1}) = f(x)^{-1}$

■

Definição 1.5. Seja $f: G \longrightarrow J$ um homomorfismo de grupos. O núcleo de f, denotado por $N(f)\ ou\ Ker(f)$ é o seguinte conjunto.

$$N(f) = \{\, x \in G: f(x) = e_J\}$$

Proposição 1.4. Sejam G, J grupos quaisquer, H um subgrupo de G e $f: G \longrightarrow J$ homomorfismo. Então $f(H) = \{f(x); x \in H\}$ é um subgrupo de J.

Demonstração:

$i)$ Como $e_g \in H$, porque H é um subgrupo de G, então $f(e_g) = e_j \in f(H)$ e, portanto, $f(H) \neq \emptyset$.

$ii)$ Sejam $c, d \in f(H)$. Então $f(a) = c\ e\ f(b) = d$, para convenientes elementos $a, b \in H$. Logo, $c.d^{-1} = f(a).[f(b)]^{-1} = f(a).f(b^{-1}) = f(a.b^{-1})$. Como $a.b^{-1} \in H$, pois por hipótese, H é um subgrupo de G, então $c.d^{-1} \in f(H)$

■

Em outros termos, a proposição anterior garante que um homomorfismo de grupos $f: G \longrightarrow J$ transforma subgrupos de G em subgrupos de J. Em particular, $Im(f)$ é um subgrupo de J

Proposição 1.5. Sejam G, J grupos quaisquer e $f: G \longrightarrow J$ um homomorfismo. Então

$i)$ $N(f)$ é um subgrupo de G;

$ii)$ $Im(f)$ é um subgrupo de J

Demonstração: (i) $N(f)$ é não vazio, pois $f(e_g) = e_J$ **(proposição 1.3)** $e_g \in N(f)$ e, portanto $N(f) \neq \emptyset$. Por outro lado, se $a, b \in N(f)$, então $f(a) = f(b) = e_J$ e, portanto:

$$f(a.b^{-1}) = f(a).f(b^{-1}) = f(a).[f(b)]^{-1} = e_J.{e_J}^{-1} = e_J$$

Isso mostra que $a.b^{-1} \in N(f)$.

O item (ii) segue da **proposição 1.4**, pois a $Im(f) = f(G)$

■

Proposição 1.6. Sejam G, J grupos e $f: G \longrightarrow J$ um homomorfismo. Então $N(f) = \{e_g\}$ se, e somente se, f é injetiva.

Demonstração:

($\Longleftarrow$) Por hipótese, f é injetor e temos de mostrar que o único elemento de $N(f)$ é e_g (elemento neutro de G). Para isso, toma-se $a \in N(f)$ e demonstra-se que necessariamente $a = e_g$. De fato, como $a \in N(f)$ então $f(a) = e_J$. Mas devido a **proposição 1.3.** $f(e_g) = e_J$. Portanto, $f(a) = f(e_g)$. Como, porém, f é injetiva, por hipótese, então $a = e_g$

($\Longrightarrow$) Sejam $x_1, x_2 \in G$ elementos tais que $f(x_1) = f(x_2)$. Multiplicando-se cada membro dessa igualdade por $[f(x_2)]^{-1}$, obtém-se $f(x_1).[f(x_2)]^{-1} = e_J$. Mas sabe-se que $f(x_1).[f(x_2)]^{-1} = f(x_1.{x_2}^{-1})$ **(referente da proposição 1.3)**. Então $f(x.{x_2}^{-1}) = e_J$, o que mostra que $x.{x_2}^{-1} \in N(f) = \{e_J\}$. Portanto, $x_1.{x_2}^{-1} = e_J$, logo $x_1 = x_2$. De onde f é injetor, como queríamos provar.

■

1.4. Grupos Cíclicos, Classes Laterais, Subgrupos Normais e Grupos Quocientes.

Considere $(\mathrm{G}, *)$ um grupo qualquer e H um subgrupo qualquer de G. Nas demonstrações seguintes das proposições usa-se a notação multiplicativa, por simplicidade. Portanto, quando referir-se a G como grupo, usa-se xy ao invés de $x * y$ e, para o elemento simétrico de x em G denota-se por x^{-1}.

Definição 1.6. Seja G um grupo multiplicativo. Se $a \in G$ e $m \in G$ um número inteiro, define-se a potência m-ésima de a, denotado por a^m, da seguinte maneira:

$i)$ Se $m \geq 0$, por recorrência, da seguinte forma:

$$a^0 = e_g (elemento\ neutro\ de\ G)$$

$$a^m = a^{m-1}a, se\ m \geq 1$$

$ii)$ Se $m < 0$

$$a^m = (a^{-m})^{-1}$$

A definição por recorrência deve ser interpretada assim: $a^1 = a^{1-1}a = a^0 a = e_g a = a$; $a^2 = a^{2-1}a = a^1 a = aa$; $a^3 = a^{3-1}a = a^2 a = (aa)a$, etc. Uma sequência imediata dessa definição é que, para todo inteiro m, vale ${e_g}^m = e_g$

Proposição 1.7. Seja G um grupo multiplicativo qualquer. Se m, n são números inteiros e $a \in G$, então:

(i) $a^m a^n = a^{m+n}$;

(ii) $a^{-m} = (a^m)^{-1}$;

(iii) $(a^m)^n = a^{mn}$.

Demonstração:

(i) Demonstra-se por indução sobre n o seguinte caso: $n \geq 0$ e $m + n \geq 0$.

Se $n = 0$, então $a^m a^n = a^m a^0 = a^m e_g = a^m = a^{m+0} = a^{m+n}$. Portanto, a propriedade é verdadeira. Seja $r \geq 0$ e suponha-se que, para qualquer inteiro m tal que $m + n \geq 0$, se tenha $a^{m+r} = a^m a^r$. Então $a^m a^{r+1} = a^m (a^r a) = (a^m a^r)a = a^{m+r} a = a^{(m+r)+1}$. Logo está provado.

(ii) Observar-se que, devido (i), $a^{-m} a^m = a^{(-m)+m} = a^0 = e_g$, analogamente, $a^m a^{-m} = e_g$. Portanto, cada uma dessas potências é inversa da outra. Logo $a^{-m} = (a^m)^{-1}$

(iii) Suponha-se $n < 0$. Então:

$$(a^m)^n = [(a^m)^{-n}]^{-1} = (a^{-mn})^{-1} = a^{mn}$$

■

Definição 1.7. Um grupo multiplicativo G será chamado de grupo cíclico se, para algum elemento $a \in G$, denota-se por $[a]$ o subconjunto de G, ou seja, $[a] = \{a^m : m \in \mathbb{Z}\}$, se verificar a igualdade $G = [a]$. O elemento a é chamado de gerador do grupo G. E no caso aditivo temos a seguinte notação $G = \{m.a : m \in \mathbb{Z}\}$

Exemplo 1.4. Seja $\mathbb{C}^*$ um conjunto multiplicativo e seja $I \in \mathbb{C}^*$. Por definição, $[i] = \{i^m : m \in \mathbb{Z}\}$. Mas, como se vê no estudo dos números complexos, esse conjunto so tem 4 elementos, $1, i, -1, -i$ obtidos respectivamente quando $m = 4q, m = 4q + 1, m = 4q + 2\ em = 4q + 3$, portanto, $[i] = \{1, i, -1, -i\}$. Logo $I = [i]$ é cíclico.

Exemplo 1.5. O grupo aditivo $\mathbb{Z}$ é cíclico, pois todos os seus elementos são múltiplos de 1 ou -1. De fato, $\mathbb{Z} = \{m.1; m \in \mathbb{Z}\}$ ou $\mathbb{Z} = \{m.(-1); m \in \mathbb{Z}\}$. Portanto, $\mathbb{Z} = [1] = [-1]$. Os números 1 e -1 são, na verdade, os únicos geradores de $\mathbb{Z}$.

Proposição 1.8. Sejam G um grupo e H um subgrupo de G e $x, y \in G$ qualquer. A relação

$$yRx \Leftrightarrow x^{-1}y \in H$$

É uma relação de equivalência em G.

Demonstração:

(i) **(Reflexiva)** seja $x \in G$ qualquer. Temos, $x^{-1}x = e_g \in H$, logo xRx

(ii) **(Simétrica**) sejam $x, y \in G$ quaisquer. Temos que,

$$yRx \Longrightarrow x^{-1}y \in H \Longrightarrow (x^{-1}y)^{-1} = y^{-1}x \in H \Longrightarrow xRy$$

(iii) **(Transitiva)** sejam $x, y, z \in G$ quaisquer, tais que yRx e xRz. Então, $x^{-1}y \in H$ e $z^{-1}x \in H$. Assim,

$$(z^{-1}x).(x^{-1}y) \in H \Longrightarrow z^{-1}y \in H \Longrightarrow yRz$$

Analogamente, se G é um grupo e $H \subset G$, a relação

$$xR^*y \Leftrightarrow yx^{-1} \in H$$

É também uma relação de equivalência.

Agora se verifica a seguinte relação,

$$yRx \Leftrightarrow x^{-1}y \in H \Leftrightarrow \exists h \in H\ , tal\ que$$

$$x^{-1}y = h \Leftrightarrow y = xh \Leftrightarrow y \in xH = \{xh; h \in H\}$$

A classe de equivalência de $x \in G$, definida pela relação R, é:

$$xH = \{y \in G; yRx\}$$

De maneira semelhante tem-se a relação $xR^*y \Leftrightarrow yx^{-1} \in H$, a classe de equivalência de $y \in G$ é:

$$\{y \in G; xR^*y\} = Hx$$

A partir dessas análises, temos as seguintes definições:

Definição 1.8. A classe de equivalência $xH = \{xh; h \in H\}$ é chamada de classe lateral de x à esquerda de H em G

Definição 1.9. A classe de equivalência $Hx = \{hx; h \in H\}$ é chamada de classe lateral de x à direita de H em G

Definição 1.10. Um subgrupo H de um grupo G é chamado de subgrupo normal se, para todo $x \in G$, se verifica:

$$xH = Hx$$

Exemplo 1.6. Seja $f: G \longrightarrow J$ homomorfismo de grupos. Mostra-se que $N(f)$ é um subgrupo normal de G.

Na **proposição 1.5** mostrou-se que $N(f)$ é um subgrupo de G. Agora se mostra que todo $x \in G$ tem-se $xH = Hx$. Demonstra-se por dupla inclusão.

Primeira inclusão $xN(f) \subseteq N(f)x$. Seja $y \in xN(f)$ qualquer. Então, existe $n \in N(f)$ tal que $y = xn$. Sabendo que $N(f) = \{ x \in G: f(x) = e_J\}$. Note que

$$y = xn = xnx^{-1}x$$

Assim, temos

$$f(xnx^{-1}) = f(x)f(n)f(x^{-1}) = f(x)e_jf(x)^{-1} = f(x)f(x)^{-1} = e_j$$

Portanto, $xnx^{-1} \in N(f)$. Logo existe $n_1 \in N(f)$ tal que, $xnx^{-1} = n_1$

Assim, temos $y = xnx^{-1}x = n_1x \in N(f)x$

Dessa forma, conclui-se que $xN(f) \subseteq N(f)x$.

Analogamente, demonstra-se que $N(f)x \subseteq xN(f)$

Portanto, $xN(f) = N(f)x$. E com isso, $N(f)$ é um subgrupo normal de G.

■

Sejam G um grupo e $H \subseteq G$ um subgrupo normal de G. Sabe-se que $x, y \in G$

$$yRx \Leftrightarrow x^{-1}y \in H$$

É uma relação de equivalência em G. O conjunto a seguir:

$$G/H = \{xH; x \in G\} = \{Hx; x \in G\}$$

É o conjunto das classes de equivalência módulo H

Lema 1.2. Sejam G um grupo e H um subgrupo de G e $x, y \in G$ quaisquer. Então:

(i) $y \in xH \Leftrightarrow xH = yH$

(ii) $y \in Hx \Leftrightarrow Hx = Hy$

Demonstração:

(i) $(\Longrightarrow)$ como $y \in xH$, temos yRx, por simetria temos que xRy. Mostra-se que $xH \subseteq yH$. se $z \in xH$, então zRy. Mas xRy logo, pela transitividade, temos zRy, portanto $z \in yH$

$y \subseteq xH$ é análogo.

$(\Longleftarrow)$ como $y \in yH$ e $yH = xH$, então $y \in xH$

(ii) É semelhante ao item (i), apenas trocamos as posições das letras x, y

Definição 1.11. Sejam G um grupo e H subgrupo normal de G. Nessas condições, o grupo quociente G por H é o par formado pelo conjunto quociente G/H e a restrição aos elementos desse conjunto da multiplicação de subconjuntos de G.

Proposição 1.9. Sejam G um grupo e H subgrupo normal de G. A seguinte operação

$$\cdot : G/H \times G/H \longrightarrow G/H$$

$$(xH, yH) \longmapsto xyH$$

Então $(G/H\ ,\ \cdot)$ é um grupo quociente.

Demonstração:

Mostra-se, primeiro, que a operação está bem definida. Para tanto, sejam $xH, yH, x_1H, y_1H \in G/H$ tais que, $xH = x_1H$ e $yH = y_1H$. Mostraremos que $xyH = x_1y_1H$. Como $xH = x_1H$ e $yH = y_1H$, pelo **Lema 1.2.** temos que $x_1 \in xH$ e $y_1 \in yH$, ou seja, existem $h_1, h_2 \in H$ tais que, $x_1 = xh_1$ e $y_1 = yh_2$. Assim $x_1\, y_1 = \mathrm{x}h_1\mathrm{y}h_2 = \mathrm{x}(h_1\mathrm{y})h_2 = \mathrm{x}(\mathrm{y}h_1)h_2 = \mathrm{x}y(h_1h_2)$

Como $h_3, h_2 \in H$, temos que $h_1h_2 \in H$, ou seja, existe $h \in H$ tal que $h_3h_2 = h$

Portanto, $x_1\, y_1 = xy(h_1h_2) = xyh \in xyH$

Logo, pelo **Lema 1.2**. temos que $xyH = x_1\, y_1H$. Com isso, conclui-se que a operação é bem definida.

Agora prova-se os axiomas de grupos

Associatividade: Sejam $xH, yH\ , zH \in G/H$ quaisquer. Assim,

$$(xH \cdot yH) \cdot zH = xyH \cdot zH = (xy)zH = x(yz)H = xH \cdot yzH = xH \cdot (yH \cdot zH)$$

Existência do elemento neutro: Considere $eH = H \in G/H$ e dado $xH \in G/H$ qualquer, temos:

$$eH \cdot xH = exH = xH = xH \cdot eH = xeH$$

Logo eH é o elemento neutro de G/H.

Existência do elemento simétrico: seja $xH \in G/H$ qualquer. Note que $x^{-1} \in G/H$, temos:

$$xH \cdot x^{-1}H = xx^{-1}H = eH$$

$$x^{-1}H \cdot xH = x^{-1}xH = eH$$

Logo $x^{-1}H$ é o simétrico de xH. Concluímos então, que $(G/H\,,\ \cdot)$ é um grupo.

O teorema a seguir já foi citato ao longo do trabalho. Porém, daremos mais ênfase demonstrando-o com mais detalhes.

