



**UNIVERSIDADE ESTADUAL DA PARAÍBA - UEPB**  
CENTRO DE CIÊNCIAS E TECNOLOGIAS- CCT  
CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

**Erivaldo de Oliveira Silva**

## **Extensões Algébricas dos Racionais**

**Campina Grande - PB**  
**2013**

**ERIVALDO DE OLIVEIRA SILVA**

## **Extensões Algébricas dos Racionais**

Trabalho de Conclusão do Curso apresentado ao Centro de Ciências e Tecnologias- CCT da Universidade Estadual da Paraíba - UEPB , em cumprimento às exigências legais para a obtenção do título de Graduado no Curso de Licenciatura Plena em Matemática .

Orientação do Professor Ms. Marciel Medeiros de Oliveira

**Campina Grande - PB  
2013**

É expressamente proibida a comercialização deste documento, tanto na forma impressa como eletrônica. Sua reprodução total ou parcial é permitida exclusivamente para fins acadêmicos e científicos, desde que na reprodução figure a identificação do autor, título, instituição e ano da dissertação.

Silva, Jamilya Maria da.  
Função seno, função cosseno e aplicações [manuscrito] : / Jamilya Maria da Silva. - 2013.  
39 p. : il.  
  
Digitado.  
Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências Humanas e Exatas, 2013.  
"Orientação: Prof. Me. Marceli Medeiros de Oliveira, Departamento de Matemática".

1. Funções trigonométricas. 2. Função seno. 3. Função cosseno. I. Título.

21. ed. CDD 510

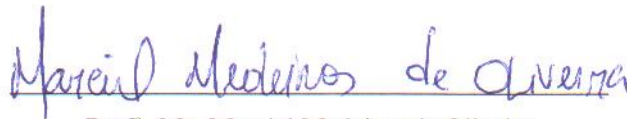
ERIVALDO DE OLIVEIRA SILVA

## Extensões Algébricas dos Racionais

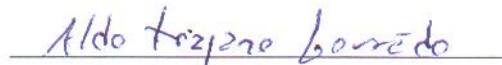
Trabalho de Conclusão do Curso apresentado ao Centro de Ciências e Tecnologias- CCT da Universidade Estadual da Paraíba - UEPB , em cumprimento às exigências legais para a obtenção do título de Graduado no Curso de Licenciatura Plena em Matemática .

Aprovado pela banca examinadora em 20 de dezembro de 2013.

### Banca Examinadora



Prof<sup>o</sup>. Ms. Marciel Medeiros de Oliveira  
Departamento de Matemática - Campus VI/UEPB  
Orientador



Prof<sup>o</sup> Dr. Aldo Trajano Lourêdo  
Departamento de matemática Campus I/UEPB  
Examinador



Prof<sup>o</sup> Dr. Vandenberg Lopes Vieira  
Departamento de Matemática - Campus I/UEPB  
Examinador

# Resumo

Neste trabalho apresentamos um estudo sobre extensões algébricas dos racionais, mais precisamente, apresentaremos uma construção de corpos  $K$ , com  $\mathbb{Q} \subset K \subset \mathbb{C}$  através de um processo chamado de adjunção de raízes de um polinômio. Nesse sentido, iniciamos com uma apresentação de conceitos básicos envolvendo anéis. Em seguida, fazemos uma introdução à extensão de corpos e finalmente construiremos os corpos  $K$  nas condições citadas.

**Palavras-Chave:** *Anéis, Extensão de corpos e extensão algébrica dos racionais.*

# Abstract

We present a study of algebraic extensions of rational, more precisely, we present a construction bodies  $K$  with contained in the body  $K$  and contained in the body of this complex by adjunct roots of a polynomial. Accordingly we started with a presentation of basic concepts involving rings. Then make an introduction to the extension of bodies and finally build bodies  $K$  in the mentioned conditions.

**Palavras-Chave:** *Rings, Extension of bodies and algebraic extension of the rational.*

# SUMÁRIO

|  |           |
|--|-----------|
| <b>1. Introdução</b> . . . . .                               | <b>8</b>  |
| 1.1. Anéis, ideais e homomorfismos . . . . .                 | 9         |
| 1.2. homomorfismos de anéis . . . . .                        | 13        |
| 1.3. Corpo de frações de um domínio . . . . .                | 15        |
| 1.4. Polinômio em uma variável . . . . .                     | 17        |
| <b>2. Introdução à extensão de corpos</b> . . . . .          | <b>26</b> |
| <b>3. Extensões Algébricas dos Racionais</b> . . . . .       | <b>30</b> |
| 3.1. Adjunção de Raízes . . . . .                            | 30        |
| 3.2. Corpo de decomposição de um polinômio . . . . .         | 34        |
| 3.3. Grau de uma Extensão . . . . .                          | 37        |
| <b>Referências</b> . . . . .                                 | <b>46</b> |
| <b>A. Algumas noções básicas de Álgebra Linear</b> . . . . . | <b>47</b> |

# 1 Introdução

Em matemática, Teoria de Galois é um ramo da álgebra abstrata.

No nível mais básico, ela usa grupo de permutações para descrever como as várias raízes de certa equação polinomial estão relacionadas umas com as outras. Este foi o ponto de vista original de Évariste Galois.

A abordagem moderna da Teoria de Galois, desenvolvida por Richard Dedekind, Leopold Kronecker e Emil Artin, entre outros, envolve o estudo de automorfismos de extensões de corpos.

Uma abstração além da Teoria de Galois é conseguida pela teoria das conexões de Galois.

O nascimento da teoria de Galois foi originalmente motivado pela seguinte questão, que é conhecida como o teorema de Abel-Ruffini: "Por que não existe uma fórmula para as raízes de uma equação polinomial de quinta ordem (ou maior) em termos de coeficiente de polinômios, usando somente as operações algébricas usuais (adição, subtração, multiplicação, divisão) e aplicação de radicais (raiz quadrada, raiz cúbica, etc)?" A Teoria de Galois não somente provê uma bela resposta para essa questão. Ela também explica em detalhes por que é possível resolver equações de grau 4 ou menores da forma descrita acima e porque suas soluções assumem as formas que têm.

A Teoria de Galois dá uma clara explicação a questões referentes a problemas de construção com régua e compasso. Caracteriza de forma elegante as construções que podem ser executadas com este método.

Não iremos aqui dar um maior aprofundamento quanto à Teoria de Galois, mas iremos estudar conceitos básicos indispensáveis, mais precisamente, destacaremos alguns resultados sobre extensões de corpos através do processo de adjunção de raízes polinômios. Estudaremos principalmente as extensões algébricas do corpo de números racionais.

Nesse sentido apresentamos no primeiro capítulo os conceitos básicos envolvendo anéis; já no segundo capítulo estudaremos os principais conceitos envolvendo extensões de corpos e finalizaremos o terceiro capítulo estudando extensões algébricas dos racionais.



## 1.1. Anéis, ideais e homomorfismos

Neste capítulo apresentamos os conceitos básicos envolvendo estudo dos anéis, os quais são necessários para o desenvolvimento dos capítulos subseqüentes.

**Definição 1.1** *Seja  $A$  um conjunto não vazio onde estejam definidas duas operações, as quais chamaremos de soma e produto em  $A$  e denotaremos por  $+$  e  $\cdot$ .*

*Assim,*

$$\begin{array}{ccc} + : A \times A & \longrightarrow & A \\ (a, b) & \longmapsto & a + b \end{array} \quad e \quad \begin{array}{ccc} \cdot : A \times A & \longrightarrow & A \\ (a, b) & \longmapsto & a \cdot b \end{array}$$

*Chamaremos  $(A, +, \cdot)$  um **anel** se as seguintes propriedades são verificadas quaisquer que sejam  $a, b, c \in A$ :*

i)  $(a + b) + c = a + (b + c)$ ;

ii) *Existe  $0 \in A$  tal que  $a + 0 = 0 + a = a$ ;*

iii) *Para qualquer  $a \in A$  existe um único  $b \in A$ , denotado por  $b = -a$ , tal que  $a + b = b + a = 0$ ;*

iv)  $a + b = b + a$ ;

v)  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ ;

vi)  $a \cdot (b + c) = a \cdot b + a \cdot c$  e  $(a + b) \cdot c = a \cdot c + b \cdot c$ .