1.5. Teorema do isomorfismo de grupos

Sejam G e J grupos. Dado $f: G \longrightarrow J$ homomorfismo. Agora iremos construir um isomorfismo, a partir de f. Já foi explicado ao longo do trabalho, que um isomorfismo é um homomorfismo injetor e sobrejetor. Vamos resolver por parte essa questão. A construção de um homomorfismo sobrejetor é imediata, basta mudar o contradomínio de f, para $Im(f)$, o que resolve a sobrejetividade. Mas, e a injetividade? Seria o seguinte: Se $x, y \in G$ são tais que $f(x) = f(y)$, então

$$f(x) = f(y) \Longrightarrow f(x)f(y)^{-1} = e_j \Longrightarrow f(x)f(y^{-1}) = f(xy^{-1}) = e_j$$

Isso significa que $xy^{-1} \in N(f)$

Teorema 1.1 (Teorema do isomorfismo para grupos)

Sejam G e J grupos e $f: G \longrightarrow J$ homomorfismo. Então, a função:

$$\varphi: G/N(f) \longrightarrow Im(f)$$

$$xN(f) \longmapsto f(x)$$

É um isomorfismo.

Demonstração: Primeiro vamos verificar se φ está bem definida. Para tanto, sejam $xN(f), yN(f) \in G/N(f)$ quaisquer, tais que $xN(f) = yN(f)$. Assim, yRx, ou seja, $x^{-1}y \in N(f)$. Note que $\varphi\big(xN(f)\big) = f(x)$ e $\varphi\big(yN(f)\big) = f(y)$, então:

$$\varphi\big(xN(f)\big).\left(\varphi\big(yN(f)\big)\right)^{-1} = f(x).\big(f(y)\big)^{-1} = f(x).f(y^{-1}) = f(xy^{-1}) = e_j$$
$$\Longrightarrow \varphi\big(xN(f)\big) = \varphi\big(yN(f)\big)$$

Portanto, φ está bem definida.

Mostra-se agora que φ é um homomorfismo. Sejam $xN(f), yN(f) \in G/N(f)$ quaisquer, assim

$$\varphi\big(xN(f)yN(f)\big) = \varphi\big(xyN(f)\big) = f(xy) = f(x)f(y) = \varphi(xN(f))\varphi(yN(f))$$

Logo φ é um homomorfismo

Mostra-se que φ é injetiva. Seja $xN(f) \in N(\varphi)$. Então

$$\varphi\big(xN(f)\big) = e_j \Longrightarrow f(x) = e_j$$

Logo $x \in N(f)$, assim

$$N(\varphi) = \{xN(f); x \in N(f)\} = \{N(f)\}$$

A classe $e_jN(f) = N(f)$ é o elemento neutro do grupo quociente $G/N(f)$. Com isso, pela **proposição 1.6** temos que φ é injetiva.

Mostra-se, agora, que φ é sobrejetiva. É de imediato. Seja $y \in Im(f)$ qualquer. Então existe $x \in G$ tal que, $f(x) = y$ logo existe $xN(f) \in G/N(f)$ tal que,

$$\varphi\big(xN(f)\big) = f(x) = y$$

Portanto φ é sobrejetiva

Como φ é um homomorfismo injetor e sobrejetor, temos então que, φ é um isomorfismo, ou seja, $G/N(f)$ é isomorfo a $Im(f)$, em notação fica, $G/N(f) \simeq Im(f)$, como queria-se demonstrar.

■

Exemplo 1.7. Dado $m > 1$, seja aplicação $p_m: \mathbb{Z} \longrightarrow \mathbb{Z}_m$ definida por

$$p_m(x) = \bar{x}$$

Vamos mostrar que p_m é um homomorfismo. seja $x, y \in \mathbb{Z}$, sendo $p_m(x) = \bar{x}$ e $p_m(y) = \bar{y}$

$$p_m(x + y) = \overline{x + y} = \bar{x} + \bar{y} = p_m(x) + p_m(y)$$

Logo, p_m é homomorfismo.

A aplicação p_m também é sobrejetor. Se $a \in \mathbb{Z}_m$, então $a = \bar{x}$, para algum $x \in \{0,1,2, \ldots, m-1\}$, e, portanto, $p_m(x) = \bar{x} = a$, com isso é sobrejetor

O núcleo $N(p_m)$ é o conjuto dos inteiros x tais que $\bar{x} = \bar{0}$,ou seja, o conjunto dos inteiros x tais que $x \equiv 0(mod\ m)$, portanto, $N(p_m) = [m] = \{0, \pm m, \pm 2m, \ldots\}$. com isso o teorema do homomorfismo nos garante que $\mathbb{Z}/[m]$ e $\mathbb{Z}_m$ são isomorfos, $\mathbb{Z}/[m] \simeq \mathbb{Z}_m$.

2. ANÉIS, HOMOMORFISMOS E ISOMORFISMOS DE ANÉIS.

Neste capitulo apresenta-se conceitos básicos para o estudo de anéis e dos capítulos subsequentes.

A primeira ideia abstrata formal de anel foi dada pelo Alemão A. Fraenkel (1891-1965), em 1914, embora o nome já estivesse sido introduzido por D. Hilbert (1852-1943) perto do final do século XIX. Essa noção de anel deu-se a partir da ideia de inteiro algébrico. Um número complexo se diz inteiro algébrico se é raiz de um polinômio cujo coeficiente do termo de maior grau é 1 e os demais são números inteiros.

Definição 2.1. Um sistema matemático constituído de um conjunto não vazio $\mathcal{A}$ e um par de operações sobre $\mathcal{A}$, denotado por $(\mathcal{A}, +, *)$ com $+$ (soma) e $*$ (multiplicação), tais que para quaisquer $x, y, z \in \mathcal{A}$.

$$+: \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A} \qquad \text{e} \qquad *: \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}$$

$$(x, y) \longmapsto x + y \qquad\qquad (x, y) \longmapsto x * y$$

As seguintes condições são satisfeitas para que $(\mathcal{A}, +, *)$ seja anel:

(i) $(\mathcal{A}, +)$ é um grupo abeliano, ou seja:

(a) Se $x, y, z \in \mathcal{A}$, então $x + (y + z) = (x + y) + z$ **(associatividade)**

(b) Se $x, y, \in \mathcal{A}$, então $x + y = y + x$ **(comutatividade)**

(c) Existe um número $0_{\mathcal{A}} \in \mathcal{A}$ tal que, qualquer que seja $x \in \mathcal{A}$, $x + 0_{\mathcal{A}} = x$ **(existência do elemento neutro)**

(d) Qualquer que seja $x \in \mathcal{A}$, existe um elemento em $\mathcal{A}$, indicado genericamente por $-x$, tal que $x + (-x) = 0_{\mathcal{A}}$ **(elemento oposto)**

(ii) $(\mathcal{A}, *)$ é associativa na multiplicação, isto é:

Se $x, y, z \in \mathcal{A}$, então $x * (y * z) = (x * y) * z$

(iii) $(\mathcal{A}, +, *)$ a multiplicação é distributiva em relação à adição, então:

Se $x, y, z \in \mathcal{A}$,então $x * (y + z) = x * y + x * z$ e $(x + y) * z = x * z + y * z$

Assim, $(\mathcal{A}, +, *)$ é um anel.

Definição 2.2. Seja $(\mathcal{A}, +, *)$ um anel, então:

(i) Para quaisquer $x, y \in \mathcal{A}$, com a operação multiplicativa, então $x * y = y * x$ é comutativo. Logo $(\mathcal{A}, +, *)$ é um **anel comutativo**.

(ii) $(\mathcal{A}, +, *)$ é um anel com unidade se existe $1_{\mathcal{A}} \in \mathcal{A}$, tal que, $\forall\, x \in \mathcal{A}$ verifica-se a seguinte operação $1_{\mathcal{A}} * x = x * 1_{\mathcal{A}} = x$

(iii) Se $x, y \in \mathcal{A}$, $x * y = 0$, então $x = 0$ ou $y = 0$, dizemos que $(\mathcal{A}, +, *)$ é um **anel sem divisores de zero.**

Se $(\mathcal{A}, +, *)$ é um anel comutativo, com unidade e sem divisores de zero, dizemos que $(\mathcal{A}, +, *)$ é um **domínio de integridade**.

Definição 2.3. Se um domínio de integridade $(\mathcal{A}, +, *)$ satisfazer a propriedade:

(i) Para qualquer $x \in \mathcal{A} - \{0\}$, existe $y \in \mathcal{A}$ tal que $x * \mathrm{y} = \mathrm{y} * \mathrm{x} = 1$, diz-se que $(\mathcal{A}, +, *)$ é um corpo.

Observação 2.1. Será comum usarmos expressões como "Seja $(\mathcal{A}, +, *)$ um anel" ou mesmo "Seja $\mathcal{A}$ um anel". Por simplicidade usa-se a segunda ficando submetido as operações usuais soma e multiplicação. E também, em vez de $x * \mathrm{y}$ usa-se $x\mathrm{y}$ ou $x.\mathrm{y}$ na multiplicação.

Exemplo 2.1. Alguns anéis numéricos importantes, com as operações usuais, são $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_m$. Já $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ são exemplos de corpos munidos das operações usuais.

Exemplo 2.2. Seja $\mathcal{A} = \mathbb{Z}^{\mathbb{Z}} = \{f; f: \mathbb{Z} \longrightarrow \mathbb{Z}\}$. Se $f, g \in \mathcal{A}$, então $f + g$ e fg é um anel.

$$f + g: \mathbb{Z} \longrightarrow \mathbb{Z} \text{ e } (f + g)(x) = f(x) + g(x)$$

Com $x \in \mathbb{Z}$

$$fg: \mathbb{Z} \longrightarrow \mathbb{Z} \text{ e } (fg)(x) = f(x)g(x)$$

Para todo $x \in \mathbb{Z}$

Associatividade na soma: Sejam $f, g, h \in \mathcal{A}$, então qualquer $x \in \mathbb{Z}$, temos:

$$\begin{aligned}\big((f + g) + h\big)(x) &= (f + g)(x) + h(x) = f(x) + g(x) + h(x) \\ &= f(x) + (g + h)(x) = (f + (g + h)(x)\end{aligned}$$

A associatividade na soma é válida em $\mathbb{Z}$

Com isso temos $(f+g)+h = f+(g+h)$

Comutatividade na soma: Sejam $f, g \in \mathcal{A}$, com $x \in \mathbb{Z}$, então:

$$(f+g)(x) = f(x)+g(x) = g(x)+f(x) = (g+f)(x)$$

Logo com a comutatividade da soma nos inteiros, temos $(f+g) = (g+f)$

Existência do elemento neutro na soma: Seja a função $e_{\mathcal{A}}: \mathbb{Z} \longrightarrow \mathbb{Z}$ definida por $e_{\mathcal{A}}(x) = 0$ com $e_{\mathcal{A}} \in \mathcal{A}$. Para todo $x \in \mathbb{Z}$ e $f \in \mathcal{A}$, temos:

$$(f+e_{\mathcal{A}})(x) = f(x)+e_{\mathcal{A}}(x) = f(x)+0 = f(x) = 0+f(x) = e_{\mathcal{A}}(x)+f(x) = (e_{\mathcal{A}}+f)$$

O elemento neutro na soma dos números inteiros é satisfeito, então:

$$f+e_{\mathcal{A}} = e_{\mathcal{A}}+f = f$$

Existência do simétrico na soma: Seja $f \in \mathcal{A}$. Então vai existir $-f \in \mathcal{A}$ tal que, para todo $x \in \mathbb{Z}$, tem-se $(-f)(x) = -f(x)$. Com isso temos:

$$\big(f+(-f)\big)(x) = f(x)+\big(-f(x)\big) = f(x)-f(x) = 0 = e_{\mathcal{A}}(x) \text{ e}$$
$$\big((-f)+f\big)(x) = (-f)(x)+f(x) = -f(x)+f(x) = 0 = e_{\mathcal{A}}(x)$$

Dessa maneira, $-f$ é o elemento simétrico de f. Logo $(\mathcal{A}, +)$ é um grupo abeliano.

Associatividade na multiplicação: Sejam $f, g, h \in \mathcal{A}$, tal que $x \in \mathbb{Z}$, então:

$$\big((f.g).h\big)(x) = (f.g)(x).h(x) = \big(f(x).g(x)\big).h(x) = f(x).g(x).h(x)$$
$$= f(x).\big(g(x).h(x)\big) = f(x).\big(g.h(x)\big) = (f.(g.h)(x))$$

Logo a associatividade na multiplicação é válida, pois:

$$f(gh) = (fg)h$$

Comutatividade na multiplicação: Sejam $f, g \in \mathcal{A}$ e para todo $x \in \mathbb{Z}$, temos:

$$(f.g)(x) = f(x).g(x) = g(x).f(x) = (g.f)(x)$$

A comutatividade do produto em $\mathbb{Z}$, satisfaz:

$$fg = gf$$

Distributividade na multiplicação em relação à soma: Sejam $f, g, h \in \mathcal{A}$ quaisquer e, para todo $x \in \mathbb{Z}$, temos:

$$\big((f+g).h\big)(x) = (f+g)(x).h(x) = \big(f(x)+g(x)\big).h(x)$$
$$= f(x).h(x) + g(x).h(x) = (f.h)(x) + (g.h)(x)$$

Logo a distributiva na soma nos números inteiros é válida, pois:

$$(f+g)h = fh + gh \text{ e}$$
$$f(g+h) = fg + fh$$

Existência do elemento neutro na multiplicação: Seja $f \in \mathcal{A}$ qualquer. Considere a função $e: \mathbb{Z} \longrightarrow \mathbb{Z}$, tal que $e(x) = 1$ com $e \in \mathcal{A}$ para todo $x \in \mathbb{Z}$, temos:

$$(f.e)(x) = f(x).e(x) = f(x).1 = f(x) = 1.f(x) = e(x).f(x) = (e.f)(x)$$

Dessa forma, e é o elemento neutro de $\mathbb{Z}$.

$$(fe) = (ef) = f$$

Portanto, conclui-se que $(\mathcal{A}, +, *)$ é um anel comutativo e com unidade.

Definição 2.4. Seja $(\mathcal{A}, +, *)$ um anel e $\mathcal{B}$ um subconjunto não vazio de $\mathcal{A}$. Diz-se que $\mathcal{B}$ é um subanel de $\mathcal{A}$ se:

(i) $\mathcal{B}$ é fechado para as operações dotam o conjunto $\mathcal{A}$ da estrutura de anel, ou seja, para todo $x, y \in \mathcal{B}$ tem-se $x - y \in \mathcal{B}$ e $x.y \in \mathcal{B}$

(ii) $(\mathcal{B}, +, *)$ Tambem é um anel

Exemplo 2.3. As operações usuais dos conjuntos numéricos:

$\mathbb{Z}$ é um subanel de $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. $n.\mathbb{Z}$ é um subanel de $\mathbb{Z}$ e, também, $\mathbb{Z}[\sqrt{p}]$ é um subanel de $\mathbb{Q}[\sqrt{p}]$ e este é subanel de $\mathbb{R}$.

Proposição 2.1. Seja $\mathcal{A}$ um anel e $\mathcal{B}$ um subconjunto não vazio de $\mathcal{A}$. Então $\mathcal{B}$ é um subanel de $\mathcal{A}$ se, e somente, se $x - y$, $x.y \in \mathcal{B}$, sempre que $x, y \in \mathcal{B}$

Demonstração: $\Longrightarrow$ seja $\mathcal{B}$ um subanel de $\mathcal{A}$. Pela definição ocorre que $\mathcal{B}$ é um subgrupo abeliano de $\mathcal{A}$. Portanto $x - y \in \mathcal{B}$ sempre que $x, y \in \mathcal{B}$ e, também, $x.y \in \mathcal{B}$ sempre que $x, y \in \mathcal{B}$

$\Leftarrow$ Por hipótese, se $x, y \in \mathcal{B}$, então $x - y \in \mathcal{B}$. Isso prova que $\mathcal{B}$ é um subgrupo aditivo de $\mathcal{A}$. E a operação soma é fechada, assim como na multiplicação $x.y \in \mathcal{B}$ com $x, y \in \mathcal{B}$

Agora nos resta mostrar os itens (ii) e (iii) das propriedades de anéis, para que $\mathcal{B}$ seja um anel.

Se $x, y, z \in \mathcal{B}$, então $x, y, z \in \mathcal{A}$ e, portanto, $x(yz) = (xy)z$ que mostra a associatividade na multiplicação em $\mathcal{B}$.

Se $x, y, z \in \mathcal{B}$, então $x, y, z \in \mathcal{A}$, portanto $(x + y)z = xz + yz$ e $x(y + z) = xy + xz$. Logo, isso mostra que a distributividade da multiplicação em relação a soma em $\mathcal{B}$. Portanto $\mathcal{B}$ é um anel, como queria-se demostrar.

■

Exemplo 2.4. Seja $\mathcal{B}$ um conjunto, tal que $\mathcal{B} = \{x + y\sqrt{2}\,; x, y \in \mathbb{Z}\}$. Mostra-se que $\mathcal{B}$ é um subanel de $\mathcal{A} = \mathbb{R}$, pois, se $x + y\sqrt{2}, z + w\sqrt{2} \in \mathcal{B}$, então:

$$\left(x + y\sqrt{2}\right) - \left(z + w\sqrt{2}\right) = (x - z) + (y - w)\sqrt{2} \in \mathcal{B}$$

E,

$$\begin{aligned}\left(x + y\sqrt{2}\right).\left(z + w\sqrt{2}\right) &= xz + xw\sqrt{2} + zy\sqrt{2} + 2yw \\ &= (xz + 2yw) + (xw + zy)\sqrt{2} \in \mathcal{B}\end{aligned}$$

Portanto, $\mathcal{B}$ é um subanel de $\mathcal{A} = \mathbb{R}$

Definição 2.5. Um subanel $\mathcal{B}$ de um corpo K é chamado um subcorpo de K, se dado $x \in \mathcal{B} - \{0\}$ existe $y \in \mathcal{B}$ tal que $xy = 1$

Exemplo 2.5. Observe que $\mathbb{Q}$ é um subcorpo de $\mathbb{R}$, já $\mathbb{R}$ é subcorpo de $\mathbb{C}$. $\mathbb{Q}[\sqrt{p}]$ é um subcorpo de $\mathbb{R}$

Proposição 2.2. Sejam K um corpo e $\mathcal{B}$ um subconjunto não vazio de K. Para que $\mathcal{B}$ seja um subcorpo de K é necessário e suficiente que:

(i) $0,1 \in \mathcal{B}$

(ii) Se $x, y \in \mathcal{B}$, então $x - y \in \mathcal{B}$

(iii) Se $x, y \in \mathcal{B}$ $y \neq 0$, então $xy^{-1} \in \mathcal{B}$

Demonstração: Por brevidade, demonstra-se apenas a condição suficiente. Por hipótese temos $\mathcal{B}$ um subgrupo do grupo aditivo K. Além disso $x, y \in \mathcal{B}^*$, então $x, y \in \mathcal{B}$ e $y \neq 0$ e, daí, $xy^{-1} \in \mathcal{B}$ por hipótese. Mas, $x.y^{-1} \neq 0$ por estarmos num corpo, então $xy^{-1} \in \mathcal{B}^*$. Logo $\mathcal{B}^*$ é um subgrupo do grupo multiplicativo K^*. $x.0 = 0.x = 0$, qualquer que seja $x \in \mathcal{B}$. Como a distributividade da multiplicação em relação à soma, por valerem em K, também vale em $\mathcal{B}$. Com isso, $\mathcal{B}$ é um subcorpo de K

■

Exemplo 2.6. Seja $\mathcal{B}$ um conjunto não vazio, onde $\mathcal{B} = \{x + y\sqrt{2}\,; x, y \in \mathbb{Q}\}$ é um subcorpo de $\mathbb{R}$ dos números reais

(i) $0 = 0 + 0\sqrt{2}$ e $1 = 1 + 0\sqrt{2}$, logo $0{,}1 \in \mathcal{B}$

(ii) Se $x, y \in \mathcal{B}$, então $x = a + b\sqrt{2}$ e $y = c + d\sqrt{2}$ $(a, b, c, d \in \mathbb{Q})$. Logo $x - y = (a - c) + (b - d)\sqrt{2}$. Como $(a - c), (b - d) \in \mathbb{Q}$ então $x - y \in \mathcal{B}$

(iii) Se $x, y \in \mathcal{B}$ e $y \neq 0$, então $x = a + b\sqrt{2}$ e $y = c + d\sqrt{2}$ $(a, b, c, d \in \mathbb{Q}, c \neq 0\ ou\ d \neq 0)$, então

$$xy^{-1} =$$

$$= \frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{\left(a + b\sqrt{2}\right).(c - d\sqrt{2})}{\left(c + d\sqrt{2}\right).(c - d\sqrt{2})} = \frac{(ac - 2bd) + (bc - ad)\sqrt{2}}{c^2 - 2d^2} =$$

$$= \frac{(ac - 2bd)}{c^2 - 2d^2} + \frac{(bc - ad)\sqrt{2}}{c^2 - 2d^2}$$

Como $c^2 - 2d^2 \neq 0$, pois, caso contrário, $\frac{c}{d} = \sqrt{2}$, o que é impossível, já que $c, d \in \mathbb{Q}$, então $\frac{(ac-2bd)}{c^2-2d^2} + \frac{(bc-ad)\sqrt{2}}{c^2-2d^2}$ são números racionais, portanto, $xy^{-1} \in \mathcal{B}$

■

Definição 2.6. Seja $\mathcal{A}$ um anel e seja $\mathcal{I}$ um subanel de $\mathcal{A}$. Dizemos que $\mathcal{I}$ é um ideal à esquerda de $\mathcal{A}$ se, $a.x \in \mathcal{I}$, $\forall a \in \mathcal{A}$ e $\forall x \in \mathcal{I}$. E também, $\mathcal{I}$ é um ideal à direita de $\mathcal{A}$ se, $x.a \in \mathcal{I}$, $\forall a \in \mathcal{A}$ e $\forall x \in \mathcal{I}$. Simbolicamente, diz-se que $\mathcal{I}$ é um ideal de $\mathcal{A}$ se, $\mathcal{A}.\mathcal{I} \subset \mathcal{I}$ e $\mathcal{I}.\mathcal{A} \subset \mathcal{I}$.

Exemplo 2.7. Para quaisquer n elementos $x_1, x_2, \dots, x_n$ $(n \geq 1)$ de um anel comutativo $\mathcal{A}$, indica-se por $\langle x_1, x_2, \dots, x_n \rangle$ o seguinte subconjunto de $\mathcal{A}$:

$$\langle x_1, x_2, \dots, x_n \rangle = \{a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \, ; a_1, a_2, \dots, a_n \in \mathcal{A}\}$$

Mostra-se que esse subconjunto é um ideal em $\mathcal{A}$. De fato:

(a) $0 = 0x_1 + 0x_2 + \cdots + 0x_n \in \langle x_1, x_2, \dots, x_n \rangle$ e, portanto, esse conjunto não é vazio.

(b) Se $b, c \in \langle x_1, x_2, \dots, x_n \rangle$, então $b = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n$ e $c = d_1 x_1 + d_2 x_2 + \cdots + d x_n$, e que os a_i e os d_i $(1 \leq i \leq n)$ são os elementos de $\mathcal{A}$. E a partir disso, $(a_i - d_i) \in \mathcal{A}, (i = 1,2, \dots, n)$ e que $b - c = (a_i - d_i)x_1 + \cdots + (a_n - d_n)a_n$, concluímos que $b - c \in \langle x_1, x_2, \dots, x_n \rangle$.

(c) Se b é um elemento de $\langle x_1, x_2, \dots, x_n \rangle$, ou seja, $b = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n$ e se $c \in \mathcal{A}$, então:
$cb = \langle ca_1 \rangle x_1 + \cdots + \langle ca_n \rangle x_n \in \langle x_1, x_2, \dots, x_n \rangle$, pois cada um dos produtos cx_i pertence a $\mathcal{A}$. Portanto, o conjunto $\langle x_1, x_2, \dots, x_n \rangle$ é um ideal de $\mathcal{A}$, e mais, que esse conjunto é gerador de $\mathcal{A}$ por um elemento de seus elementos.

Definição 2.7. Se $\mathcal{A}$ é um anel comutativo e $S = \{x_1, x_2, \dots, x_n\} \subset \mathcal{A}$, então o ideal $\langle x_1, x_2, \dots, x_n \rangle$ é chamado ideal gerado por S. O ideal gerado por um conjunto unitário $\{x\}$ é chamado ideal principal gerado por x. Se todos os ideais de um anel comutativo são principais, então esse anel recebe o nome de anel principal.

Exemplo 2.8. Seja $\mathcal{A}$ um anel e $x_1, x_2, \dots, x_n \in \mathcal{A}$. É de direta verificação que o conjunto

$$\mathcal{A}x_1 + \mathcal{A}x_2 + \cdots + \mathcal{A}x_n = \{a_1 x_1 + \cdots + a_n x_n; a_i \in \mathcal{A}\}$$

É um ideal à esquerda de $\mathcal{A}$, o qual é chamado de ideal principal gerado por $x_1, x_2, \dots, x_n \in \mathcal{A}$.

O ideal $\mathcal{I} = \mathcal{A}.x_1$ é dito ideal principal gerado por $x_1 \in \mathcal{A}$. Analogamente define-se o ideal à direita de $\mathcal{A}$ gerado por $x_1, x_2, \dots, x_n \in \mathcal{A}$.

Exemplo 2.9. Mostra-se que o conjunto $I = \{x \in \mathbb{Z}; 9 \; divide \; 21x\}$ é um ideal em $\mathbb{Z}$ e encontrar seu gerador.

O numero $0 \in I$, pois 9 divide 0.

Se $x, y \in I$, então 9 divide $21x$ e 9 divide $21y$ e, portanto, 9 é divisor de $21x - 21y = 21(x - y)$, o que mostra que $(x - y) \in I$.

Se $x \in I$, então 9 divide $21x$ e dai segue que 9 divide $21(ax)$ pra qualquer $a \in \mathbb{Z}$, ou seja, $ax \in I$.

Sendo um ideal em $\mathbb{Z}$, então I é gerado pelo menor de seus elementos estritamente positivos. Ao verificar-se, encontra-se o numero 3, como um desses elementos. Portanto, $I = \langle 3 \rangle$.

Observação 2.2. São chamados de ideais triviais do anel $\mathcal{A}$ os subanéis de $\mathcal{A}$ $\{0_{\mathcal{A}.}\}$ e $\mathcal{A}$. Os nãos triviais são chamados de ideais próprios de $\mathcal{A}$.

Exemplo 2.10. Vamos mostrar um exemplo de ideais no anel $\mathcal{A} = [0,1]$ das funções contínuas $f: [0,1] \longrightarrow \mathbb{R}$ com as operações usuais de $+$ e $.$ de funções.

(i) Seja $x \in [0,1]$ e seja $\mathcal{I} = \{f \in \mathcal{A}; f(x) = 0\}$ é de imediato que $0 \in \mathcal{I}$, pois 0 é função constante

(ii) Sejam $f, g \in \mathcal{I}$ e $x \in [0,1]$, então $\in (f - g)(x) = f(x) - g(x) = 0 - 0 = 0$

Portanto, $f - g \in \mathcal{I}$

(iii) Sejam $f \in \mathcal{A}$ e $g \in \mathcal{I}$, então $(f.g)(x) = f(x).g(x) = f(x).0 = 0$. Logo, $f.g \in \mathcal{I}$ e, assim $\mathcal{I}$ é um ideal à esquerda de $\mathcal{A}$. De modo semelhante faz-se para ideal à direita de $\mathcal{A}$. Portanto, $\mathcal{I}$ é um ideal de $\mathcal{A}$.

Vamos agora definir as relações das classes de equivalências determinada por um ideal de um anel. Seja $\mathcal{A}$ um anel qualquer e $\mathcal{I}$ um ideal de $\mathcal{A}$. Assim, o ideal $\mathcal{I}$ define-se o anel $\mathcal{A}$ a relação:

$$y \equiv x (mod\ \mathcal{I}) \Leftrightarrow y - x \in \mathcal{I}$$

Vamos provar que $\equiv (mod\ \mathcal{I})$ defini uma relação de equivalência. Sejam $x, y, z \in \mathcal{A}$, temos:

(i) $x \equiv x (mod\ \mathcal{I})$ pois $0 = x - x \in \mathcal{I}$

(ii) $x \equiv y (mod\ \mathcal{I}) \Longrightarrow y \equiv x (mod\ \mathcal{I})$ pois se $x - y \in \mathcal{I}$, então $x - y = -(x - y) \in \mathcal{I}$

$(iii)\ x \equiv y(mod\ \mathcal{I})$ e $x \equiv y(mod\ \mathcal{I}) \Longrightarrow x \equiv z(mod\ \mathcal{I})$, pois $x - y \in \mathcal{I}$ e $y - z \in \mathcal{I} \Longrightarrow x - z = (x - y) + (y - z) \in \mathcal{I}$

Logo está bem definida.

Denota-se por $\bar{x}$ a classe de equivalência de $x \in \mathcal{A}$ pela relação $\equiv (mod\ \mathcal{I})$. Então

$$\bar{x} = \{y \in \mathcal{A};\ y \equiv x(mod\ \mathcal{I})\}$$

Pode-se detonar, também, a classe $\bar{x}$ por $\bar{x} = \{x + z; z \in \mathcal{I}\}$. E com isso, chama-se de conjunto quociente de $\mathcal{A}$ pelo ideal $\mathcal{I}$, ao conjunto $\mathcal{A}/\mathcal{I} = \{\bar{x} = x + z;\ x \in \mathcal{A}\}$. E será definido as seguintes operações em $\mathcal{A}/\mathcal{I}$

$$+: \mathcal{A}/\mathcal{I} \times \mathcal{A}/\mathcal{I} \longrightarrow \mathcal{A}/\mathcal{I} \qquad \text{e} \qquad .: \mathcal{A}/\mathcal{I} \times \mathcal{A}/\mathcal{I} \longrightarrow \mathcal{A}/\mathcal{I}$$
$$(\bar{x}, \bar{y}) \longmapsto \overline{x + y} \qquad\qquad (\bar{x}, \bar{y}) \longmapsto \overline{x.y}$$

Já foi mostrado que se $\mathcal{I}$ é um ideal de um anel comutativo $\mathcal{A}$, também ele é um subanel de $\mathcal{A}$, e, portanto, um subgrupo do grupo aditivo de $\mathcal{A}$. E como esse grupo é comutativo, então $\mathcal{I}$ é um subgrupo normal de $(\mathcal{A}, +)$. Logo, tem sentido em considerar-se o grupo quociente $\mathcal{A}/\mathcal{I}$, e que este grupo pode se converter em um anel, de maneira muito natural. Veja a proposição a seguir.