*Se um anel  $(A, +, \cdot)$  satisfaz a propriedade:*

vii) *Existe  $1 \in A - \{0\}$ , tal que  $a \cdot 1 = 1 \cdot a = a$ ,  $\forall a \in A$ , dizemos que  $(A, +, \cdot)$  é um **anel com unidade** 1.*

*Se um anel  $(A, +, \cdot)$  satisfaz a propriedade:*

viii) *Para qualquer  $a, b \in A$ , se  $a \cdot b = b \cdot a$ , dizemos que  $(A, +, \cdot)$  é um **anel comutativo**.*

*Se um anel  $(A, +, \cdot)$  satisfaz a propriedade:*

ix) *Dados  $a, b \in A$ ,  $a \cdot b = 0 \Rightarrow a = 0$  ou  $b = 0$ , dizemos que  $(A, +, \cdot)$  é um anel **sem divisores de zero**.*

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

*E finalmente, se um domínio de integridade  $(A, +, \cdot)$  satisfaz a propriedade:*

x) *Para qualquer  $a \in A - \{0\}$ , existe  $b \in A$  tal que  $a \cdot b = b \cdot a = 1$ , dizemos que  $(A, +, \cdot)$  é um **corpo**.*

**Observação 1.1** *Por questão de simplicidade vamos denotar um anel  $(A, +, \cdot)$ , simplesmente por  $A$ , ficando subentendido as operações de soma e produto.*

**Exemplo 1.1** *Os conjuntos  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  e  $n \cdot \mathbb{Z} = \{nk : k \in \mathbb{Z}\}$  munidos da soma e produto usuais são anéis. Já o conjunto  $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$  é um anel munido da soma e produto*

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \quad \cdot : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$

$$(\bar{m}, \bar{n}) \longmapsto \overline{m+n} \quad e \quad (\bar{m}, \bar{n}) \longmapsto \overline{m \cdot n}$$

O conjunto  $\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Z}\}$  com  $p$  primo, são anéis com a soma e produto abaixo

$$(a + b\sqrt{p}) + (c + d\sqrt{p}) = (a + c) + (b + d)\sqrt{p}$$

e

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

com  $a, b, c, d \in \mathbb{Z}$ .

O conjunto  $\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Q}\}$  também é um anel com às operações análogas as operações em  $\mathbb{Z}[\sqrt{p}]$ .

Entre esses anéis, são exemplos de corpos  $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}[\sqrt{p}]$  e  $\mathbb{Z}_p$ , com  $p$  primo.

**Definição 1.2** Seja  $A$  um anel e  $B$  um conjunto não vazio de  $A$ . Dizemos que  $B$  é um **subanel** de  $A$ , se valem:

- i)  $x, y \in B \Rightarrow x - y \in B$ ;
- ii)  $x, y \in B \Rightarrow x \cdot y \in B$ .

**Exemplo 1.2** Temos que  $n\mathbb{Z}$  é subanel de  $\mathbb{Z}$ , por sua vez  $\mathbb{Z}$  é subanel de  $\mathbb{Q}$ , este que é subanel de  $\mathbb{R}$ , já  $\mathbb{R}$  é subanel de  $\mathbb{C}$ . Ademais,  $\mathbb{Z}[\sqrt{p}]$  é subanel de  $\mathbb{Q}[\sqrt{p}]$  e este é subanel de  $\mathbb{R}$ .

**Definição 1.3** Um subanel  $B$  de um corpo  $K$  é chamado um **subcorpo** de  $K$ , se dado  $a \in B - \{0\}$  existe  $b \in B$  tal que  $a \cdot b = 1$ .

**Exemplo 1.3** Observe que  $\mathbb{Q}$  é subcorpo de  $\mathbb{R}$ , já  $\mathbb{R}$  é subcorpo de  $\mathbb{C}$ . Ademais,  $\mathbb{Q}[\sqrt{p}]$  é um subcorpo de  $\mathbb{R}$ .

**Definição 1.4** Seja  $A$  um anel e seja  $I$  um subanel de  $A$ . Dizemos que  $I$  é um **ideal**  $A$  se,  $a \cdot x \in I, \forall a \in A, \forall x \in I$  e  $n \cdot a \in I, \forall a \in A, \forall n \in I$ .

Os subaneis  $\{0\}$  e  $A$  são ideais de  $A$  e são chamados de **ideais triviais** de  $A$ . Os ideais não triviais de  $A$  são chamados de **ideais próprios** de  $A$

**Exemplo 1.4** Seja  $A$  um anel comutativo e  $x_1, x_2, \dots, x_n \in A$ . É de direta verificação que o conjunto definido por

$$A \cdot x_1 + A \cdot x_2 + \dots + A \cdot x_n = \{a_1 \cdot x_1 + a_2 \cdot x_2 + \dots + a_n \cdot x_n ; a_i \in A\}$$

é um ideal de  $A$ , o qual é chamado de **ideal gerado** por  $x_1, x_2, \dots, x_n \in A$ . Os ideais do tipo  $I = A \cdot x_1$  são chamados **ideais principais**.

**Observação 1.2** Um anel em que todos os ideais são principais é chamado **anel principal**. O anel  $\mathbb{Z}$  é um anel principal.

**Observação 1.3** se  $A$  é um anel com unidade  $1$  e  $J$  é um ideal de  $A$  tal que  $1 \in J$ , então  $J = A$ . De fato, primeiro note que  $J \subset A$ , pois  $J$  é ideal de  $A$ . Por outro lado, mostremos que  $A \subset J$ . Reciprocamente, seja  $x \in A$ , como  $J$  é ideal e  $1 \in J$ , então  $x = x \cdot 1 \in J$ . Logo,  $A \subset J$ . Portanto  $A = J$ .

**Definição 1.5** Seja  $A$  um anel e seja  $M$  um ideal de  $A$ . Dizemos que  $M$  é um **ideal maximal** de  $A$  se,  $M \neq A$  e se  $J$  é ideal de  $A$  tal que  $M \subset J \subset A$ , então  $J = M$  ou  $J = A$ .

**Exemplo 1.5** O ideal  $p\mathbb{Z}$  em  $\mathbb{Z}$  com  $p$  primo é maximal. De fato, seja  $p$  primo e  $J = p \cdot \mathbb{Z}$ . Vamos provar que  $J$  é um ideal maximal em  $\mathbb{Z}$ . considere  $I$  um ideal de  $\mathbb{Z}$  tal que,

$$J \subset I \subset \mathbb{Z}$$

pelo fato de todo ideal de  $\mathbb{Z}$  ser principal, temos que existem inteiros  $n$  tais que  $I = n \cdot \mathbb{Z}$ . Assim,  $p \in p \cdot \mathbb{Z} \subset n \cdot \mathbb{Z}$ , e daí segue  $p = n \cdot k$  para algum  $k \in \mathbb{Z}$ , e portanto  $n|p$  e teremos  $n = \pm 1$  ou  $n = \pm p$ . se  $n = \pm 1$  vem que  $I = \mathbb{Z}$  e se  $n = \pm p$  vem que  $I = J$ .

**Teorema 1.1** Seja  $K$  um anel comutativo com unidade  $1 \in K$ . Então as seguintes condições são equivalentes:

- i)  $K$  é um corpo;
- ii)  $\{0\}$  é um ideal maximal em  $K$ ;
- iii) Os únicos ideais de  $K$  são os triviais.

**Demonstração:** i)  $\Rightarrow$  ii). Seja  $K$  um corpo e seja  $J$  um ideal de  $K$  tal que  $\{0\} \subset J \subset K$ . Suponhamos  $J \neq \{0\}$ . Assim existe  $0 \neq a \in J$ . Como  $K$  é um corpo existe  $b \in K$  tal que  $b \cdot a = 1$  e portanto  $1 \in J$  e daí segue imediatamente que  $J = K$ .

ii)  $\Rightarrow$  iii). Segue imediatamente das definições.

iii)  $\Rightarrow$  i). Seja  $0 \neq a \in K$  e  $I = K \cdot a$  o ideal principal de  $K$  gerado por  $a$ . Como  $1 \in K$ , temos  $a = 1 \cdot a \in I$ , nos diz que  $I \neq \{0\}$  e assim pela nossa hipótese, teremos  $I = K$ .

Daí segue,

$$1 \in K = K \cdot a$$

donde existe  $b \in K$  tal que  $1 = b \cdot a$ . ■

**Definição 1.6** Um domínio de integridade  $D$  é dito de **característica 0** se  $ma = 0$  sempre que  $a \in D$ ,  $a \neq 0$  e  $m \in \mathbb{N}$ . Por outro lado,  $D$  diz-se de **característica finita** se existe  $a \in D$ ,  $a \neq 0$ , tal que  $ma = 0$  para algum inteiro  $m \neq 0$ . Nesse caso definimos como a **característica de  $D$**  o menor inteiro positivo  $m$  tal que  $ma = 0$  para alguma  $a \in D$ ,  $a \neq 0$ .

**Exemplo 1.6** Os anéis  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  e  $\mathbb{C}$  tem característica 0, pois se  $m \neq 0$ , então  $m \cdot 1 = m$  e, portanto,  $m \cdot 1 \neq 0$ .

**Exemplo 1.7** Observemos primeiro que em  $\mathbb{Z}_m$ ,  $m \cdot \bar{1} = \bar{1} + \bar{1} + \dots + \bar{1} = \bar{m} = \bar{0}$ . Suponhamos, por outro lado, que para algum inteiro  $r$ ,  $0 < r < m$ , se tivesse  $r \cdot \bar{1} = \bar{0}$ . Como  $r \cdot \bar{1} = \bar{r}$ , então  $\bar{r} = \bar{0}$ , ou seja,  $r \equiv 0 \pmod{m}$ . Então  $m \mid r$ , o que é impossível, uma vez que  $0 < r < m$ . Logo, característica de  $\mathbb{Z}_m = m$ .