Proposição 2.3. Seja $\mathcal{I}$ um ideal do anel $\mathcal{A}$. Considere $(\mathcal{I}, +)$ como subgrupo normal de $(\mathcal{A}, +)$, então o grupo quociente $\mathcal{A}/\mathcal{I}$ é um anel com a seguinte operação do produto.

$$.: \mathcal{A}/\mathcal{I} \times \mathcal{A}/\mathcal{I} \longrightarrow \mathcal{A}/\mathcal{I}$$
$$(x + \mathcal{I}, y + \mathcal{I}) \longmapsto (x + \mathcal{I}).(y + \mathcal{I})$$

Demonstração:

Verifica-se que a operação está bem definida. Sejam $x + \mathcal{I}, y + \mathcal{I}, z + \mathcal{I} \in \mathcal{A}/\mathcal{I}$, tais que $x + \mathcal{I} = y + \mathcal{I}$ e $z + \mathcal{I} = w + \mathcal{I}$. Mostra-se que $xz + \mathcal{I} = yw + \mathcal{I}$

Como $x + \mathcal{I} = y + \mathcal{I}$, então $x - y \in \mathcal{I}$. De maneira análoga temos $z - w \in \mathcal{I}$. Por definição temos que $\mathcal{I}$ é um ideal de $\mathcal{A}$, logo $(x - y)z \in \mathcal{I}$ e $y(z - w) \in \mathcal{I}$. Assim,

$$\big((x - y)z + y(z - w)\big) = xz - yz + yz - yw = xz - yz \in \mathcal{A}$$

Ou seja, $xz + \mathcal{I} = yw + \mathcal{I}$. Portanto, a operação está bem definida.

(Associatividade): sejam $x + \mathcal{I}, y + \mathcal{I}, z + \mathcal{I} \in \mathcal{A}/\mathcal{I}$ quaisquer então,

$$(x+\mathcal{I}).\big((y+\mathcal{I}).(z+\mathcal{I})\big) = (x+\mathcal{I}).(yz+\mathcal{I}) = x(yz)+\mathcal{I}$$

E, também

$$x(yz)+\mathcal{I} = (xy)z+\mathcal{I} = (xz+\mathcal{I}).(z+\mathcal{I}) = ((x+\mathcal{I}).(y+\mathcal{I})).(z+\mathcal{I})$$

Portanto, $(x+\mathcal{I}).\big((y+\mathcal{I}).(z+\mathcal{I})\big) = ((x+\mathcal{I}).(y+\mathcal{I})).(z+\mathcal{I})$

Distributividade: sejam $x+\mathcal{I}, y+\mathcal{I}, z+\mathcal{I} \in \mathcal{A}/\mathcal{I}$ quaisquer então,

$$\big((x+\mathcal{I})+(y+\mathcal{I})\big).(z+\mathcal{I}) = \big((x+y)+\mathcal{I}\big).(y+\mathcal{I}) = (x+y)z+\mathcal{I} = (xz+yz)+\mathcal{I}$$
$$= (xz+\mathcal{I})+(yz+\mathcal{I}) = (x+\mathcal{I}).(z+\mathcal{I})+(y+\mathcal{I}).(z+\mathcal{I})$$

Por outro lado,

$$(x+\mathcal{I}).\big((y+\mathcal{I})+(z+\mathcal{I})\big) = (x+\mathcal{I}).\big((y+z)+\mathcal{I}\big) = (x(y+z)+\mathcal{I}) = (xy+xz)+\mathcal{I}$$
$$= (xy+\mathcal{I})+(xz+\mathcal{I}) = (x+\mathcal{I}).(y+\mathcal{I})+(x+\mathcal{I}).(z+\mathcal{I})$$

Portanto, $(\mathcal{A}/\mathcal{I}, +, .)$ é um anel

■

Definição 2.8. Seja $\mathcal{A}$ um anel e $\mathcal{M}$ e $\mathcal{I}$ ideais de $\mathcal{A}$. Diz-se que $\mathcal{M}$ é um ideal maximal de $\mathcal{A}$ se $\mathcal{M} \neq \mathcal{A}$, tal que $\mathcal{M} \subset \mathcal{I} \subset \mathcal{A}$, então $\mathcal{I} = \mathcal{M}$ ou $\mathcal{I} = \mathcal{A}$

Exemplo 2.11. No anel $\mathcal{A} = \mathbb{Z} \times \mathbb{Z}$ é maximal o ideal $\mathcal{M} = \mathbb{Z} \times 2\mathbb{Z}$. De fato, seja $\mathcal{I}$ um ideal em $\mathcal{A}$ tal que $\mathcal{M} \subset \mathcal{I}$. Então existe $(x, y) \in \mathcal{I}$ de modo que $(x, y) \notin \mathcal{M}$, ou seja, temos $y = 2q+1$, um número ímpar. Como $(x-1, 2q) \in \mathcal{I}$ pois trata-se de um elemento de $\mathcal{M}$, então

$$(x, 2q+1) - (x-1, 2q) = (1,1) \in \mathcal{I}$$

Portanto, a unidade de $\mathcal{A}$ ao ideal $\mathcal{I}$ vale a igualdade $\mathcal{A} = \mathcal{I}$. Assim, o único ideal em $\mathcal{A}$, estritamente maior que $\mathcal{M}$, é $\mathcal{A}$.

Exemplo 2.12. Vamos mostrar que $2\mathbb{Z}$ é um ideal maximal em $\mathbb{Z}$. De fato, se $\mathcal{I}$ é um ideal em $\mathbb{Z}$ que contem $2\mathbb{Z}$, então $\mathcal{I}$ possui um numero impar $2k+1$. Mas, como $2k \in \mathcal{I}$, pois $2k$ pertence a $2\mathbb{Z}$ e $\mathcal{I} \supset 2\mathbb{Z}$, então $(2k+1)-(2k)=1 \in \mathcal{I}$. Ou seja, $\mathcal{I}=\mathbb{Z}$. Pela definição de ideal máxima, está provada.

Proposição 2.4. Todo ideal maximal em um anel comutativo com unidade é necessariamente um ideal primo.

Demonstração: Seja $\mathcal{M}$ um ideal maximal de um anel comutativo $\mathcal{A}$. Da definição de ideal maximal ocorre $\mathcal{M} \neq \mathcal{A}$. Basta provar que, se x, y são elementos de $\mathcal{A}$, tais que $xy \in \mathcal{M}$, então $x \in \mathcal{M}$ ou $y \in \mathcal{M}$. Suponha-se que $x \notin \mathcal{M}$ e considerar o ideal $\mathcal{I} = \langle x \rangle + \mathcal{M}$ e com isso $\mathcal{M} \subset \mathcal{I}$

Como, porém $x \in \mathcal{I}$, pois $x = 1.x + 0$ e $0 \in \mathcal{M}$, pela suposição de $x \notin \mathcal{M}$, então $\mathcal{I}$ contém $\mathcal{M}$ e, portanto, $\mathcal{I} = \mathcal{A}$. Isso significa que a unidade de $\mathcal{A}$ pode ser escrita assim:

$$1 = rx + m$$

Em que r e m são elementos de $\mathcal{A}$ e $\mathcal{M}$, respectivamente. Multiplicando ambos os lados dessa igualdade por y, temos:

$$y = r(yx) + ym$$

Isso mostra que $y \in \mathcal{M}$, já que $xy, m \in \mathcal{M}$

■

Teorema 2.1. Seja $\mathcal{A}$ um anel comutativo e com unidade $1 \in \mathcal{A}$. Então as seguintes condições são equivalentes:

(i) $\mathcal{A}$ é um corpo

(ii) $\{0\}$ é um ideal maximal em $\mathcal{A}$

(iii) Os únicos ideais de $\mathcal{A}$ são os triviais

Demonstração: $(i) \Longrightarrow (ii)$ Seja $\mathcal{A}$ um corpo, por hipótese, e seja $\mathcal{I}$ um ideal de $\mathcal{A}$ tal que $\{0\} \subset \mathcal{I} \subset \mathcal{A}$. Suponha-se $\mathcal{I} \neq \{0\}$. Assim existe $0 \neq x \in \mathcal{I}$. Como $\mathcal{A}$ é um corpo existe $y \in \mathcal{A}$ tal que $y.x = 1$ e, portanto $1 \in \mathcal{I}$ e daí, segue imediatamente que $\mathcal{I} = \mathcal{A}$. $(ii) \Longrightarrow (iii)$ Segue imediatamente das definições. $(iii) \Longrightarrow (i)$ Seja $0 \neq x \in \mathcal{A}$ e $\mathcal{I} = \mathcal{A}.x$ o ideal principal de $\mathcal{A}$ gerado por x. Como $1 \in \mathcal{A}$, temos $\in x = 1.x \in \mathcal{I}$, ou seja, $\mathcal{I} \neq \{0\}$ e assim pela nossa hipótese, teremos $\mathcal{I} = \mathcal{A}$, logo

$$1 \in \mathcal{A} = \mathcal{A}.x$$

Donde existe $y \in \mathcal{A}$ tal que $1 = y.x$

Definição 2.9. Seja $\mathcal{A}$ um anel. Suponha-se que para algum inteiro $n > 0$ e para qualquer $x \in \mathcal{A}$ verifica-se a igualdade $n.x = 0$. Então existe um menor inteiro estritamente positivo r tal que $r.x = 0$. Esse inteiro r é chamado de característica do anel $\mathcal{A}$ indicado por $c(\mathcal{A})$.

Exemplo 2.13. Os anéis $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ tem característica 0, pois, se $m \neq 0$ então $m.1 = m$ e, portanto, $1.m \neq 0$

Teorema 2.2. Sejam $\mathcal{A}$ um anel comutativo com unidade 1 e $\mathcal{I}$ um ideal de $\mathcal{A}$. Então $\mathcal{I}$ é um ideal maximal de $\mathcal{A}$ se, e somente se, $\mathcal{A}/\mathcal{I}$ é um corpo.

Demonstração:

$\Longrightarrow$ Pela definição temos que $\mathcal{I}$ é um ideal de $\mathcal{A}$, e seja $\bar{0} \neq \bar{x} \in \bar{\mathcal{A}} = \mathcal{A}/\mathcal{I}$. Temos que provar que $\exists\, \bar{y} \in \bar{\mathcal{A}}$ tal que $\bar{x}.\bar{y} = 1$. De fato, se $\mathcal{L} = \mathcal{A}.x$ ideal gerado por x, temos que : $\mathcal{I} + \mathcal{L} = \{a + b; a \in \mathcal{I}, b \in \mathcal{L}\}$ é um ideal contento $\mathcal{I}$, e mais $\bar{x} \neq \bar{0}$ se, e somente se, $x \notin \mathcal{I}$. Como $x = 1.x \in \mathcal{L} \subset \mathcal{I} + \mathcal{L}$ temos que $\mathcal{I} + \mathcal{L}$ é um ideal que contém $\mathcal{I}$ e mais $\mathcal{I} + \mathcal{L} \neq \mathcal{I}$. Pela maximalidade de $\mathcal{I}$ segue que $\mathcal{A} = \mathcal{I} + \mathcal{L}$ e daí vem, $1 \in \mathcal{I} + \mathcal{L}$ implica que existe $u \in \mathcal{I}, v \in \mathcal{L}$ tais que $1 = u + v$.

Assim, existe $u \in \mathcal{I}, v \in \mathcal{L} = \mathcal{A}.x$ e temos que $v = y.x$ para algum $y \in \mathcal{A}$, ou seja, existe $y \in \mathcal{A}$ e $u \in \mathcal{I}$ tais que $1 = u + y.x$. Passando barra em ambos os membros, segue que, $\bar{1} = \overline{u + y.x} = \bar{u} + \overline{y.x} = \bar{0} + \bar{y}.\bar{x}$, isto é, $\bar{y}.\bar{x} = \bar{x}.\bar{y} = 1$, como queríamos demonstrar.

■

$\Leftarrow$ Fazendo a volta, suponha-se que $\bar{\mathcal{A}} = \mathcal{A}/\mathcal{I}$ seja um corpo. Assim $\bar{0}, \bar{1} \in \bar{\mathcal{A}}$ implica que $\mathcal{I} \neq \mathcal{A}$. Se $\mathcal{M} \neq \mathcal{I}$ é um ideal de $\mathcal{A}$ e $\mathcal{I} \subset \mathcal{M} \subset \mathcal{A}$, então teremos que existe $x \in \mathcal{M}$, $x \neq \mathcal{I}$, ou seja, $\bar{x} \neq \bar{0}$, com $\bar{x} \in \bar{\mathcal{A}}$. Como $\mathcal{A}$ é um corpo existe $\bar{y} \in \bar{\mathcal{A}}$ tal que $\bar{x}.\bar{y} = \bar{1}$, ou ainda,

$$x.y \equiv 1(mod\ \mathcal{I}) \Leftrightarrow x.y - 1 \in \mathcal{I} \Leftrightarrow \exists\, u \in \mathcal{I}$$

Tal que $xy - 1 = u$, e isto nos diz que, $1 = xy - u$. Como $x \in \mathcal{M}$ segue que $xy \in \mathcal{M}$ e como $u \in \mathcal{I} \subset \mathcal{M}$ temos também $u \in \mathcal{M}$. Logo conclui-se que $1 = xy - u \in \mathcal{M}$ e imediatamente $\mathcal{M} = \mathcal{A}$.

■

Sejam $\mathcal{A}, \mathcal{B}$ anéis quaisquer. Dentre as operações de $\mathcal{A}$ em $\mathcal{B}$, tem a importância destacada aquelas que preservam as leis de composições internas que fazem $\mathcal{A}$ e $\mathcal{B}$ anéis.

Definição 2.10. Sejam $\mathcal{A}$ e $\mathcal{B}$ dois anéis. Uma aplicação $f: \mathcal{A} \longrightarrow \mathcal{B}$ é chamado de homomorfismo de anéis de $\mathcal{A}$ em $\mathcal{B}$ se as seguintes condições são verificadas:

$i)$ Para todo $x, y \in \mathcal{A} \Longrightarrow f(x + y) = f(x) + f(y)$

(ii) Para todo $x, y \in \mathcal{A} \Longrightarrow f(x.y) = f(x).f(y)$

Exemplo 2.14. Sejam $\mathcal{A} = \mathbb{Z}$ e $\mathcal{B} = \mathbb{Z} \times \mathbb{Z}$. A aplicação $f: \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ dada por $f(x) = f(x, 0), \forall x \in \mathbb{Z}$ é um homomorfismo de anéis porque,

$$f(x + y) = (x + y, 0) = (x, 0) + (y, 0) = f(x) + f(y)$$

$$f(x.y) = (xy, 0) = (x, 0).(y, 0) = f(x).f(y)$$

Teorema 2.3. Sejam $\mathcal{A}$ e $\mathcal{B}$ anéis e $f: \mathcal{A} \longrightarrow \mathcal{B}$ um homomorfismo de anéis, então:

(i) $Imf = \{f(x); x \in \mathcal{A}\}$ é um subanel de $\mathcal{B}$;

(ii) $N(f) = \ker(f) = \{\, x \in \mathcal{A}; f(x) = 0_{\mathcal{B}}\}$ é um ideal de $\mathcal{A}$ e f é injetiva $\Leftrightarrow N(f) = \{0\}$;

(iii) Os anéis $\mathcal{A}/N(f)$ e Imf são isomorfos.

Demonstração: $(i) \Longrightarrow$ vamos mostrar que Imf é subanel de $\mathcal{B}$

$$0_{\mathcal{B}} = f(0) \in Imf$$

$$f(x), f(y) \in Imf \Longrightarrow f(x) - f(y) = f(x - y) \in Imf$$

$$f(x), f(y) \in Imf \Longrightarrow f(x).f(y) = f(x.y) \in Imf$$

Com isso Imf é um subanel de $\mathcal{B}$.