Vamos agora definir a seguinte relação em  $A$ . Dados

$$x, y \in A, x \equiv y \pmod{J} \Leftrightarrow x - y \in J.$$

Primeiramente vamos provar que  $\equiv \pmod{J}$  define uma relação de equivalência em  $A$ .

De fato, quaisquer que sejam  $x, y, z \in A$ , temos

i)  $x \equiv x \pmod{J}$  pois  $0 = x - x \in J$ .

ii)  $x \equiv y \pmod{J} \Rightarrow y \equiv x \pmod{J}$  pois se  $x - y \in J$  então  $y - x = -(x - y) \in J$ .

iii)  $x \equiv y \pmod{J}$  e  $y \equiv z \pmod{J} \Rightarrow x \equiv z \pmod{J}$  pois,  $x - y \in J$  e  $y - z \in J \Rightarrow x - z = (x - y) + (y - z) \in J$ .

Denotaremos por  $\bar{x}$  a **classe de equivalência** de  $x \in A$  segundo a relação  $\equiv \pmod{J}$ .

Assim,

$$\bar{x} = \{y \in A : y \equiv x \pmod{J}\}$$

Agora observe que  $y \in \bar{x} \Leftrightarrow y - x \in J$ , e por isso também denotaremos essa classe  $\bar{x}$  por  $\bar{x} = \{x + z : z \in J\}$ . Ademais, chamaremos de **conjunto quociente** de  $A$  pelo ideal  $J$ , ao conjunto  $A/J = \{\bar{x} = x + J : x \in A\}$ .

Definiremos as seguintes operações em  $A/J$

$$+ : A/J \times A/J \longrightarrow A/J \quad \text{e} \quad \cdot : A/J \times A/J \longrightarrow A/J \\ (\bar{a}, \bar{b}) \longmapsto \overline{a+b} \quad (\bar{a}, \bar{b}) \longmapsto \overline{a \cdot b}.$$

Munido destas operações temos que  $A/J$  é um anel, chamado anel quociente.

**Observação 1.4** Se  $A$  tem unidade, então  $A/J$  também tem. De fato, considere  $1$  a unidade de  $A$  e  $x \in A$ . Temos que,

$$1 \cdot x = x \cdot 1 = x, \forall x \in A$$

agora seja  $\bar{x} \in A/J$ , daí,  $\bar{x} = x + J = x \cdot 1 + J = \bar{x} \cdot \bar{1} \in A/J$

**Exemplo 1.8** O anel quociente  $\mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$  com as operações induzidas pela soma e multiplicação de inteiros. Observe que

$$\bar{0} = 0 + 4\mathbb{Z} = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$$

$$\bar{1} = 1 + 4\mathbb{Z} = \{\dots, -11, -7, -3, 1, 5, 9, 13, \dots\}$$

$$\bar{2} = 2 + 4\mathbb{Z} = \{\dots, -10, -6, -2, 2, 6, 10, 14, \dots\}$$

$$\bar{3} = 3 + 4\mathbb{Z} = \{\dots, -9, -5, -1, 3, 7, 11, 15, \dots\}$$

Ademais, ao juntarmos todas estas classes resulta no próprio  $\mathbb{Z}$ .

**Teorema 1.2** Sejam  $A$  um anel comutativo com unidade  $1$  e  $J$  um ideal de  $A$ . Então  $J$  é um ideal maximal de  $A$  se, e somente se,  $A/J$  é um corpo.

**Demonstração:** ( $\Rightarrow$ ) Suponhamos  $J$  ideal maximal de  $A$ , e seja  $\bar{0} \neq \bar{a} \in \bar{A} = A/J$ . Temos que provar que existe  $\bar{b} \in \bar{A}$  tal que  $\bar{a} \cdot \bar{b} = \bar{1}$ . De fato, se  $L = A \cdot a$  ideal principal de  $A$  gerado por  $a$ , temos que:  $J + L = \{x + y : x \in J, y \in L\}$  é um ideal contendo  $J$ , e mais  $\bar{a} \neq \bar{0}$  se e somente se,  $a \notin J$ . Como  $a = 1 \cdot a \in L \subset J + L$  temos que  $J + L$  é um ideal que contém  $J$  e mais  $J + L \neq J$ . Pela maximalidade de  $J$  segue que  $A = J + L$  e daí vem,  $1 \in J + L$  implica que existe  $u \in J, v \in L$  tais que  $1 = u + v$ .

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

( $\Leftarrow$ ) Por outro lado, suponhamos que  $\bar{A} = A/J$  seja um corpo. Assim,  $\bar{0}, \bar{1} \in \bar{A}$  implica que,  $J \neq A$ .

Se  $M \neq J$  é um ideal de  $A$  e  $J \subset M \subset A$ , então teremos que existe  $a \in M, a \notin J$ , ou seja,  $\bar{a} \neq \bar{0}$ , com  $\bar{a} \in \bar{A}$ . Como  $\bar{A}$  é corpo existe  $\bar{b} \in \bar{A}$  tal que  $\bar{a} \cdot \bar{b} = \bar{1}$ , ou ainda,

$$ab \equiv 1 \pmod{J} \Leftrightarrow ab - 1 \in J \Leftrightarrow \exists u \in J$$

tal que  $ab - 1 = u$ , e isto nos diz que,  $1 = ab - u$ . Como  $a \in M$  segue que  $ab \in M$  e como  $u \in J \subset M$  temos também  $u \in M$ . Logo concluímos que  $1 = ab - u \in M$  e imediatamente temos  $M = A$  como queríamos demonstrar. ■

## 1.2. homomorfismos de anéis

Podemos descobrir informações sobre um anel examinando sua interação com outros anéis. Fazemos isto através dos homomorfismos. Um homomorfismo é uma aplicação que preserva as operações soma e produto dos anéis.

Sejam  $A$  e  $B$  dois anéis e sejam  $0$  o elemento neutro de  $A$  e  $0'$  o elemento neutro de  $B$ . Se ambos anéis  $A$  e  $B$  possuem unidade, denotaremos por  $1$  a unidade de  $A$  e por  $1'$  a unidade de  $B$ .

**Definição 1.7** Uma função  $f : A \rightarrow B$  diz-se um **homomorfismo** de  $A$  em  $B$  se satisfaz as seguintes condições:

- i)  $f(x + y) = f(x) + f(y)$ ,  $\forall x, y \in A$ ;
- ii)  $f(x \cdot y) = f(x) \cdot f(y)$ ,  $\forall x, y \in A$ .

**Exemplo 1.9** Sejam  $A$  e  $B$  dois anéis quaisquer. Então  $f : A \rightarrow B$ , dada por  $f(a) = 0$ ,  $a \in A$  é claramente um homomorfismo de anéis. Vejamos, sejam  $a, b \in A$ . Têm-se:

$$f(a + b) = 0 = 0 + 0 = f(a) + f(b)$$

$$f(a \cdot b) = 0 = 0 \cdot 0 = f(a) \cdot f(b)$$

**Teorema 1.3** Sejam  $A$  e  $B$  anéis e  $f : A \rightarrow B$  um homomorfismo. Então:

- i)  $Im f = \{f(a) : a \in A\}$  é um subanel de  $B$ .
- ii)  $ker(f) = \{a \in A : f(a) = 0'\}$  é um ideal de  $A$  e  $f$  é injetiva se, e somente se,  $ker(f) = \{0\}$ ;
- iii) Os anéis  $\frac{A}{ker(f)}$  e  $Im f$  são isomorfos.

**Demonstração:** Vamos demonstrar o item iii), para isso definiremos uma função

$$F : \frac{A}{ker(f)} \longrightarrow Im f$$

$$\bar{a} \longmapsto f(a)$$

Primeiramente, devemos verificar que  $F$  é uma função bem definida, isto é, se  $a_1, a_2 \in A$  são tais que  $\bar{a}_1 = \bar{a}_2$ , então  $f(a_1) = f(a_2)$ . E de fato, se  $\bar{a}_1 = \bar{a}_2$ , então  $a_1 - a_2 \in ker(f)$ , logo  $f(a_1 - a_2) = 0$ ; além disso  $f(a_1 - a_2) = f(a_1) - f(a_2)$ , pois  $f$  é um homomorfismo; portanto,  $f(a_1) = f(a_2)$ .

Agora,  $F$  é uma aplicação sobrejetiva e é um homomorfismo pois, para elementos  $a_1, a_2 \in A$ , temos:

a)  $F(\bar{a}_1 + \bar{a}_2) = F(\overline{a_1 + a_2}) = f(a_1 + a_2)$  pela definição de  $F$ .

por  $f$  ser um homomorfismo vem que  $f(a_1 + a_2) = f(a_1) + f(a_2) = F(\bar{a}_1) + F(\bar{a}_2)$ .

b) Analogamente ao item a) têm-se;

$$F(\bar{a}_1 \cdot \bar{a}_2) = F(\overline{a_1 \cdot a_2}) = f(a_1 \cdot a_2)$$

$$f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2) = F(\bar{a}_1) \cdot F(\bar{a}_2)$$

Por fim, temos que  $ker(F) = \{\bar{a} \in \frac{A}{ker(f)} : f(a) = 0\} = \{\bar{a} \in \frac{A}{ker(f)} : a \in ker(f)\} = \{\bar{0}\}$ . Logo  $F$  é injetiva. ■

### 1.3. Corpo de frações de um domínio

Podemos observar que todos os anéis que estudamos estão dentro de um corpo. Logo podemos formar suas frações, como na relação inteiros e racionais. Mas vamos formalizar melhor isso para casos onde o corpo não é tão evidente.

Neste parágrafo, seguindo a construção do corpo de frações

$$\mathbb{Q} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0 \right\}$$

a partir do domínio  $\mathbb{Z}$ , vamos construir um corpo  $K$  a partir de um dado domínio  $D$ .

Seja  $D$  um domínio de integridade qualquer e seja  $D^* = D - \{0\}$ . Vamos definir uma relação de equivalência no conjunto,

$$\mathcal{A} = D \times D^* = \{(a, b) : a \in D, b \in D^*\}.$$

De fato, se  $(a, b), (c, d) \in \mathcal{A}$  então  $(a, b) \sim (c, d) \Leftrightarrow ad = bc$ , claramente define uma relação de equivalência no conjunto  $\mathcal{A}$ .

Vamos denotar por  $\frac{a}{b}$  (em vez de  $\overline{(a, b)}$ ) a classe de equivalência

$$\frac{a}{b} = \{(x, y) \in \mathcal{A} : xb = ya\}.$$

Assim,

$$\frac{a}{b} = \frac{x}{y} \text{ em } \frac{\mathcal{A}}{\sim} \Leftrightarrow bx = ay \text{ em } D.$$

Agora vamos definir operações  $+$  e  $\cdot$  no conjunto quociente

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

Sejam  $(a, b)$  e  $(c, d) \in D \times D^*$ . Então, definindo a soma e produto abaixo

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

Observe que se  $b, d \in D^*$  então  $b \cdot d \in D^*$  pois  $D$  é um domínio de integridade. Note que as operações são bem definidas.

Vamos denotar por  $a^* = \frac{a}{1}$  onde  $a \in D$  e  $1$  é a unidade de  $D$ , e denotaremos

$$D^* = \left\{ a^* = \frac{a}{1} : a \in D \right\} \subset K = \left\{ \frac{a}{b} : a \in D, b \in D^* \right\}.$$

Observe que  $D^*$  é um domínio de integridade com unidade  $1^* \in D^*$ . Aliás  $1^*$  é tal que, se  $\frac{a}{b} \in K$  então  $\frac{a}{b} \cdot 1^* = 1^* \cdot \frac{a}{b} = \frac{a}{b}$  e mais ainda, qualquer  $\frac{a}{b} \in K$ , temos  $\frac{a}{b} + 0^* = 0^* + \frac{a}{b} = \frac{a}{b}$ . Consideremos agora a seguinte função:

$$\begin{aligned} \varphi : D &\longrightarrow D^* \\ a &\longmapsto a^* \end{aligned}$$

É de imediata verificação que:

a)  $Im \varphi = D^*$ .

b)  $Ker(\varphi) = \{a \in D : a^* = 0^*\} = \{0\}$ .

c)  $\varphi(a+b) = (a+b)^* = a^* + b^* = \varphi(a) + \varphi(b) \forall a, b \in D$ .

d)  $\varphi(a \cdot b) = (a \cdot b)^* = a^* \cdot b^* = \varphi(a) \cdot \varphi(b) \forall a, b \in D$ .

Portanto  $D \simeq D^* \subset K$ . Observe também que, se  $\frac{a}{b} \neq 0^*$  em  $K$ , isto é,  $a \neq 0$  em  $D$ , então  $\frac{b}{a} \in K$  e mais,  $\frac{a}{b} \cdot \frac{b}{a} = 1^*$ . Como  $D \simeq D^* \subset K$  dizemos que  $D$  está imerso em  $K$ . Observe também que  $b^* \cdot \frac{1}{b} = 1^*$  se  $b \neq 0$ ,  $b \in D$ . Assim, denotaremos por  $(b^*)^{-1} = \frac{1}{b}$  se  $b \neq 0$ ,  $b \in D$ . Agora note que:

$$D^* = \{a^*; a \in D\} \subset K = \{a^* \cdot (b^*)^{-1}; a^* \in D^*, b^* \in D^*\}$$

pois, seja  $a^* \in D^*$  e considere  $b^* = 1 \in D^*$ . Observe que  $a^*$  pode ser escrito como:

$$a^* = a^* \cdot 1 = a^* \cdot (1)^{-1}$$

mas  $a^* \cdot (1)^{-1} \in K$ , portanto,

$$D^* = \{a^* : a \in D\} \subset K = \{a^* \cdot (b^*)^{-1} : a^* \in D^*, b^* \in D^*\}$$

com  $b^* \neq 0^*$ . O corpo  $K$  que construímos nesta seção recebe o nome de **corpo de frações do domínio  $D$** .

**Exemplo 1.10**  $\mathbb{Q}$  é o corpo de frações de  $\mathbb{Z}$

**Exemplo 1.11**  $\mathbb{Q}[\sqrt{2}] = \{\frac{m}{n} + \frac{p}{q}\sqrt{2} : m, n, p, q \in \mathbb{Z}\}$  é o corpo de frações de  $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$



## 1.4. Polinômio em uma variável

Polinômios são uma classe importante de funções simples e infinitamente diferenciáveis. Devido à natureza da sua estrutura, os polinômios são muito simples de se avaliar e por consequência são usados extensivamente em análise numérica. Os polinômios, a priori, formam um plano conceitual importante na álgebra, entretanto possuem também uma relevante importância na geometria, quando se deseja calcular expressões que envolvem valores desconhecidos.

**Definição 1.8** *Seja  $K$  um corpo qualquer. Chamaremos de um **polinômio** sobre  $K$  em uma indeterminada  $x$  a uma expressão formal*

$$p(x) = a_0 + a_1x + \dots + a_mx^m + \dots$$

onde  $a_i \in K$ ,  $\forall i \in \mathbb{N}$  e  $\exists n \in \mathbb{N}$  tal que  $a_j = 0$ ,  $\forall j \geq n$ .

Dizemos que dois polinômios

$$p(x) = a_0 + a_1x + \dots + a_mx^m + \dots$$

e

$$q(x) = b_0 + b_1x + \dots + b_kx^k + \dots$$

sobre  $K$  são **iguais** se, e somente se  $a_i = b_i$  em  $K$ ,  $\forall i \in \mathbb{N}$ .

Se  $p(x) = 0 + 0x + \dots + 0x^m + \dots$  indicaremos  $p(x)$  por  $0$  e o chamaremos de polinômio **identicamente nulo** sobre  $K$ . Assim um polinômio  $p(x) = a_0 + a_1x + \dots + a_mx^m + \dots$  sobre  $K$  é identicamente nulo se, e somente se  $a_i = 0 \in K$ ,  $\forall i \in \mathbb{N}$ .

Se  $a \in K$  indicaremos por  $a$  ao polinômio  $p(x) = a_0 + a_1x + \dots + a_nx^n + \dots$  onde  $a_0 = a$ , e  $a_i = 0$ ,  $\forall i \geq 1$ . Chamaremos ao polinômio  $p(x) = a$ ,  $a \in K$  de **polinômio constante**  $a$ .

**Exemplo 1.12** *São exemplos de polinômios constantes no corpo dos reais,*

$$p(x) = 5, f(x) = \sqrt{2}, g(x) = \frac{2}{3}$$

de modo geral,  $p(x) = k$ , com  $k \in \mathbb{R}$ .

Se  $p(x) = a_0 + a_1x + \dots + a_nx^n + \dots$  é tal que  $a_n \neq 0$  e  $a_j = 0$ ,  $\forall j > n$  dizemos que  $n$  é o **grau** do polinômio  $p(x)$  e nesse caso indicaremos  $p(x) = a_0 + a_1x + \dots + a_nx^n + \dots$ , e o **grau** de  $p(x)$  por  $\partial p(x) = n$ .

**Exemplo 1.13** No polinômio  $p(x) = 2x^3 + 4x^2 + 3x + 1$ , note que o termo que possui um maior expoente é  $2x^3$ . Portanto o grau deste polinômio é 3.