$(ii) \Longrightarrow$ Vamos provar que $N(f) = \{x \in \mathcal{A}: f(x) = 0_{\mathcal{B}}\}$ é um ideal de $\mathcal{A}$

a) $0 \in N(f)$ pois $f(0) = 0_{\mathcal{B}}$

b) $x, y \in N(f) \Longrightarrow f(x - y) = f(x) - f(y) = 0_{\mathcal{B}} - 0_{\mathcal{B}} = 0_{\mathcal{B}}$

Ou seja, $x - y \in N(f)$

Seja $x \in \mathcal{A}$ e $n \in N(f)$ então

$$f(x.n) = f(x).f(n) = f(x).0_{\mathcal{B}} = 0_{\mathcal{B}}$$

$$f(n.x) = f(n).f(x) = 0_{\mathcal{B}}.f(x) = 0_{\mathcal{B}}$$

Ou seja, $x.n$ e $n.x \in N(f)$, com isso $N(f)$ é um ideal de $\mathcal{A}$

Agora, se f é injetiva, segue imediatamente que $N(f) = \{0\}$ pois, $f(0) = 0_{\mathcal{B}}$

Se $f(x) = f(y)$, $x, y \in \mathcal{A}$ e $N(f) = \{0\}$ segue $f(x) - f(y) = 0_{\mathcal{B}} \Longrightarrow f(x - y) = 0_{\mathcal{B}}$ então $x - y \in N(f) = \{0\} \Longrightarrow x = y$ e isto prova o item (ii)

(iii) Para demonstramos este item, primeiro define-se a função bijetora:

$$\psi: \mathcal{A}/N(f) \longrightarrow Imf$$
$$\bar{x} \longmapsto f(a)$$

Dados $x, y \in \mathcal{A}$ são tais que $\bar{x} = \bar{y}$, então $f(x) = f(y)$. E de fato, se $\bar{x} = \bar{y}$, então $\bar{x} - \bar{y} = 0 \in N(f)$, logo $f(\bar{x} - \bar{y}) = 0$ e, além disso, $f(\bar{x} - \bar{y}) = f(\bar{x}) - f(\bar{y})$, pois f é um homomorfismo. Portanto, $f(x) = f(y)$.

Agora ψ é uma aplicação sobrejetiva e é um homomorfismo, pois para $x, y \in \mathcal{A}$ temos

(a) $\psi(\bar{x} + \bar{y}) = \psi(\overline{x + y}) = \psi(x + y)$ pela definição de ψ por f se um homomorfismo vem que $f(x + y) = f(x) + f(y) = \psi(\bar{x}) + \psi(\bar{y})$

(b) $\psi(\bar{x}.\bar{y}) = \psi(\overline{x.y}) = f(x.y)$ e $f(x.y) = f(x).f(y) = \psi(\bar{x}).\psi(\bar{y})$

Por fim, temos $N(f) = \{\bar{x} \in \mathcal{A}/N(f)\,; f(x) = 0\} = \{\bar{x} \in \mathcal{A}/N(f)\,; x \in N(f)\} = \bar{0}$

Logo ψ é injetiva

■

Definição 2.11. Sejam $\mathcal{A}$ e $\mathcal{B}$ anéis quaisquer. Uma aplicação $f: \mathcal{A} \longrightarrow \mathcal{B}$ chamamos de isomorfismo de $\mathcal{A}$ em $\mathcal{B}$ se:

(i) f é bijetora

(ii) f é um homomorfismo de anéis, isto é,

Para todo $x, y \in \mathcal{A}$ tem-se $f(x+y) = f(x) + f(y)$ e $f(x.y) = f(x).f(y)$

Observação 2.3.

Naturalmente todos os resultados válidos para homomorfismo de anéis também são válidos para isomorfismo. A demonstração de isomorfismo de anéis é análoga a que se fez para grupos.

Exemplo 2.15. Seja $\mathcal{A} = \mathbb{Z}[\sqrt{2}] = \{m + n\sqrt{2}; m, n \in \mathbb{Z}\}$ e consideramos $f: \mathcal{A} \longrightarrow \mathcal{A}$ definida por $f(m + n\sqrt{2}) = m - n\sqrt{2}$. f é um homomorfismo pois

$$f\left((m + n\sqrt{2}) + (r + s\sqrt{2})\right) = f(m + n\sqrt{2}) + f(r + s\sqrt{2}) = (m - n\sqrt{2}) + (r - s\sqrt{2})$$
$$= (m + r) - (n + s)\sqrt{2}$$

E, também

$$f\left((m + n\sqrt{2}).(r + s\sqrt{2})\right) = f\left((m + n\sqrt{2}).f(r + s\sqrt{2})\right) = \left((m - n\sqrt{2}).(r - s\sqrt{2})\right)$$
$$= (mr + 2sn) - (ms + nr)\sqrt{2}$$

É injetor pois,

Seja $f(m + n\sqrt{2})$ e $f(r + s\sqrt{2}) \in \mathcal{A}$, tal que $f(m + n\sqrt{2}) = f(r + s\sqrt{2})$, então $f(m + n\sqrt{2}) - f(r + s\sqrt{2}) = 0 \Longrightarrow (m + n\sqrt{2}) - (r + s\sqrt{2}) = 0 \Longrightarrow (m + n\sqrt{2}) = (r + s\sqrt{2})$

E sobrejetor,

Dado $y = m + n\sqrt{2} \in \mathcal{A}$ basta tomar $x = m - n\sqrt{2} \in \mathcal{A}$ então

$$f(x) = f(m - n\sqrt{2}) = m + n\sqrt{2} = y$$

2.1. Corpo de frações de anel de integridade

Todo corpo, como já vimos, é um anel de integridade. Logo se pode dizer que todo corpo contém um subanel que é anel de integridade: ele próprio. Agora vamos construir um corpo K do qual $\mathcal{A}$ seja um subanel unitário. A construção é a mesma, no plano formal, pela qual se obtém o corpo dos números racionais a partir do anel de inteiros.

Seja $\mathcal{A}$ um anel de integridade. No conjunto $\mathcal{A} \times \mathcal{A}^*$ consideramos a relação $\sim$ definida da seguinte maneira:

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

Não é difícil provar que $\sim$ é uma relação de equivalência sobre $\mathcal{A} \times \mathcal{A}^*$. Por brevidade mostraremos apenas que $\sim$ goza da propriedade transitiva

De fato, consideremos $(a, b), (c, d), (e, f) \in \mathcal{A} \times \mathcal{A}^*$. Se $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$, então $ad = bc$ e $cf = de$. Multiplicando os dois membros da primeira igualdade por f e os da segunda por b, obtemos $adf = bcf$ e $bcf = deb$. Segue daí que $adf = deb$ e, portanto, cancelando-se d, o que é possível, pois $d \neq 0$ e $\mathcal{A}$ é um anel de integridade, $af = be$ onde $(a, b) \sim (e, f)$

Usa-se a notação $\frac{a}{b}$ em vez de $\overline{(a, b)}$ para apresentar a classe de equivalência determinada pelo par (a, b). Os elementos do conjunto quociente $K = \mathcal{A} \times \mathcal{A}^* / \sim$, com a notação adotada, são as frações $\mathbb{Q} = \{\frac{a}{b} ; a \in \mathcal{A}, b \in \mathcal{A}^*\}$.

Evidentemente,

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = cb$$

Agora define-se as operações da soma e produto no conjunto quociente

$$\mathcal{A}/\sim = \left\{\frac{a}{b}; a \in \mathcal{A}, b \in \mathcal{A}^*\right\} = K$$

Quaisquer que sejam $(a, b), (c, d) \in \mathcal{A} \times \mathcal{A}^*$, definiremos

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd} \quad \text{e} \quad \frac{a}{b}.\frac{c}{d}=\frac{ac}{bd}$$

Pode-se provar que essas definições independem das particulares representações das classes de equivalência. Observe que se $b,d \in \mathcal{A}^*$ então $b.d \in \mathcal{A}^*$, pois $\mathcal{A}^*$ é um domínio de integridade. Suponhamos que $(a,b) \sim (m,n)$ e $(c,d) \sim (r,s)$. Então $an = bm$ e $cs = dr$. Multiplicando membro a membro essas igualdades, temos $(an)(cs) = (bm)(dr)$ e daí $(ac)(ns) = (bd)(mr)$. Isso significa, no presente contexto, que $(ac,bd) \sim (ns,mr)$ e, portanto, que $\frac{a}{b}.\frac{c}{d} = \frac{m}{n}.\frac{r}{s}$

Rotineiramente se demonstra que $(K,+,.)$ é um corpo. Vamos denotar por $a^* = \frac{a}{1}$, onde $a \in \mathcal{A}$ e 1 é a unidade de $\mathcal{A}$. E denotaremos:

$$\mathcal{A}^* = \left\{a^* = \frac{a}{1}, a, 1 \in \mathcal{A}\right\} = K$$

Considere a seguinte função:

$$\varphi: \mathcal{A} \longrightarrow \mathcal{A}^*$$
$$a \longmapsto a^*$$

É de imediata verificação que:

$(i)\ Im\varphi = \mathcal{A}^*$

$(ii)\ Ker(\varphi) = \{a \in \mathcal{A}: a^* = 0^*\} = \{0\}$

$(iii)\ \varphi(a+b) = (a+b)^* = a^* + b^* = \varphi(a) + \varphi(b)\ \forall\ a,b \in \mathcal{A}$

$(iv)\ \varphi(a.b) = (a.b)^* = a^*.b^* = \varphi(a).\varphi(b)\ \forall\ a,b \in \mathcal{A}$

Desse modo, $\mathcal{A} \simeq \mathcal{A}^* \subset K$, ou seja, $\mathcal{A}$ é isomorfo sobre $\mathcal{A}^*$. Observe que se $\frac{a}{b} \neq 0$ em K, isto é,$a \neq 0$ em $\mathcal{A}$, então $\frac{b}{a} \in K$ e mais, $\frac{a}{b}.\frac{b}{a} = 1^*$. Como $\mathcal{A}$ é isomorfo a $\mathcal{A}^* \subset K$ dize-se que $\mathcal{A}$ está imerso em K. Observa-se também que $b^*.\frac{1}{b} = 1^*$ se $b \neq 0, b \in \mathcal{A}$. Assim denota-se por $(b^*)^{-1} = \frac{1}{b}$ se $b \neq 0, b \in \mathcal{A}$. Logo

$$\mathcal{A}^* = \{a^*; a \in \mathcal{A}\} \subset K = \{a^*.(b^*)^{-1}: a^*, b^* \in \mathcal{A}^*, b^* \neq 0\}$$

Portanto, o corpo K construído nesse paragrafo recebe o nome de **corpo de frações do domínio** $\mathcal{A}$

Exemplo 2.16. $\mathbb{Q}[\sqrt{2}] = \{\frac{m}{n} + \frac{p}{q}\sqrt{2}, m, n, p, q \in \mathbb{Z}\}$ é o corpo de frações de $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}, a, b \in \mathbb{Z}\}$.

2.2. Polinômios sobre um anel.

Polinômios são definidos como uma sequência de números complexos em que esse faz parte de uma classe de funções simples e infinita. Ao longo deste capitulo representa-se por $\mathcal{A}$ como um anel de integridade infinito e, também, este anel pode ser um corpo infinito, caso em que será indicado por K.

Definição 2.12. Uma função $f: \mathcal{A} \longrightarrow \mathcal{A}$ denomina-se função polinomial de uma indeterminada x sobre $\mathcal{A}$ se existem elementos $a_0, a_1, a_2, \ldots, a_r$ em $\mathcal{A}$ tais que para todo $x \in \mathcal{A}$ tem-se:

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_rx^r \ldots$$

$$a_i \in \mathcal{A}, \forall\, i \in \mathbb{N}$$

Diz-se que dois polinômios são iguais quando assumem valores iguais para todo $x \in \mathcal{A}$, simbolicamente, sejam os polinômios:

$$P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_rx^r \ldots$$

$$Q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_sx^s \ldots$$

São iguais se, e somente se $a_i = b_i$ em $\mathcal{A}$, $\forall\, i \in \mathbb{N}$

Se $P(x) = 0 + 0x + 0x^2 + \cdots + 0x^r \ldots$ indica-se $P(x)$ por 0 e o chama-se de polinômio identicamente nulo sobre $\mathcal{A}$, ou seja, $P(x)$ sobre $\mathcal{A}$ é identicamente nulo se, e somente se $a_i = 0 \in \mathcal{A}$, $\forall\, i \in \mathbb{N}$.

Chama-se de polinômio constante a sobre $\mathcal{A}$, se $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, onde $a_0 = a$ e $a_i = 0$, $\forall\, i \geq 1$

Exemplo 2.17. São exemplos de polinômios constantes no corpo dos reais

$$P(x) = 7, f(x) = \sqrt{5}, g(x) = \frac{13}{11}$$

Representa-se por $\mathcal{A}[x]$ o conjunto de todos os polinômios sobre $\mathcal{A}$, em uma indeterminada x.

Proposição 2.5. A soma de dois polinômios sobre $\mathcal{A}$ é também um polinômio sobre $\mathcal{A}$, isto é, $\mathcal{A}[x]$ é fechado em relação a operação adição.

Demonstração: Sejam P e Q dois polinômios sobre $\mathcal{A}$, tais que:

$$P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_rx^r + \cdots$$

$$Q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_sx^s + \cdots$$

Temos que,

$(P + q)(x) = P(x) + Q(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots$

Pode-se simplificar essa soma como

$P(x) + Q(x) = c_1x + \cdots + c_kx^k + \cdots$

Onde, $c_i = (a_i + b_i) \in \mathcal{A}$. Portanto $P + Q \in \mathcal{A}$

Proposição 2.6. O produto de dois polinômios sobre $\mathcal{A}$ é também um polinômio sobre $\mathcal{A}$, isto é, $\mathcal{A}[x]$ é fechado em relação a operação multiplicação.

Demonstração: sejam P e Q polinômios sobre $\mathcal{A}$, tais que:

$$P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m + \cdots$$

$$Q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n + \cdots$$

Então vem que,

$$P(x).Q(x) = c_0 + \cdots + c_kx^k$$

Onde, $c_0 = a_0b_0$, $c_1 = a_0b_1 + a_1b_0$, $c_2 = a_0b_2 + a_1b_1 + a_2b_0$, ... $c_k = a_0b_k + \cdots + a_kb_o$, com $k \in \mathbb{N}$. Portanto, $P.Q \in \mathcal{A}$

Observe que a definição acima da **proposição 2.6** de produto de polinômios provém da regra $x^mx^n = x^{m+n}$, já demonstrado na **proposição 1.7**, e da propriedade distributiva.

Nota-se que $\mathcal{A}[x]$ é um domínio de integridade onde o polinômio nulo 0 é o elemento neutro de $\mathcal{A}[x]$ e o polinômio constante 1 é a unidade de $\mathcal{A}[x]$.

Definição 2.13. Seja $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m + \cdots$ um polinômio não nulo. Chama-se grau de P e representa-se por ∂P ou grP, o número natural n tal que $a_m \neq 0$ e $a_i = 0$ para todo $i > n$. Nessas condições a_m é chamado de coeficiente dominante.

Em outras palavras, o grau de um polinômio é simplesmente o índice de seu coeficiente dominante.

Exemplo 2.18. $P(x) = 4x^3 + 7x^2 + 2$ em $\mathbb{Z}[x]$ tem grau 3, $\partial P(x) = 3$

2.3. Divisibilidade em $\mathcal{A}[x]$ exata

Dados $f(x), g(x) \in \mathcal{A}[x]$, diz-se que um polinômio $g(x)$ divide $f(x)$ se existe um polinômio $Q(x) \in \mathcal{A}[x]$ tal que $f(x) = g(x).Q(x)$. Indica-se pela notação $g \mid f$ para divisão de g sobre f. E $g \nmid f$ para representar g não divide f.