Vamos denotar por  $K[x]$  o conjunto de todos os polinômios sobre  $K$ , em uma indeterminada  $x$ . Observe que não está definido o grau do polinômio 0, e  $\partial$  pode ser interpretada como uma função do conjunto de todos os polinômios não nulos no conjunto  $\mathbb{N}$ . Assim,

$$\begin{aligned} \partial : K[x] - \{0\} &\longrightarrow \mathbb{N} \\ p(x) &\longmapsto \partial p(x) = \text{grau de } p(x) \end{aligned}$$

Agora vamos definir soma e produto no conjunto  $K[x]$ . Sejam

$$p(x) = a_0 + a_1x + \dots + a_mx^m + \dots$$

e

$$q(x) = b_0 + b_1x + \dots + b_rx^r + \dots$$

dois elementos do conjunto  $K[x]$ . Definimos

$$p(x) + q(x) = c_1x + \dots + c_kx^k + \dots$$

onde  $c_i = (a_i + b_i) \in K$ , e

$$p(x) \cdot q(x) = c_0 + \dots + c_kx^k + \dots$$

onde  $c_0 = a_0b_0$ ,  $c_1 = a_0b_1 + a_1b_0$ ,  $c_2 = a_0b_2 + a_1b_1 + a_2b_0, \dots$ ,  $c_k = a_0b_k + \dots + a_kb_0$ , com  $k \in \mathbb{N}$ .

Observe que a definição acima de produto provém da regra  $x^m \cdot x^n = x^{m+n}$  e da propriedade distributiva. Convencionam-se também as regras  $x^0 = 1$  e  $x^1 = x$ .

Note que  $K[x]$  é um domínio de integridade, onde o polinômio 0 é o elemento neutro de  $K[x]$  e o polinômio constante 1 é a unidade de  $K[x]$ .

Observe que se identificarmos os elementos  $a \in K$  com os polinômios constantes  $p(x) = a$  podemos pensar em  $K[x]$  contendo o corpo  $K$ .

**Teorema 1.4** (Algoritmo da Divisão) Sejam  $f(x), g(x) \in K[x]$  e  $g(x) \neq 0$ . Então existem únicos  $q(x), r(x) \in K[x]$  tais que:

$$f(x) = q(x) \cdot g(x) + r(x)$$

onde  $r(x) = 0$  ou  $\partial r(x) < \partial g(x)$ .

**Demonstração:** Seja  $f(x) = a_0 + a_1x + \dots + a_nx^n$  e  $g(x) = b_0 + b_1x + \dots + b_mx^m$ , com  $(\partial g(x) = m)$ .

Existência:

Se  $f(x) = 0$  basta tomar  $q(x) = r(x) = 0$ . Suponhamos  $f(x) \neq 0$ . Assim  $\partial f = n$ . Se  $n < m$  basta tomar  $q(x) = 0$  e  $r(x) = f(x)$ . Assim podemos assumir  $n \geq m$ . Agora seja  $f_1(x)$  o polinômio definido por

$$f(x) = a_nb_m^{-1}x^{n-m} \cdot g(x) + f_1(x)$$

observe que  $\partial f_1(x) < \partial f(x)$ . Vamos demonstrar o Teorema por indução sobre  $\partial f = n$ .

Se  $n = 0$ ,  $n \geq m \Rightarrow m = 0$  e portanto  $f(x) = a_0 \neq 0$ ,  $g(x) = b_0 \neq 0$  e teremos,

$$f(x) = a_0b_0^{-1}g(x)$$

e basta tomar  $q(x) = a_0b_0^{-1}$  e  $r(x) = 0$ . Pela igualdade  $f_1(x) = f(x) - a_nb_m^{-1}x^{n-m}g(x)$  e  $\partial f_1(x) < \partial f(x) = n$ . Temos pela hipótese de indução que: existem  $q_1(x)$ ,  $r_1(x)$  tais que:

$$f_1(x) = q_1(x) \cdot g(x) + r_1(x)$$

onde  $r_1(x) = 0$  ou  $\partial r_1(x) < \partial g(x)$ . Daí segue imediatamente que:

$$f(x) = (q_1(x) + a_nb_m^{-1}x^{n-m})g(x) + r_1(x)$$

e portanto tomando  $q(x) = q_1(x) + a_nb_m^{-1}x^{n-m}$  e  $r_1(x) = r(x)$  provamos a existência dos polinômios  $q(x)$  e  $r(x)$  tais que  $f(x) = q(x) \cdot g(x) + r(x)$ , e  $r(x) = 0$  ou  $\partial r(x) < \partial g(x)$ .

Agora vamos provar a unicidade. Sejam  $q_1(x)$ ,  $q_2(x)$ ,  $r_1(x)$  e  $r_2(x)$  tais que:

$$f(x) = q_1(x) \cdot g(x) + r_1(x) = q_2(x) \cdot g(x) + r_2(x)$$

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

Daí segue:

$$(q_1(x) - q_2(x)) \cdot g(x) = r_2(x) - r_1(x).$$

Mas se  $q_1(x) \neq q_2(x)$  o grau do polinômio do lado esquerdo da igualdade acima é maior ou igual ao  $\partial g(x)$  enquanto que o  $\partial(r_2(x) - r_1(x)) < \partial g(x)$  o que é uma contradição. Logo  $q_1(x) = q_2(x)$  e daí segue

$$r_1(x) = f(x) - q_1(x)g(x) = f(x) - q_2(x)g(x) = r_2(x)$$

como queríamos demonstrar. ■

**Teorema 1.5** *Todo ideal de  $K[x]$  é principal.*

**Demonstração:** Seja  $J$  um ideal de  $K[x]$ . Se  $J = \{0\}$  então  $J$  é gerado por 0. Suponhamos que  $J \neq \{0\}$  e escolhamos  $0 \neq p(x) \in J$  tal que  $\partial p(x)$  seja o menor possível. Se  $p(x) = a \neq 0$  então  $1 = a^{-1} \cdot a \in J$  e assim segue imediatamente que  $J = K[x]$  é gerado por  $1 \in K[x]$ . Suponhamos então  $\partial p(x) > 0$ . Como  $p(x) \in J$  claramente temos  $K[x] \cdot p(x) \subset J$ . Agora vamos provar que  $J \subset K[x] \cdot p(x)$ . De fato, seja  $f(x) \in J$ . Pelo algoritmo de Euclides temos que existem  $q(x), r(x) \in K[x]$  tais que  $f(x) = q(x) \cdot p(x) + r(x)$  onde ou  $r(x) = 0$  ou  $\partial r(x) < \partial p(x)$ . Agora, como  $f(x), p(x) \in J$  segue imediatamente que  $r(x) = f(x) - q(x) \cdot p(x) \in J$  e pela minimalidade de nossa escolha do polinômio  $p(x) \in J$  segue que  $r(x) = 0$  e portanto temos  $f(x) = q(x) \cdot p(x) \in K[x] \cdot p(x)$  como queríamos demonstrar. ■

**Definição 1.9** *Sejam  $f(x), g(x)$  polinômios não nulos em  $K[x]$  e seja  $d(x) \in K[x]$  um polinômio mônico tal que  $d(x)$  divide  $f(x)$  e  $g(x)$  e se  $h(x) \in K[x]$  é tal que  $h(x)$  divide  $f(x)$  e  $g(x)$ , então  $h(x)$  divide  $d(x)$ . A este polinômio  $d(x)$  chamamos de **máximo divisor comum** de  $f(x)$  e  $g(x)$ . Se  $d(x) = 1$ , então  $f(x)$  e  $g(x)$  são primos entre si.*

**Teorema 1.6** *(Existência de M.D.C). Sejam*

$$p_1(x), \dots, p_m(x) \in K[x] - \{0\}$$

e seja o ideal  $J = K[x] \cdot p_1(x) + \dots + K[x] \cdot p_m(x)$  de  $K[x]$  gerado pelos polinômios não nulos  $p_1(x), \dots, p_m(x)$ .

Se  $d(x) \in K[x]$  é tal que  $J = K[x] \cdot d(x)$  então são válidas as seguintes propriedades:

i) existem  $r_1(x), \dots, r_m(x) \in K[x]$  tais que

$$d(x) = r_1(x) \cdot p_1(x), \dots, r_m(x) \cdot p_m(x);$$

ii)  $d(x)$  é um divisor comum de  $p_1(x), \dots, p_m(x)$ ;

iii) Se  $h(x)$  é um divisor comum qualquer de  $p_1(x), \dots, p_m(x)$ , então  $h(x)$  é também um divisor de  $d(x)$ .

**Demonstração:** i) sai da igualdade

$$K[x] \cdot d(x) = K[x] \cdot p_1(x), \dots, K[x] \cdot p_m(x).$$

ii) Seja  $i \in \{1, \dots, m\}$  e  $K[x] \cdot d(x) = K[x] \cdot p_1(x), \dots, K[x] \cdot p_m(x)$ . temos que,

$$p_i(x) \in K[x] \cdot p_i(x) \subset K[x] \cdot p_1(x) + \dots + K[x] \cdot p_m(x) = K[x] \cdot d(x)$$

e portanto existe  $r_i(x) \in K[x]$  tal que  $p_i(x) = r_i(x) \cdot d(x)$ , isto é,  $d(x)$  é um divisor de cada  $p_i(x)$ , com  $i = 1, \dots, m$ .

iii) Seja  $h(x)$  um divisor comum em  $K[x]$ , de  $p_1(x), \dots, p_m(x)$ , isto é, existe  $r_i(x) \in K[x]$  tal que  $p_i(x) = r_i(x) \cdot h(x)$ , com  $i = 1, \dots, m$ .

Assim,

$$K[x] \cdot p_i(x) \subset K[x] \cdot h(x), \forall i \in \{1, \dots, m\}$$

e daí segue que,

$$K[x] \cdot d(x) = K[x] \cdot p_1(x), \dots, K[x] \cdot p_m(x) \subset K[x] \cdot h(x),$$

ou seja, existe  $r(x) \in K[x]$  tal que  $d(x) = r(x) \cdot h(x)$  ■

**Definição 1.10** *Seja  $f(x) \in K[x]$  tal que  $\partial f(x) \geq 1$ . Dizemos que  $f(x)$  é um **polinômio irreduzível** sobre  $K$  se toda vez que  $f(x) = g(x) \cdot h(x)$ , com  $g(x), h(x) \in K[x]$  então temos  $g(x) = a$  constante em  $K$  ou  $h(x) = b$  constante em  $K$ . Se  $f(x)$  for não irreduzível sobre  $K$  dizemos que  $f$  é **reduzível** sobre  $K$ .*

**Exemplo 1.14** *O polinômio  $p(x) = x^2 - 2 \in \mathbb{Q}[x]$  é irreduzível em  $\mathbb{Q}[x]$ , porém  $p(x) = x^2 - 2$  é reduzível em  $\mathbb{R}[x]$ , pois,*

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

**Exemplo 1.15** *O polinômio  $p(x) = x^2 + 1$  é irreduzível em  $\mathbb{R}[x]$ , mas é reduzível em  $\mathbb{C}[x]$*

**Teorema 1.7** *Sejam  $K$  um corpo e  $p(x) \in K[x]$ . As seguintes condições são equivalentes:*

- i)  $p(x)$  é irreduzível sobre  $K$ .
- ii)  $J = K[x] \cdot p(x)$  é um ideal maximal em  $K[x]$ .
- iii)  $\frac{K[x]}{J}$  é um corpo, onde  $J = K[x] \cdot p(x)$ .

**Demonstração:** Vamos mostrar que  $i) \iff ii)$ .

$i) \implies ii)$ : Suponhamos  $p(x) \in K[x]$ , com  $p(x)$  irreduzível sobre  $K$  e seja  $J = K[x] \cdot p(x) = \{g(x) \cdot p(x); g(x) \in K[x]\}$ . Como grau  $p(x) \geq 1$  temos imediatamente que  $J \neq K[x]$ . Se  $I = K[x] \cdot h(x)$  é um ideal de  $K[x]$  tal que  $I \supset J$  vamos provar que  $I = J$  ou  $I = K[x]$ . Assim,  $p(x) \in K[x] \cdot p(x) \subset K[x] \cdot h(x)$  nos diz que,  $p(x) = g(x) \cdot h(x)$  para algum  $g(x) \in K[x]$ . Como  $p(x)$  é irreduzível temos que  $g(x) = a \in K - \{0\}$  constante ou  $h(x) = b \in K - \{0\}$  constante. Se  $g(x) = a \neq 0$  constante temos que  $h(x) = a^{-1} \cdot p(x)$  e portanto  $I = K[x] \cdot h(x) \subset K[x] \cdot p(x) = J$  e isto nos dá  $I = J$ . Se  $h(x) = b \neq 0$  constante temos  $I = K[x] \cdot h(x) = K[x]$  e isto termina a implicação  $i) \implies ii)$ .

$ii) \implies i)$ : Seja  $J = K[x] \cdot p(x)$  um ideal maximal em  $K[x]$ . Assim  $J \neq K[x]$  nos diz que  $\partial p(x) \geq 1$ . Suponhamos  $g(x), h(x) \in K[x]$  e  $p(x) = g(x) \cdot h(x)$ . Assim segue imediatamente

que  $J \subset I = K[x] \cdot h(x)$  e como  $J$  é maximal temos que  $J = I$  ou  $I = K[x]$ . Se  $J = I$  segue que  $h(x) \in J = K[x] \cdot p(x)$  e isto nos diz que  $h(x) = f(x) \cdot p(x)$  para algum  $f(x) \in K[x]$ . Daí segue que  $p(x) = g(x) \cdot f(x) \cdot p(x)$ . Como  $p(x) \neq 0$  e  $K[x]$  é um domínio de integridade teremos  $1 = g(x) \cdot f(x)$ , isto é,  $g(x) \in K[x]$  é um polinômio invertível em  $K[x]$ . Portanto temos imediatamente que  $g(x) = a \neq 0$  é um polinômio constante. Se  $I = K[x]$  segue imediatamente que  $h(x) = b \neq 0$  constante ou seja  $p(x)$  é irredutível sobre  $K$  como queríamos demonstrar. ■

**Teorema 1.8** *Seja  $K$  um corpo então todo polinômio  $f(x) \in K[x] - \{0\}$  pode ser escrito na forma,*

$$f(x) = u \cdot p_1(x) \dots p_m(x)$$

onde  $u \in K - \{0\}$  e  $p_1(x), p_2(x), \dots, p_m(x)$  são polinômios irredutíveis sobre  $K$  (não necessariamente distintos). Mais ainda, essa expressão é única a menos da constante  $u$  e da ordem dos polinômios  $p_1(x), \dots, p_m(x)$ .

**Demonstração:** Seja  $f(x) \in K[x] - \{0\}$ . Vamos provar por indução sobre o  $\partial f(x) = n$ . Se  $n = 0$ ,  $f(x) = u$  constante não nula. Assim podemos assumir  $\partial f(x) = n \geq 1$ . Vamos supor pela hipótese de indução que todo polinômio não nulo de grau menor que  $n$  pode ser escrito na expressão desejada e vamos demonstrar que  $f(x)$  também pode ser escrito naquela expressão.

Suponhamos, por absurdo, que  $f(x)$  não possa ser escrito como produto de irredutíveis. Então  $f(x)$  é um polinômio irredutível sobre  $K$ . Assim, existem

$$g(x), h(x) \in K[x], 1 \leq \partial g(x) < n, 1 \leq \partial h(x) < n$$

tais que

$$f(x) = g(x)h(x)$$

Agora, por indução temos,

$$g(x) = a \cdot p_1(x) \dots p_r(x), a \in K - \{0\} \text{ e } p_1(x), \dots, p_r(x)$$

polinômios irredutíveis sobre  $K$ . Analogamente,

$$h_1(x) = b \cdot p_{r+1}(x) \dots p_m(x), b \in K - \{0\} \text{ e } p_{r+1}(x), \dots, p_m(x)$$

polinômios irredutíveis sobre  $K$ . Assim

$$f(x) = up_1(x) \dots p_m(x) = u'q_1(x) \dots q_s(x)$$

onde  $u, u' \in k - \{0\}$  e  $p_1(x), \dots, p_m(x), q_1(x) \dots q_s(x)$  são polinômios irredutíveis sobre  $K$ . Assim temos,

$$p_1(x) \mid q_1(x) \dots q_s(x)$$

e daí segue que existe  $u'_i \in K - \{0\}$  tal que  $q_i(x) = u'_i \cdot p_1(x)$  (nesse caso dizemos que  $q_i(x)$  e  $p_1(x)$  são associados em  $K[x]$ ). Agora o Teorema segue por indução sobre  $m$ .

Se  $m = 1$  e  $p_1(x)$  irredutível temos que necessariamente  $s = 1$  e  $p_1(x)$  e  $q_1(x)$  são associados em  $K[x]$ .

Suponhamos  $m > 1$ . De  $q_i(x) = u'_i \cdot p_1(x)$  e sendo  $K[x]$  um domínio temos que:

$$u \cdot p_2(x) \dots p_m(x) = u' \cdot u_i \cdot q_1(x) \dots p_{i-1}(x) \cdot p_{i+1}(x) \dots p_s(x)$$

e daí segue pela hipótese de indução que  $m - 1 = s - 1$  (isto é,  $m = s$ ) e mais, cada  $q_j(x)$  está associado com algum  $p_i(x)$  através de uma constante, e isto termina a demonstração. ■

**Proposição 1.1** (Gauss). *Seja  $f(x) \in \mathbb{Z}[x]$  tal que  $f(x)$  é irredutível sobre  $\mathbb{Z}$  então  $f(x)$  é irredutível sobre  $\mathbb{Q}$ .*

**Demonstração:** Suponhamos que  $f(x)$  seja irredutível sobre  $\mathbb{Z}$ , mas  $f(x) = g(x) \cdot h(x)$ , onde  $g(x), h(x) \in \mathbb{Q}[x]$  e  $1 \leq \partial g(x), \partial h(x) < \partial f(x)$ . Claramente existe inteiro positivo  $m$  tal que  $m \cdot f(x) = g_1(x) \cdot h_1(x)$  onde  $g_1(x), h_1(x) \in \mathbb{Z}[x]$ .