Exemplo 2.19. Em $\mathbb{R}[x]$ o polinômio $x - 1$ dividi o polinômio $x^2 - 1$, pois

$$x^2 - 1 = (x - 1).(x + 1)$$

Teorema 2.4. (Algoritmo da divisão)

Dados os polinômios $f(x), g(x) \in \mathcal{A}[x]$, com $g(x) \neq 0$ e o coeficiente $g(x)$ inversível, então existem polinômios $Q(x), r(x)$ tais que:

$$f(x) = g(x).Q(x) + r(x)$$

Em que $r(x) = 0$ ou $\partial r(x) < \partial g(x)$

Demonstração*:* (Existência)

Para demonstração supõem-se $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$, com $m \geq 0$ e $b_m \neq 0$. Vamos analisar os seguintes casos.

(i) $f(x) = 0$ (Polinômio identicamente nulo). Neste caso $q(x) = r(x) = 0$, pois $0 = g(x).0 + 0$

(ii) $f(x) \neq 0$ e $\partial f(x) < \partial g(x)$. Quando isso acontece, basta tomar $q(x) = 0$ e $r(x) = f(x)$, uma vez que $f(x) = g(x).0 + f(x)$ e, por hipótese, $\partial f(x) < \partial g(x)$

(iii) $f(x) \neq 0$ e $\partial f(x) \geq \partial g(x)$. Neste caso, procede por indução (segundo princípio)

Agora seja $f_1(x)$ o polinômio definido por

$$f_1(x) = f(x) - a_n b^{-1}{}_m x^{n-m}.g(x)$$

Se $f_1(x) = 0$ ou $\partial f_1(x) < \partial g(x)$, então $Q(x) = a_n b^{-1}{}_m x^{n-m}$ e $r(x) = f_1(x)$. Caso contrário tem-se $\partial f_1(x) \geq \partial g(x)$ e $\partial f_1(x) < n$, pois o coeficiente dominante $f(x)$ é igual ao polinômio expresso por:

$$f(x) = a_n b^{-1}{}_m x^{n-m}.g(x)$$

Portanto, devido a hipótese de indução, existem polinômios $Q_1(x)$ e $r_1(x)$ tais que

$$f_1 = g(x).Q_1(x) + r_1(x)$$

Onde $r_1(x) = 0$ ou $\partial r_1(x) < \partial g(x)$

Daí segue que

$$f(x) = a_n b^{-1}{}_m x^{n-m}.g(x) = g(x)Q_1(x) + r_1(x)$$

E, portanto

$$f(x) = a_n b^{-1}{}_m x^{n-m}.g(x) + g(x).Q_1 + r_1(x)$$

Ou

$$f(x) = [a_n b^{-1}{}_m x^{n-m} + q_1]g(x) + r_1(x)$$

E, com isso, tomando $q(x) = a_n b^{-1}{}_m x^{n-m} + Q_1$ e $r_1(x) = r(x)$ prova-se a existência dos polinômios $q(x)$ e $r(x)$ tais que $f(x) = Q(x).g(x) + r(x)$ e $r(x) = 0$ ou $\partial r(x) < \partial g(x)$.

Agora prova-se a unicidade. Sejam $Q_1(x), Q_2(x), r_1(x), r_2(x)$ tais que

$$f(x) = Q_1(x).g(x) + r_1(x) = Q_2(x).g(x) + r_2(x)$$

Onde $r_1(x) = 0$ ou $\partial r_i(x) < \partial g(x), i = 1,2$

Daí segue,

$$\big(Q_1(x) - Q_2(x)\big).g(x) = r_2(x) - r_1(x)$$

Mas se $Q_1(x) \neq Q_2(x)$ o grau do polinômio do lado de igualdade acima é maior ou igual ao $\partial g(x)$ enquanto que $\partial(r_2(x) - r_1(x)) < \partial g(x)$ o que é uma contradição. Logo $Q_1(x) = Q_2(x)$ e, portanto

$$r_1(x) = f(x) - Q_1(x).g(x) = f(x) - Q_2.g(x) = r_2$$

Como queria-se demonstrar

■

Teorema 2.5. Todo ideal de $\mathcal{A}[x]$ é principal

Demonstração: Seja $\mathcal{I}$ um ideal de $\mathcal{A}[x]$. Se $\mathcal{I} = \{0\}$ então $\mathcal{I}$ é gerado por 0. Suponha-se que $\mathcal{I} \neq \{0\}$ e que $0 \neq P(x)$ tal que $\partial P(x)$ seja menor possível. Se $P(x) = a$ constante $\neq 0$ então $1 = a^{-1}.a \in \mathcal{I}$ e assim segue imediatamente que $\mathcal{I} = \mathcal{A}[x]$ é gerado por $1 \in \mathcal{A}[x]$. Suponhamos então $\partial P(x) > 0$.

Como $P(x) \in \mathcal{I}$ temos $\mathcal{A}[x].P(x) \subset \mathcal{I}$. Agora se prova que $\mathcal{I} \subset \mathcal{A}[x].P(x)$ e isto demonstra o teorema. De fato, seja $f(x) \in \mathcal{I}$ pelo algoritmo de Euclides temos que $\exists\, Q(x), r(x) \in \mathcal{A}[x]$ tais que $f(x) = Q(x).p(x) + r(x)$, onde $r(x) = f(x) - Q(x).P(x) \in \mathcal{I}$ e pela minimalidade da nossa escolha do polinômio $P(x) \in \mathcal{I}$ segue que $r(x) = 0$ e portanto, temos $f(x) = Q(x).P(x) \in \mathcal{A}[x].P(x)$. Como queríamos demonstrar

■

Definição 2.14. Sejam $f(x), g(x) \in \mathcal{A}[x]$, polinômios não nulos e seja $d(x) \in \mathcal{A}[x]$ um polinômio mônico tal que $d(x)$ divide $f(x)$ e $g(x)$ e todo divisor desses, também é de $d(x)$, ou seja, $d_1(x) \in \mathcal{A}[x]$ tal que $d_1(x) \mid f(x)$ e $d_1(x) \mid g(x)$, então $d_1(x) \mid d(x)$. A este polinômio $d(x)$ chama-se de máximo divisor comum de $f(x)$ e $g(x)$. Se $d(x) = 1$, então $f(x)$ e $g(x)$ são primos entre sí.

Teorema 2.6. (Existência de M.D.C) Sejam

$$P_1(x), \dots, P_m(x) \in \mathcal{A}[x] - \{0\}$$

E seja o ideal $\mathcal{I} = \mathcal{A}[x].P_1 + \cdots + \mathcal{A}[x].P_m(x)$ gerados pelos polinômios não nulos $P_1(x), \dots, P_m(x)$. Se $d(x) \in \mathcal{A}[x]$ é tal que $\mathcal{I} = \mathcal{A}[x].d(x)$ então as seguintes propriedades são válidas:

(i) Existem $r_1(x), \dots, r_m(x) \in \mathcal{A}[x]$ tais que $d(x) = r_1(x).p_1(x), \dots, r_m(x).P_m(x)$;

(ii) $d(x)$ é um divisor comum de $P_1(x), \dots, P_m(x)$;

(iii) Se $d_1(x)$ é um divisor comum qualquer de $P_1(x), \dots, P_m(x)$, então $d_1(x)$ é também um divisor de $d(x)$

Demonstração: (i) Temos que da igualdade

$$\mathcal{A}[x].d(x) = \mathcal{A}[x].P(x), \dots, \mathcal{A}[x].P_m(x)$$

(ii) Seja $i = (1, \dots, m)$ e $\mathcal{A}[x].d(x) = \mathcal{A}[x].P_1(x), \dots, \mathcal{A}[x].P_m(x)$, temos que,

$$P_i(x) \in \mathcal{A}[x].P_i(x) \subset \mathcal{A}[x].P_1(x) + \cdots + \mathcal{A}[x].P_m(x) = \mathcal{A}[x].d(x)$$

E, portanto, existe $r_i(x) \in \mathcal{A}[x]$ tal que $P_i(x) = r_i(x).d(x)$ isto é, $d(x)$ é um divisor de cada $P_i(x)$, com $i = (1, \dots, m)$

(iii) Seja $d_1(x)$ um divisor comum em $\mathcal{A}[x]$, de $P_1(x), \dots, P_m(x)$, isto é, existe $r_i(x) \in \mathcal{A}[x]$ tal que $P_i(x) = r_i(x).d(x)$, com $i = (1, \dots, m)$

Assim,

$$\mathcal{A}[x].P_i(x) \subset \mathcal{A}[x].d_1(x), \forall\, i = (1, \dots, m)$$

E daí segue que,

$$\mathcal{A}[x].d(x) = \mathcal{A}[x].P_1(x), \dots, \mathcal{A}[x].P_m(x) \subset \mathcal{A}[x].d_1(x)$$

Ou seja, existe $r(x) \in \mathcal{A}[x]$ tal que $d(x) = r(x).d_1(x)$

■

Definição 2.15. Um polinômio não nulo e não invertível $P(x) \in \mathcal{A}[x]$ se diz irredutível sobre $\mathcal{A}[x]$ se uma decomposição de $P(x)$ num produto de dois polinômios de $\mathcal{A}[x]$, ou seja, se $P(x) = f(x).g(x)$ então $f(x)$ é invertível ou $g(x)$ invertível. Se $P(x)$ for não irredutível sobre $\mathcal{A}[x]$ dizemos que $P(x)$ é redutível sobre $\mathcal{A}[x]$.

Exemplo 2.20. O polinômio $P(x) = x^2 - 3$ é irredutível em $\mathbb{Q}[x]$, porém $P(x) = x^2 - 3$ é redutível em $\mathbb{R}[x]$, pois,

$$x^2 - 3 = \left(x - \sqrt{3}\right).\left(x + \sqrt{3}\right), \text{com } \sqrt{3} \in \mathbb{R}$$

Proposição 2.7. Todo polinômio de grau 1 sobre um corpo K é irredutível.

Demonstração: De fato, seja $P(x)$ um polinômio de grau 1 e se $P(x) = f(x).g(x)$, então $\partial P(x) = \partial f(x) = \partial g(x)$. Mas, como $\partial P(x) = 1$, então $\partial f(x) + \partial g(x) = 1$. Como essa igualdade só é possível se $\partial f(x) = 1$ ou $\partial g(x) = 0$, ou vice-versa, então $f(x)$ ou $g(x)$ é invertível.

Definição 2.16. Seja K um corpo. Se todo polinômio não constante de $K[x]$ tem pelo menos uma raiz em K,diz-se que K é um corpo algebricamente fechado.

Proposição 2.8. Um polinômio sobre um corpo K algebricamente fechado é irredutível se, e somente se, tem grau 1

Demonstração: Seja $P(x) \in K[x]$ um polinômio irredutível. Como K é algebricamente fechado, existe $a \in K$ tal que $P(a) = 0$. Logo, $x - a \mid P(x)$ e, portanto, existe $g(x) \in K[x]$ tal que:

$$P(x) = (x - a).g(x)$$

Como, porém, $P(x)$ é irredutível, então o polinômio $g(x)$ é constante não nulo, isto é, existe $u \in K$ tal que $g(x) = u$, para todo $x \in K$. Portanto

$$P(x) = ux - ua$$

Em que ua é constante. Logo, o grau de $P(x)$ é 1. A reciproca é verdadeira, devido a proposição anterior

■

Teorema 2.7. Sejam K um corpo e $P(x) \in K[x]$. Então as seguintes condições são equivalentes.

(i) $P(x)$ é irredutível sobre K

(ii) $\mathcal{J} = K[x].P(x)$ é um ideal maximal em $K[x]$

(iii) $K[x]/\mathcal{J}$ é um corpo, onde $\mathcal{J} = K[x].P(x)$

Demonstração: Vamos mostrar que $(i) \Leftrightarrow (ii)$

$(i) \Longrightarrow (ii)$ Suponha-se $P(x) \in K[x]$, com $P(x)$ irredutível sobre K e seja $\mathcal{I} = K[x].P(x) = \{g(x).P(x); g(x) \in K[x]\}$. Como o grau de $P(x) \geq 1$ temos imediatamente que $\mathcal{I} \neq K[x]$. Se $I = K[x].h(x)$ é um ideal de $K[x]$ tal que $I \supset \mathcal{I}$. Prova-se que $I = \mathcal{I}$ ou $I = K[x]$. Assim, $P(x) \in K[x].P(x) \subset K[x].h(x)$ nos diz que $P(x) = g(x).h(x)$ para algum $g(x) \in K[x]$. Como $P(x)$ é irredutível tem que $g(x) = a$ invertível ou $h(x) = b$ invertível $\in K[x] - \{0\}$, onde a e b são constantes. Se $g(x) = a \neq 0$, temos que $h(x) = a^{-1}.P(x)$ e, portanto, $I = K[x].h(x) \subset K[x].P(x) = \mathcal{I}$ e isto nos dá $I = \mathcal{I}$. Se $h(x) = b \neq 0$ tem-se $I = K[x].h(x) \subset K[x]$ e isso termina a implicação $(i) \Longrightarrow (ii)$.

$(ii) \Longrightarrow (i)$ Agora seja $\mathcal{I} = K[x].P(x)$ um ideal maximal em $K[x]$. Assim $\mathcal{I} \neq K[x]$ nos diz que $\partial P(x) \geq 1$. Suponhamos $g(x), h(x) \in K[x]$ e $P(x) = g(x).h(x)$. Assim, segue imediatamente que $\mathcal{I} \subset I = K[x].h(x)$ e como $\mathcal{I}$ é um ideal maximal, temos que $\mathcal{I} = I$ ou $I = K[x]$. Se $\mathcal{I} = I$ segue que $h(x) \in \mathcal{I} = K[x].P(x)$ e isto nos diz que $h(x) = f(x).P(x)$, para algum $f(x) \in K[x]$. Daí segue $P(x) = g(x).f(x).P(x)$, como $P(x) \neq 0$ e $K[x]$ é um domínio de integridade, teremos $1 = g(x).f(x)$, isto é, $g(x) \in K[x]$ é um polinômio irredutível em $K[x]$. Portanto, $g(x) = a \neq 0$ é um polinômio constante. Se $I = K[x]$ segue que $h(x) = b \neq 0$ constante, ou seja, $P(x)$ é irredutível sobre K. Como queríamos demonstrar.

■

Teorema 2.8. Seja K um corpo algebricamente fechado e $f(x)$ um polinômio de $\partial f(x) \geq 1$ sobre K cujo coeficiente dominante denota-se por a. Então podem ser determinados elementos $u_1, u_2, \ldots, u_n \in K$ tais que.

$$f(x) = a(x-u_1)(x-u_2)\ldots(x-u_n)$$

Demonstração: Demonstra-se por indução sobre n:

Se o $\partial f(x) = 1$, então $f(x) = ax + b$, com $a \neq 0$. Pondo a em evidência, temos:

$$f(x) = a(x + \frac{b}{a})$$

O que demonstra o teorema para $n = 1$

Seja $f(x)$ um polinômio de grau $n > 1$ e suponha-se o teorema verdadeiro para todo polinômio de grau $n-1$. Como K é algebricamente fechado, $f(x)$ tem uma raiz u_1 em K e, portanto:

$$f(x) = (x-u_1)Q(x), \text{com } Q(x) \in K[x]$$

Como $Q(x)$ tem grau $n-1$ e coeficiente dominante igual ao de $f(x)$, pela hipótese de indução, existem $u_1, u_2, \ldots, u_n \in K$ tais que:

$$Q(x) = a(x-u_1)(x-u_2)\ldots(x-u_n)$$

E com isso temos,

$$f(x) = a(x-u_1)(x-u_2)\ldots(x-u_n), \text{com } u_i = 1,2,\ldots n \text{ raizes de } f(x)$$

■

Definição 2.17. Um polinômio não constante pertencente a $K[x]$, se diz primitivo se a unidade de K é um máximo divisor comum de seus coeficientes.