Assim temos,

$$g_1(x) = a_0 + a_1x + \dots + a_r x^r, \quad a_i \in \mathbb{Z}.$$

$$h_1(x) = b_0 + b_1x + \dots + b_s x^s, \quad b_j \in \mathbb{Z}.$$

suponhamos agora que  $p \mid m$ , com  $p$  primo. Vamos provar que  $p \mid a_i \forall i \in \{1, \dots, r\}$  ou  $p \mid b_j \forall j \in \{1, \dots, s\}$ .

De fato, se existe  $i \in \{1, \dots, r\}$  e existe  $j \in \{1, \dots, s\}$  tais que  $p \nmid a_i$  e  $p \nmid b_j$  consideremos  $i$  e  $j$  menores possíveis com esta propriedade. Ora, como  $p \mid m$  temos que  $p$  divide o coeficiente de  $x^{i+j}$  do polinômio  $m \cdot f(x) = g_1(x) \cdot h_1(x)$ , isto é,

$$p \mid (b_0 a_{i+j} + b_1 a_{i+j-1} + \dots + b_j a_i + \dots + b_{i+j-1} a_1 + b_{i+j} a_0)$$

Pela nossa escolha de  $i$  e  $j$  temos que  $p$  divide cada parcela, exceto  $b_j a_i$ , do coeficiente de  $x^{i+j}$  de  $g_1(x) \cdot h_1(x)$ . Como  $p$  divide toda a expressão segue também que  $p \mid b_j a_i$  e como  $p$  é um número primo temos que  $p \mid b_j$  ou  $p \mid a_i$  que é uma contradição.

Assim, se  $p$  primo,  $p \mid m \Rightarrow p \mid a_i \forall i \in \{1, \dots, r\}$  ou  $p \mid b_j \forall j \in \{1, \dots, s\}$ . Sem perda de generalidade, suponhamos que  $p \mid a_i \forall i \in \{1, \dots, r\}$ . Assim,  $g_1(x) = p \cdot g_2(x)$  onde  $g_2(x) \in \mathbb{Z}[x]$ ,

e se  $m = p \cdot m_1$  temos

$$p \cdot m_1 f(x) = p \cdot g_2(x) \cdot h_1(x)$$

$$m_1 f(x) = g_2(x) \cdot h_1(x)$$

como o número de fatores primo de  $m$  é finito, prosseguindo no argumento acima (ou por indução sobre o número de fatores primos de  $m$ ) chegamos que:

$$f(x) = g^*(x) \cdot h^*(x)$$

onde,

$$g^*(x) \cdot h^*(x) \in \mathbb{Z}[x]$$

e  $g^*(x)$  e  $h^*(x)$  são múltiplos racionais de  $g(x)$  e  $h(x)$ , respectivamente, contradizendo a irreduzibilidade de  $f(x)$  sobre  $\mathbb{Z}$ . ■

**Teorema 1.9** (*Critério de Eisenstein*) *Seja  $f(x) = a_0 + a_1x + \dots + a_nx^n$  um polinômio em  $\mathbb{Z}[x]$ . Suponhamos que exista um inteiro primo  $p$  tal que:*

i)  $p \nmid a_n$

ii)  $p \mid a_0, a_1, a_{n-1}$

iii)  $p^2 \nmid a_0$ .

Então  $f(x)$  é irreduzível sobre  $\mathbb{Q}$ .

**Demonstração:** Pela Proposição anterior é suficiente provar que  $f(x)$  é irreduzível sobre  $\mathbb{Z}$ . Suponhamos por contradição que,

$$f(x) = g(x) \cdot h(x), \quad g(x), h(x) \in \mathbb{Z}[x]$$

e

$$1 \leq \partial g(x), \partial h(x) < \partial f(x) = n$$

seja,

$$g(x) = b_0 + b_1x + \dots + b_r x^r \in \mathbb{Z}[x], \quad \partial g(x) = r$$

$$h(x) = c_0 + c_1x + \dots + c_s x^s \in \mathbb{Z}[x], \quad \partial h(x) = s$$

Assim  $n = r + s$ .

Agora  $b_0 \cdot c_0 = a_0$  e assim  $p \mid b_0$  ou  $p \mid c_0$  e como  $p^2 \nmid a_0$  segue que  $p$  divide apenas um dos inteiros  $b_0, c_0$ . Vamos admitir, sem perda de generalidade, que  $p \mid b_0$  e  $p^2 \nmid c_0$ .

Agora  $a_n = b_r \cdot c_s$  é o coeficiente de  $x^n = x^{r+s}$  e portanto  $p \nmid b_r$  e  $p \mid b_0$ . Seja  $b_i$  o primeiro coeficiente de  $g(x)$  tal que  $p \nmid b_i$ .



Agora  $a_i = b_0 \cdot c_i + b_1 \cdot c_{i-1} + \dots + b_i \cdot c_0$  e portanto como  $p|b_0, \dots, b_{i-1}$ ,  $p \nmid b_i$  e  $p \nmid c_0 \Rightarrow p \nmid a_i \Rightarrow i = n$  o que é um absurdo pois  $1 \leq i \leq r < n$ . ■

Para finalizar este capítulo vamos definir corpo algebricamente fechado. Seja  $K$  um corpo. Dizemos que  $K$  é **algebricamente fechado** se qualquer  $f(x) \in K[x]$ , existe  $\alpha \in K$  tal que  $f(\alpha) = 0$ . Por exemplo o corpo dos complexos  $\mathbb{C}$  é algebricamente fechado, enquanto o corpo dos reais  $\mathbb{R}$  não é algebricamente fechado.

**Exemplo 1.16** Considere o polinômio  $p(x) = x^2 + 1$ , note que não existe nenhum valor em  $\mathbb{R}$  que torne possível a igualdade,

$$x^2 + 1 = 0$$

Por isso dizemos que  $\mathbb{R}$  não é algebricamente fechado. O mesmo não ocorre em  $\mathbb{C}$

## 2 Introdução à extensão de corpos

Neste capítulo vamos estabelecer alguns conceitos básicos envolvendo extensões de corpos, os quais são fundamentais para o entendimento do próximo capítulo.

**Definição 2.1** Um corpo  $L$  é dito uma **extensão de um corpo**  $K$ , se  $K$  for subcorpo de  $L$  e denotamos por  $L \supset K$ .

**Exemplo 2.1** O corpo  $\mathbb{R}$  é uma extensão do corpo  $\mathbb{Q}$ , por sua vez  $\mathbb{C}$  é extensão de  $\mathbb{R}$  e de  $\mathbb{Q}$ .

**Definição 2.2** Sejam  $L$  uma extensão de  $K$  e  $\alpha \in L$ . Dizemos que  $\alpha$  é **algébrico sobre**  $K$  se existe  $f(x) \in K[x] - \{0\}$  tal que  $f(\alpha) = 0$ . Caso o contrário dizemos que  $\alpha$  é **transcendente sobre**  $K$ .

**Definição 2.3** Sejam  $L$  uma extensão de  $K$ . Dizemos que  $L$  é uma **extensão algébrica** de  $K$  se todo  $\alpha \in L$  é algébrico sobre  $K$ .

**Exemplo 2.2** O corpo  $\mathbb{R}$  é uma extensão do corpo  $\mathbb{Q}$ . Desde que  $\sqrt{2}$  é uma raiz do polinômio  $f(x) = x^2 - 2$ , temos que  $\sqrt{2}$  é algébrico sobre  $\mathbb{Q}$ . Note que  $i \in \mathbb{C}$  é algébrico sobre  $\mathbb{Q}$  pois é raiz de  $p(x) = x^2 + 1$ .

**Exemplo 2.3** O corpo  $\mathbb{R}$  é uma extensão do corpo  $\mathbb{Q}$ . O número real  $\pi$  é transcendente sobre  $\mathbb{Q}$ , uma vez que,  $\pi$  não é raiz de nenhum polinômio em  $\mathbb{Q}[x]$ . Por outro lado,  $\pi$  é algébrico em  $\mathbb{R}$  pois é raiz do polinômio  $f(x) = x - \pi \in \mathbb{R}[x]$ .

**Proposição 2.1** Se  $\alpha \in K$ , então  $\alpha$  é algébrico sobre  $K$ .

**Demonstração:** Basta tomar  $f(x) = x - \alpha \in K[x]$  e temos que  $f(\alpha) = \alpha - \alpha = 0$ . Logo  $\alpha$  é algébrico sobre  $K$ . ■

Seja  $\alpha \in L$  algébrico sobre  $K$  e seja  $p(x) \in K[x]$ , mônico e de menor grau tal que  $p(\alpha) = 0$ . Pela minimalidade do grau de  $p(x)$  segue que  $p(x)$  é o único polinômio mônico irredutível em  $K[x]$  tal que  $p(\alpha) = 0$ , o qual será denotado aqui por  $p(x) = \text{irr}(\alpha, K)$ .