Exemplo 2.21. O polinômio $f(x) = 2 + 2x + 3x^2 \in \mathbb{Z}[x]$ é primitivo, pois $mdc(2,3) = 1$

Proposição 2.9. Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ um polinômio não nulo. Então existem um elemento $d \in K$ e um polinômio $f^*(x) \in K[x]$ de mesmo grau de $f(x)$, tais que $f(x) = d.f^*(x)$

Demonstração: Se $d = mdc(a_0, a_1, \ldots, a_n)$ então $a_0 = dq_0, a_1 = dq_1, \ldots, a_n = dq_n$, onde $q_0, q_1, \ldots, q_n \in K$ são primos entre si. Daí:

$$f(x) = (dq_0) + (dq_1)x + \cdots + (dq_n)x^n$$

Fazendo-se $f^*(x) = f(x) = q_0 + q_1x + \cdots + q_nx^n$

Então $f^*(x)$ tem o mesmo grau de $f(x)$ é primitivo e $f(x) = df^*(x)$

■

Proposição 2.10. Seja $f(x) \in K[x]$ um polinômio não constante. Se $f(x)$ é irredutível então $f(x)$ é primitivo.

Demonstração: Suponha-se que $f(x)$ não fosse primitivo e seja d o mdc dos seus coeficientes, então, devido a proposição anterior, temos $f(x) = df^*(x)$ em que $\partial f^*(x) = \partial f(x)$. Como d não é invertível em K, também não o é em $K[x]$. Por outro lado, $f^*(x)$ não é invertível em $K[x]$. Então $f(x) = df^*(x)$ é uma composição não trivial de f em $K[x]$, o que contraria a hipótese de $f(x)$ ser irredutível sobre K de onde, $f(x)$ é primitivo.

■

Contraexemplo: Um polinômio primitivo pode não ser irredutível. O polinômio $f(x) = 2 + 5x + 2x^2$ é primitivo, mas composto em $\mathbb{Z}[x]$, uma vez que $f(x) = (2x + 1)(x + 2)$.

Lema 2.1. Se $f(x), g(x) \in K[x]$ são polinômios primitivos e para elementos $a, b \in K$ tem-se a igualdade $af(x) = bg(x)$, então $a \sim b$ e $f(x) \sim g(x)$.

Demonstração: Faça-se $af(x) = h(x)$ e seja d o mdc dos coeficientes de $h(x)$. Então $h(x) = dh^*(x)$, em que $h^*(x)$ é um polinômio primitivo com o mesmo grau de $h(x)$ (proposição anterior). Por outro lado, como $af(x) = h(x)$, então a divide todos os coeficientes de $h(x)$ e, portanto, a divide d em K. Logo, $d = ac$, para $c \in K$. Desse modo,

$$h(x) = dh^*(x) = ach^*(x) = af(x)$$

Como $a \neq 0$, então a igualdade fica $f(x) = ch^*(x)$ o que mostra que c divide $f(x)$ e, portanto, seus coeficientes. Como $f(x)$ é primitivo, então c é invertível. Então da igualdade $d = ac$, conclui-se que $d \sim a$. Da mesma forma demonstra-se que $d \sim b$, de onde $a \sim b$.

Agora o fato de a e b serem associados implica a existência de um elemento invertível $u \in K$ tal que $b = au$. Usando esse fato em $af(x) = bg(x)$, obtemos $af(x) = aug(x)$ e, portanto $f(x) = ug(x)$. Isso mostra que $f(x) \sim g(x)$ como queríamos demonstrar.

■

Lema 2.2. (Lema de Gauss) O produto de dois polinômios primitivos $f(x), g(x) \in K[x]$ também é um polinômio primitivo.

Demonstração: Sejam $f(x), g(x) \in K[x]$, tais que

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \; e$$

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$$

E que o produto $f(x).g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n+m}x^{n+m}$ não fosse primitivo existiria então, em K, um elemento p irredutível divisor de todos os coeficientes de $f(x), g(x)$. Mas p não divide todos os coeficientes de $f(x)$, nem tampouco de $g(x)$. Seja a_r coeficientes de $f(x)$ tal que $p \nmid a_r$ e, também b_s coeficientes de $g(x)$ onde $p \nmid b_s$. Temos:

$$c_{r+s} = a_0b_{r+s} + a_1b_{r+s-1} + \cdots + a_rb_s + \cdots + a_{r+s-1}b_1 + a_{r+s}b_0$$

Devido as suposições, temos que p divide as parcelas do segundo membro dessa igualdade anteriores e posteriores ao produto a_rb_s. Como p divide c_{r+s} então p divide a_rb_s e, sendo irredutível, divide um desses fatores. Essa conclusão nos leva em um absurdo. Portanto $f(x).g(x)$ é primitivo.

■

Lema 2.3. Seja $\mathcal{A}$ o corpo de frações de K**.** Se o polinômio $f(x) \in K[x]$ é irredutível sobre $\mathcal{A}$, então também é irredutível sobre K**.**

Demonstração: Suponha-se por absurdo que $f(x)$ fosse composto em $\mathcal{A}[x]$, existiriam $g(x), h(x) \in \mathcal{A}[x]$ de grau ≥ 1, tais que $f(x) = g(x).h(x)$. Os coeficientes de $f(x)$ e $g(x)$ são frações cujos termos pertencem a $\mathcal{A}$. Indicando-se por a o produto dos denominadores dessas frações, temos:

$$a.f(x) = g_1(x).h_1(x)$$

Onde $g_1(x), h_1(x) \in K[x]$ com o mesmo grau de $g(x)$ e $h(x)$, respectivamente. Sejam b, c e d máximos divisores comuns de $f(x), g_1(x), h_1(x)$, então:

$$f(x) = b.f_1(x), g_1(x) = c.g_2, h_1(x) = d.h_2$$

Com $f_1(x), g_2(x), h_2(x)$ primitivos com mesmo grau de $f(x), g_1(x), h_1(x)$. **(proposição 2.9)** temos:

$$a.b.f_1(x) = c.d.g_2(x).h_2(x)$$

Como $g_2(x).h_2(x)$ é primitivo, devido ao **lema de Gauss** então o **lema 2.2** garante que $ab \sim cd$ e $f_1(x) \sim g_2(x).h_2(x)$

Assim, $f_1(x) = ug_2(x)h_2(x)$ com $u \in \mathcal{A}$ invertível, e, portanto,

$$f(x) = bf_1(x) = \big(bug_2(x)\big)h_2(x)$$

Como $(ub)g_2(x)$ e $h_2(x)$ são polinômios de $K[x]$ que tem graus iguais aos de $g_1(x), h_1(x)$, respectivamente, e, portanto, ≥ 1, então $f(x)$ é composto sobre $\mathcal{A}$, o que é absurdo, uma vez que essa conclusão contraria a hipótese.

■

Proposição 2.11. (Critério de Eisenstein)

Seja $f(x) \in K[x]$ tal que $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$. Se existir um elemento irredutível $p \in K$ que seja divisor de $a_0, a_1, \ldots, a_{n-1}$ mas não de a_n e se p^2 não divide a_0, então $f(x)$ é irredutível sobre o corpo das frações K.

Demonstração: Seja $\mathcal{A}$ o corpo das frações de K e suponha-se $f(x)$ composto em $\mathcal{A}[x]$, então $f(x)$ é o produto de dois polinômios de grau ≥ 1 de $\mathcal{A}[x]$. Mas, considerando a contra positiva do lema anterior, $f(x)$ também pode ser decomposto em um produto de dois fatores não triviais de $K[x]$

$$f(x) = (b_0 + b_1x + b_2x^2 + \cdots + b_rx^r)(c_0 + c_1x + c_2x^2 + \cdots + c_tx^t)$$

Como p divide $a_0 = b_0c_0$ e p^2 não divide a_0, então $p \mid b_0$ ou $p \mid c_0$, exclusivamente. Suponha-se que $p \mid b_0$, como p não divide $a_n = b_rc_t$, então $p \nmid b_r$. Isso posto, seja s $(0 < s \leq r < n)$ o menor índice tal que p não divide b_s. Portanto, $p \mid b_0, p \mid b_1, \ldots, p \mid b_{s-1}$ e p não divide b_s. Como:

$$a_s = b_0c_s + b_1c_{s-1} + b_2c_{s-2} + \cdots + b_{s-1}c_1 + b_sc_0$$

e, pois $s < n$, então $p \mid b_sc_0$. Não dividindo c_0, então $p \mid b_s$, o que é absurdo.

■

Exemplo 2.22. O polinômio $f(x) = 7 + 14x + x^{60} \in \mathbb{Z}[x]$ é irredutível em $\mathbb{Q}[x]$**.** De fato, considerando o número primo $p = 7$, vemos que $7 \mid 7, 7 \mid 14$, mas $7 \nmid 1$ e $7^2 \nmid 7$.

3. EXTENSÃO ALGÉBRICAS DE CORPOS

Neste capitulo, anota-se os conceitos de extensões de corpos atrelados as equações polinomiais, onde iremos representar corpos K, tais que $\mathbb{Q} \subset K \subset \mathbb{C}$. Para isso usam-se polinômios irredutíveis no processo da demonstração do último teorema ao final do nosso trabalho.

Definição 3.1. Uma extensão de corpo é um monomorfismo $\varphi: K \longrightarrow L$, em que K e L são subcorpos complexos. Em outras palavras, diremos que K é o corpo menor e que L é o corpo maior. Simbolicamente, $L \supset K$.

Exemplo 3.1. As funções inclusões $\varphi_1: \mathbb{Q} \longrightarrow \mathbb{R}$, $\varphi_2: \mathbb{R} \longrightarrow \mathbb{C}$ e $\varphi_3: \mathbb{Q} \longrightarrow \mathbb{C}$ são extensões de corpos, tais inclusões são monomorfismo

Definição 3.2. Uma extensão simples de um corpo L sobre o subcorpo K tal que, $K \supset L$ e $L = K(\alpha)$ para algum $\alpha \in L$, ou seja, uma extensão simples é resultado da adição de um único elemento ao corpo menor.

Exemplo 3.2. O subcorpo $\mathbb{R}(i)$ de $\mathbb{C}$, contém os elementos da forma $x + iy$, com $x, y \in \mathbb{R}$. Mas, estes elementos acabam por percorrer todo o conjunto $\mathbb{C}$, assim, $\mathbb{C} = \mathbb{R}(i)$.

Definição 3.3. Seja K um subcorpo de L, e seja $\alpha \in L$**.** Então, dizemos que α é algébrico sobre K, tal que $P(\alpha) = 0$. Caso contrário, dize-se que α é transcendente sobre K.

Exemplo 3.3. O número $\alpha = \sqrt{2}$ é algébrico sobre $\mathbb{Q}[x]$, pois o polinômio $P(x) = x^2 - 2$ tem α como raiz, isto é, $P(\alpha) = \alpha^2 - 2 = \left(\sqrt{2}\right)^2 - 2 = 0$.

Exemplo 3.4. O número π é transcendente sobre $\mathbb{Q}[x]$. Mas, π é algébrico em $\mathbb{R}[x]$, pois é raiz do polinômio $P(x) = x - \pi \in \mathbb{R}[x]$.

Definição 3.4. Seja L uma extensão de K, e suponha-se que $\alpha \in L$ é algébrico sobre K. Então o polinômio minimal de α sobre K, é o único polinômio mônico $P(x)$ sobre K de menor grau tal que $P(\alpha) = 0$.

Lema 3.1. Se α é um elemento algébrico sobre o subcorpo K de L, então o polinômio minimal de α sobre K é irredutível sobre K. Ele ainda divide qualquer polinômio em que α é um zero.

Demonstração: Suponha-se que o polinômio minimal $P(x)$ de α sobre K é irredutível, isto é, $P(x) = f(x).g(x)$, com $f(x), g(x) \in K[x]$ de graus menores que $P(x)$. Pode-se assumir que $f(x), g(x)$ são mônicos. Então, como $P(\alpha) = 0$, deve-se ter $f(\alpha).g(\alpha) = 0$, e como $K[x]$ é um domínio de integridade, $f(\alpha) = 0$ ou $g(\alpha) = 0$, o que contraria a definição de polinômio minimal. Portanto, $p(x)$ é irredutível sobre K.

Suponha-se agora que $f(x)$ é um polinômio sobre K, tal que $f(\alpha) = 0$. Assim, pelo algoritmo da divisão, existem polinômios $Q(x), r(x) \in K[x]$, tais que $f(x) = P(x).Q(x) + r(x)$, com $r(x) = 0$ ou $\partial r(x) < \partial p(x)$. Então, $0 = f(\alpha) = P(\alpha).Q(\alpha) + r(\alpha) = 0.Q(\alpha) + r(\alpha) = r(\alpha)$. Se tivermos $r(x) \neq 0$, então existe um múltiplo constante de $r(x)$ que é mônico, e deste modo, o grau deste é menor do que o grau de $P(x)$, gerando uma contradição com o fato de $m = P(x)$ ser o polinômio minimal de α sobre K. Portanto, $r(x) = 0$, e $P(x)$ divide $f(x)$.

■

Teorema 3.1. Se K é um subcorpo de L e $P(x)$ é um polinômio mônico irredutível sobre K, então existe um $\alpha \in L$, algébrico sobre K, tal que α tem $P(x)$ como o polinômio minimal sobre K.

Demonstração: Seja α um zero qualquer de $P(x)$ em L. Então, $P(\alpha) = 0$, portanto, o polinômio minimal $f(x)$ de α sobre K, divide $P(x)$. Ora, $P(x)$ é irredutível sobre K, e ambos $f(x)$ e $P(x)$ são mônicos, logo $f(x) = P(x)$

■

Definição 3.5. (Extensão Finita). Se uma extensão L de um corpo K tem dimensão finita n como espaço vetorial sobre K, então L é uma extensão finita e grau n sobre K. Esse grau será denotado por $[L:K]$

Proposição 3.1. Toda extensão finita é algébrica.

Demonstração: Sejam L/K uma extensão finita e $\alpha \in L$. Então existe $n \geq 1$ inteiro mínimo tal que $\{1, \alpha, \dots, \alpha^{n-1}\}$ é um conjunto K −linearmente independente. Ou seja, existem $a_0, \dots, a_n \in K$ não todos nulos tais que

$$\sum_{i=0}^{n} a_i \alpha^i = 0$$

A fortiori, α é raiz do polinômio não nulo

$$f = \sum_{i=0}^{n} a_i x^i$$

■

Definição 3.6. Seja L/K uma extensão algébrica. Suponha-se que existam $\alpha_1, \dots, \alpha_r \in L$ tais que:

$$K \subset K_1 = K[\alpha_1] \subset K_2 = K_1[\alpha_2] \dots \subset K_r = K_{r-1}[\alpha_r] = K[\alpha_1, \dots, \alpha_r] = L.$$

Diz-se que L/K é uma extensão finitamente gerada e que L é gerada sobre K por $\alpha_1, \dots, \alpha_r$.

Proposição 3.2. Seja L/K uma extensão algébrica. Então L/K é finita se, e somente se L/K é finitamente gerada.

Demonstração: Suponha que L/K seja finita. Se $L = K$ acabou. Senão existe $\alpha_1 \in L \setminus K$. Seja $K_1 = K[\alpha_1]$. Se $L = K_1$ acabou. Senão existe $\alpha_2 \in L \setminus K_1$. Seja $K_2 = K_1[\alpha_2]$. Prosseguindo o argumento tem-se uma sequência de corpos estrita, isto é,

$$K \subsetneq K_1 \subsetneq K_2 \subsetneq \cdots.$$

Como L/K é finita esta sequência não pode ser infinita. Logo existe r tal que $L = K_r$ e L/K é finitamente gerada.

Reciprocamente, se L/K é finitamente gerada então cada extensão K_i/K_{i-1} é finita e pela transitividade de extensão finita, conclui-se que L/K também é finita.

■

Exemplo 3.5. Seja L/K uma extensão com $[L:K] = p$ número primo. Então para todo $K \subset K' \subset K$ temos que $K' = K$ ou $K' = L$. Em particular, dado $\alpha \in L \setminus K$, então $L = K[\alpha]$.

3.1. Extensão de isomorfismo de corpos

Teorema 3.2. Se $\alpha \in L \supset K$ e se $\psi: K[x] \longrightarrow L$ é definida por $\psi\big(f(x)\big) = f(\alpha)$, então é um homomorfismo tal que:

(i) $Im(\psi) = K[\alpha], K \subset K[\alpha] \subset L$;

(ii) α é transcendente sobre K se, e somente se, $ker(\psi) = \{0\}$;

(iii) Se α é algébrico sobre K e $P(x) = irr(\alpha, K)$, então $ker(\psi) = K[x].P(x)$um ideal maximal de $K[x]$;

(iv) $K[x]/ker(\psi) \simeq K[\alpha]$

Demonstração: ψ está claramente bem definida e agora se mostra que ψ é de fato um homomorfismo de anéis.

Considere $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + \cdots + b_mx^m$ com $m \leq n$. Assim

$$\begin{aligned}\psi\big(f(x) + g(x)\big) &= \psi\big((a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_m + b_m)x^m + a_{m+1}x^{m+1} + \cdots \\ &+ a_nx^n\big) = a_0 + a_1\alpha + \cdots + a_n\alpha^n + b_0 + b_1\alpha + \cdots + b_m\alpha^m = f(\alpha) + g(\alpha) \\ &= \psi\big(f(x)\big) + \psi\big(g(x)\big)\end{aligned}$$

E também:

$$\begin{aligned}\psi\big(f(x), g(x)\big) = \psi(d_0 + d_1x + \cdots + d_nx^n &= d_0 + d_1\alpha + \cdots + d_n\alpha^n \\ &= (a_0 + a_1\alpha + \cdots + a_n\alpha^n).(b_0 + b_1\alpha + \cdots + b_m\alpha^m) = f(\alpha).g(\alpha) \\ &= \psi\big(f(x)\big).\psi(g(x))\end{aligned}$$

Onde $d_i = \sum_{j=0}^{i} a_j b_{i-j}$

Portanto, ψ é um homomorfismo de anéis.

Agora se mostra os itens (i) à (iv)

$i)$ Temos que,

$$Im(\psi) = \{f(\alpha); \psi\big(f(x)\big) = f(\alpha)\}$$

Mas ψ esta definida em $K[x]$, de modo que todo $f(x) \in K[x]$.

Dai, $Im(\psi) = \{f(\alpha); f(x) \in K[x]\}$

E por definição, isto é $K[\alpha]$. Logo, $Im(\psi) = K[\alpha]$

Para verificar-se que $K[\alpha]$ contém K, basta tomar a função $g(\alpha_i) = a_i,\ a_i \in K, i = 1,2, \ldots$

$ii)$ Seja,

$$\ker(\psi) = \{f(x) \in K[x] : \psi\big(f(x)\big) = 0\}$$

Como α é transcendente sobre K, seja $f(x) \in K[x] - \{0\}$ segue, por definição, que $f(\alpha) \neq 0$. Mas $\psi\big(f(x)\big) = f(\alpha)$ o que implica que $\psi(f(x)) \neq 0$. Logo o único polinômio que anula α é o polinômio nulo. Portanto, $ker = \{0\}$. Reciprocamente, supondo que $ker = \{0\}$, onde o polinômio nulo, vem que para todo $f(x) \neq 0 \in K[x]$ têm-se

$$\psi(f(x)) \neq 0$$

Como $\psi\big(f(x)\big) = f(\alpha)$, temos que,

$$\psi\big(f(x)\big) = f(\alpha) \neq 0$$

Deste modo α é transcendente sobre K.

Feito isso, pode-se definir $\psi : K[x] \longrightarrow L$ como uma aplicação injetiva, pois $ker(\psi) = \{0\}$. Segue do **Teorema 1.4** item (ii). Portanto, ψ é um isomorfismo de anéis.

$iii)$ Como α é algébrico sobre K, então $ker(\psi) \neq \{0\}$. Considere então $ker(\psi) = K[x].P(x)$ um ideal em $K[x]$. Como $P(x)$ é irredutível sobre K, pelo **Teorema 2.7** temos que $ker(\psi) = K[x].P(x)$ é um ideal maximal em $K[x]$

$iv)$ Segue pelo item $i)$ deste teorema que $Im(\psi) = K[x]$ e agora é imediato do **Teorema 2.3** item $iii)$ que

$$K[x]/ker(\psi) \simeq K[\alpha]$$

Corolário 3.1. Sejam extensão de K e $\alpha \in L$. Então:

$i)$ Se α é algébrico sobre K, então $K[\alpha]$ é um subcorpo de L que contém K

$ii)$ Se α é transcendente sobre K então $K[\alpha]$ é um subdomínio de L isomorfo ao domínio $K[x]$ dos polinômios em uma indeterminada x

Demonstração: (i) Adota-se um homomorfismo nas condições do **Teorema 3.2**. anterior, ou seja, $\psi: K[x] \longrightarrow L$ é definida por $\psi\big(f(x)\big) = f(\alpha)$. Suponha α algébrico sobre K e seja $P(x) = irr(\alpha, K) \in K[x]$. Pelo item (iii) do **Teorema 2.7**. tem-se que $ker(\psi) = K[x].P(x)$ é um ideal maximal e portanto,

$$\frac{K[x]}{ker(\psi)} \simeq K[\alpha]$$

Como $K[\alpha]$ é isomorfo ao corpo $\frac{K[x]}{ker(\psi)}$ segue que $K[x]$ também é um corpo.

$ii)$ Para demonstrar este item, precisa-se mostrar que $K[\alpha]$ é um subanel e que não possui divisores de zero. Considere $f(\alpha), g(\alpha) \in K[\alpha]$. Note que

1) $f(\alpha) - g(\alpha) = (f - g)(\alpha) \in K[\alpha]$

2) $f(\alpha).g(\alpha) = (f.g)(\alpha) \in K[\alpha]$

Agora, observe que $K[\alpha]$ não possui divisores de zero, pois

$$f(\alpha).g(\alpha) = 0 \Longrightarrow f(\alpha) = 0 \; ou \; g(\alpha) = 0$$

Como α é transcendente sobre $K[\alpha]$, vem que

$$f(\alpha) = 0(\alpha) \; ou \; g(\alpha) = 0(\alpha)$$

■

Corolário 3.2. Se L uma extensão de K e se $\alpha, \beta \in L$ são raízes de um mesmo polinômio irredutível sobre K, então $K[\alpha]$ e $K[\beta]$ são corpos isomorfos.

Demonstração: Por hipótese, $P(x) = irr(\alpha, K)$.Agora pelo item $iii)$ do **Teorema 2.7**, obtemos,

$$\mathcal{J} = K[x].P(x)$$

E por (iv) temos $K[\alpha] \simeq \frac{K[x]}{\mathcal{J}}$ e da mesma forma $\frac{K[x]}{\mathcal{J}} \simeq K[\beta]$ logo,

$$K[a] \simeq K[\beta]$$

São corpos isomorfos.

■

Proposição 3.3. Seja L uma extensão de K $\alpha \in L$ algébrico sobre K. Se o grau do polinômio $irr(\alpha, K)$ é n, então:

(i) Qualquer $f(x) \in K[x], f(\alpha)$ pode ser expresso de modo único na forma,

$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}, onde\ a_i \in K.$$

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

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

Demonstração: Seja $P(x) = irr(\alpha, K)$. Por hipótese temos, $\partial P(x) = n$.

$i)$ Se $f(x) \in K[x]$ então pelo algoritmo da divisão existem $q(x), r(x) \in K[x]$ tais que

$$f(x) = q(x).P(x) + r(x), onde\ r(x) = 0\ ou\ \partial r(x) < \partial P(x).$$

Assim $r(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}, onde\ a_i \in K$.

Agora temos,

$$f(\alpha) = q(\alpha).P(\alpha) + r(\alpha)$$

Como $P(\alpha) = 0$ segue que $f(\alpha) = r(\alpha)$,ou seja, $f(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$.

Agora se demonstra a unicidade da expressão.

Se $f(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}, a_i, b_i \in K, \forall i \in \{1, \dots, n-1\}$

Segue imediatamente que ao polinômio $q(x) \in K[x]$ onde

$$q(x) = (a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_{n-1} - b_{n-1})x^{n-1}$$

É tal que $q(\alpha) = 0$ e $\partial q(x) < n = \partial irr(\alpha, K)$. Assim $q(x) = 0$ e daí segue

$$a_i = b_i, \forall i \in \{1, \dots, n-1\}$$

(ii) Primeiro mostra-se que $K[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}, a_i \in$ K$\}$.Por definição $K[\alpha] = \{f(\alpha); f(x) \in K[x]\}$, agora pelo item (i) desta proposição $f(\alpha)$ pode ser expresso de modo único na forma $f(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$, onde $a_i \in K$, daí temos:

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

O fato de $K[\alpha]$ ser um subcorpo de L que contem K segue imediatamente do item (i) do **Corolário 3.1**

(iii) Para demonstrar este item basta observar que pelos itens anteriores temos;

$$\mathbb{Z}_p[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}, a_i \in \mathbb{Z}_p\}$$

Assim existe uma correspondência bijetora entre $\mathbb{Z}_p[\alpha]$ e o conjunto de todas as $n-uplas\ (a_o, a_1, \dots, a_{n-1})$ onde cada $a_i \in \mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$.

■

3.2. Algumas aplicações

Aplicação 1. Seja $\alpha = \sqrt[n]{p} \in \mathbb{R}, n \geq 2$ inteiro e $p \geq 2$ um número primo. Então α é uma raiz real do polinômio $x^n - p$ que é, pelo ***critério de Eisenstein***, irredutível sobre $\mathbb{Q}$. E $\mathbb{Q}[\alpha]$ é um subcorpo de $\mathbb{R}$ contento $\mathbb{Q}$

Primeiro verifica-se o polinômio $x^n - p$ é irredutível. Pelo critério de Eisenstein, tem-se que existe um número p primo. Então p divide x^n, por definição, e p divide p. Mas p^2 não divide p. Logo, $x^n - p$ é irredutível. Pelo item (i) do **Corolário 3.1**,temos que $\mathbb{Q}[\alpha]$ é um subcorpo de $\mathbb{R}$ contento $\mathbb{Q}$. E ainda, $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}, a_i \in \mathbb{Q}\}$.

Aplicação 2. Seja K um corpo, L/K uma extensão e $\tau \in L$ transcendente sobre K. Afirma-se que K é algebricamente fechado em $K(\tau) = \{f(\tau)/g(\tau)\,; f, g \in K[x], g \neq 0\}$. De fato, se existisse $\alpha \in K(\tau) \setminus K$ algébrico sobre K, digamos $\alpha = f(\tau)/g(\tau)$, então $K[\alpha]\ /\ K$ seria finita. Observe que $h = f(x) - \alpha g(x) \in (K[\alpha])[x]$ e $h(\tau) = 0$, ou seja, τ é algébrico sobre $K[\alpha]$. Portanto, $K(\tau) = (K[\alpha])[\tau]$ é algébrico sobre K, mas isso é impossível, pois τ é transcendente sobre K.

Aplicação 3. Seja L/K uma extensão de corpos e $A_L(K)$ o conjunto dos elementos $\alpha \in L$ que são algébricos sobre K. Agora se mostra que este conjunto é um corpo. De fato, basta mostrar que dados $\alpha, \beta \in A_L(K) - \{0\}$, então $\alpha + \beta, \alpha\beta, \alpha^{-1} \in A_L(K)$. Pelo **corolário 3.2** do **teorema 3.2.**, temos que $K[\alpha]$ e $K[\beta]$ são corpos e $K[\alpha]/K$ e $K[\beta]/K$ são finitas. Seja $K[\alpha, \beta]$ a extensão gerada sobre K por α e β. Vamos analisar o seguinte diagrama.

$$K[\alpha,\beta]$$

$$\nearrow \quad \uparrow \quad \nwarrow$$

$$K[\alpha] \;\; K[\alpha+\beta] \;\; K[\beta]$$

$$\nwarrow \quad \uparrow \quad \nearrow$$

$$K$$

A extensão $K[\alpha,\beta]$ é gerada por β sobre $K[\alpha]$. Como β é algébrico sobre K e $K \subset K[\alpha]$, conclui-se que β é algébrico sobre $K[\alpha]$. Logo a extensão $K[\alpha,\beta]/K[\alpha]$ é finita. Pela transitividade de extensões finitas, conclui-se que $K[\alpha,\beta]/K$. Mas, $K \subset K[\alpha+\beta] \subset K[\alpha,\beta]$. Logo $K[\alpha+\beta]\,/\,K$ é finita, portanto $\alpha+\beta \in A_L(K)$. Da mesma maneira mostra-se para $\alpha\beta, \alpha^{-1}$. Com isso, $\alpha+\beta, \alpha\beta, \alpha^{-1} \in A_L(K)$. Portanto, $A_L(K)$ é um corpo.

CONSIDERAÇÕES FINAIS

Esta parte da dissertação desse trabalho será usada para apresentar tópicos de estudos como sugestão para trabalhos futuros, como abranger a teoria de Galois e de construção de corpos através do processo de adjunção de raízes. Poderíamos fazer um estudo mais aprofundado da questão de grupos, mas foi mais que suficiente mostrar as definições de grupos e das implicações das definições sobre um dado conjunto munido de uma operação $\star$, para compreendermos a sequência do trabalho. Da mesma maneira, as definições de estruturas de anéis e corpos que contribuíram para abrangermos os nossos estudos sobre extensões algébricas de corpos.

Contudo, com o objetivo de tratar no nosso trabalho a demonstração do teorema 3.2. , que nos dá uma análise de como usar raízes algébricas ou transcendente α de uma extensão de corpos, L/K com $\alpha \in L \supset K$, para verificar se um polinômio é irredutível pode estar satisfazendo a noção de corpos do conjunto $K[x]$ de todos os polinômios, ou verificar se $K[x]$ pode ser ou não um corpo.

REFERÊNCIAS

DOMINGUES, Hygino H.; IEZZI, Gelson. 4 ed. Reformulada- São Paulo: atual 2003;

GONLÇALVES, A. Introdução à Álgebra. 5 ed. Rio de janeiro: IMPA, 2011;

GARCIA, Arnaldo; Lequain, Yves. Elementos de álgebra. Rio de Janeiro: IMPA, dezembro de 2001

PACHECO, Amílcar. Álgebra. Universidade Federal do Rio de janeiro. Departamento de Matemática Pura.

SILVA, Erivaldo de Oliveira. Extensão algébrica dos Racionais. 2013. 49 folhas, TCC apresentado ao curso de Matemática do centro de Ciências e Tecnologia- Universidade Estadual da Paraíba;