De fato, seja  $p(x) \in K[x]$ , pelo algoritmo da divisão existem  $g(x), r(x) \in K[x]$ , tais que,

$$p(x) = f(x)g(x) + r(x), \quad r(x) = 0 \text{ ou } \partial r(x) \leq \partial g(x),$$

como  $\alpha$  é raiz de  $p(x)$  temos,

$$\begin{aligned} 0 &= p(\alpha) = f(\alpha)g(\alpha) + r(\alpha) \\ \Rightarrow r(\alpha) &= p(\alpha) - f(\alpha)g(\alpha) = 0 \\ \Rightarrow r(\alpha) &= 0. \end{aligned}$$

Mas  $p(x)$  é o menor polinômio tal que aplicando  $\alpha$  resulta em 0, assim,  $r(x) = 0$ , daí,

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

Como  $p(x)$  é mônico, isto significa que o coeficiente do termo de maior grau é 1, logo  $f(x) = 1$  ou  $g(x) = 1$ , constante. E portanto  $p(x)$  é irredutível em  $K[x]$ . E  $p(x)$  é único, pois suponha que exista  $q(x) \in K[x]$  tal que,

$$q(\alpha) = 0,$$

note que,

$$q(\alpha) = 0 = p(\alpha) \Rightarrow q(\alpha) = p(\alpha),$$

como  $q(x)$  e  $p(x)$  são mônicos e de menor grau, segue que,

$$q(x) = p(x).$$

**Observação 2.1** Se  $\alpha \in L \supset K$  definimos  $K[\alpha] = \{f(\alpha) : f(x) \in K[x]\}$ . Ademais,  $K[\alpha]$  é um subdomínio de  $L$  que contém  $K$ .

**Exemplo 2.4** Sejam  $\mathbb{R} \supset \mathbb{Q}$  e  $\alpha = \sqrt{2} \in \mathbb{R}$  vamos mostrar que

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

De fato, por definição temos que,

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

Agora, se  $f(x) \in \mathbb{Q}[x]$ , segue pelo algoritmo da divisão que existem  $q(x)$  e  $r(x) \in \mathbb{Q}[x]$  tais que,

$$f(x) = q(x)(x^2 - 2) + r(x), \quad r(x) = a + bx$$

para  $x = \sqrt{2}$  temos que,

$$f(\sqrt{2}) = q(\sqrt{2})(2 - 2) + r(\sqrt{2}),$$

$$f(\sqrt{2}) = q(\sqrt{2})0 + r(\sqrt{2}),$$

$$f(\sqrt{2}) = 0 + r(\sqrt{2}),$$

$$f(\sqrt{2}) = r(\sqrt{2}).$$

Como  $r(x)$  é da forma,  $r(x) = a + bx$ , temos

$$f(\sqrt{2}) = r(\sqrt{2}) = a + b\sqrt{2}$$

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

**Exemplo 2.5** Sejam  $\mathbb{R} \supset \mathbb{Q}$  e  $\alpha = \sqrt[3]{2} \in \mathbb{R}$ . vamos mostrar que

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

Por definição,

$$\mathbb{Q}[\sqrt[3]{2}] = \{f(\sqrt[3]{2}) : f(x) \in \mathbb{Q}[x]\}$$

Pelo algoritmo da divisão temos que existe  $q(x)$  e  $r(x) \in \mathbb{Q}[x]$  tais que,

$$f(x) = q(x)(x^3 - 2) + r(x), \quad r(x) = a + bx + cx^2$$

para  $x = \sqrt[3]{2}$ .

$$f(\sqrt[3]{2}) = r(\sqrt[3]{2});$$

como  $r(x)$  é da forma  $r(x) = a + bx + cx^2$ , temos

$$f(\sqrt[3]{2}) = r(\sqrt[3]{2}) = a + b(\sqrt[3]{2}) + c(\sqrt[3]{2})^2,$$

com  $a, b, c \in \mathbb{Q}$ .

**Observação 2.2** De modo geral, seja  $\alpha = \sqrt[n]{p} \in \mathbb{R}$ ,  $n$  inteiro maior ou igual a 2 e  $p$  maior ou igual a 2 um número primo. Então  $\alpha$  é uma raiz real do polinômio  $x^n - p$  que é, pelo critério de Einsenstein, irredutível sobre  $\mathbb{Q}$ . Assim  $x^n - p = \text{irr}(\alpha, \mathbb{Q})$  e temos,  $\mathbb{Q}[\alpha]$  é um subcorpo de  $\mathbb{R}$  contendo  $\mathbb{Q}$  e mais ainda,

$$\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}; a_i \in \mathbb{Q}, i = 0, \dots, n-1\}.$$

**Observação 2.3** Os conceitos básicos de Álgebra Linear como os de espaço vetorial, base e dimensão que serão mencionados a seguir, estão como Apêndice no final deste trabalho.

Seja  $L$  uma extensão de  $K$ , considere a soma de  $L$  e o produto por escalar

$$\begin{aligned} + : L \times L &\longrightarrow L & \cdot : K \times L &\longrightarrow L \\ (\alpha, \beta) &\longmapsto \alpha + \beta & (\alpha, x) &\longmapsto \alpha x \end{aligned}$$

Temos que  $L$  munido dessa soma e desse produto por escalar é um  $K$ -espaço vetorial. Assim, sendo  $L$  uma extensão de  $K$ , a dimensão de  $L$  visto como  $K$ -espaço vetorial é chamada de **grau da extensão**  $L$  sobre  $K$  e denotamos por  $[L : K]$ .

Uma extensão  $L$  de  $K$  é dita **extensão finita** se tem grau finito. Caso contrário, dizemos  $L \supset K$  é **extensão infinita**.

**Exemplo 2.6**  $\mathbb{R}$  é uma extensão de  $\mathbb{Q}$  de grau infinito. ( $\pi$  é transcendente).

**Exemplo 2.7** O corpo  $\mathbb{C}$  visto como espaço vetorial sobre  $\mathbb{R}$  tem dimensão 2, pois  $\{1, i\}$  é base desse espaço vetorial. Assim,  $\mathbb{C}$  é uma extensão de grau 2 sobre  $\mathbb{R}$ , ou seja,  $[\mathbb{C} : \mathbb{R}] = 2$ .

### 3 Extensões Algébricas dos Racionais

Neste capítulo vamos construir corpos  $K$ , tais que  $\mathbb{Q} \subset K \subset \mathbb{C}$ . Para isso vamos usar o processo chamado adjunção de raízes de um polinômio. Ademais, vamos apresentar alguns resultados que são muito importantes no desenvolvimento da Teoria de Galóis.

#### 3.1. Adjunção de Raízes

**Teorema 3.1** *Se  $\alpha \in L \supset K$  e se  $\Psi : K[x] \rightarrow L$  é definida por  $\Psi(f(x)) = f(\alpha)$ , então  $\Psi$  é um homomorfismo tal que:*

- i)  $Im \Psi = K[\alpha]$ ,  $K \subset K[\alpha] \subset L$ ;*
- ii)  $\alpha$  é transcendente sobre  $K$  se, e somente se,  $ker(\Psi) = \{0\}$ ;*
- iii) Se  $\alpha$  é algébrico sobre  $K$  e  $p(x) = irr(\alpha, K)$ , então  $ker(\Psi) = K[x] \cdot p(x)$  é um ideal maximal de  $K[x]$ ;*
- iv)  $K[x]/ker(\Psi) \simeq K[\alpha]$ .*

**Demonstração:** Primeiro mostraremos que  $\Psi$  é um homomorfismo, para isso, considere  $f(x), g(x) \in K[x]$ , temos

$$\begin{aligned}\Psi(f(x) + g(x)) &= \Psi((f + g)(x)) = (f + g)(\alpha) = f(\alpha) + g(\alpha) = \Psi(f(x)) + \Psi(g(x)) \\ \Psi(f(x) \cdot g(x)) &= \Psi((f \cdot g)(x)) = (f \cdot g)(\alpha) = f(\alpha) \cdot g(\alpha) = \Psi(f(x)) \cdot \Psi(g(x))\end{aligned}$$

Portanto  $\Psi$  é homomorfismo.

Agora mostraremos os itens de (i) à (iv).

i) Temos que

$$Im \Psi = \{f(\alpha) : f(x) \in K[x]\}$$

mas  $\Psi$  está definida em  $K[x]$ , de modo que todo  $f(x) \in K[x]$ . Daí,

$$Im \Psi = \{f(\alpha) : f(x) \in K[x]\}$$

e por definição, isto é  $K[\alpha]$ . Logo,  $Im \Psi = K[\alpha]$ . Para verificar que  $K[\alpha]$  contém  $K$  basta tomar a função  $g(\alpha_i) = a_i$ ,  $a_i \in K$ ,  $i = 1, 2, \dots$

ii) Seja

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

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

$$\Psi(f(x)) \neq 0.$$

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

$$\Psi(f(x)) = f(\alpha) \neq 0.$$

Deste modo,  $\alpha$  é transcendente sobre  $K$ .

iii) Como  $\alpha$  é algébrico sobre  $K$ , então  $ker(\Psi) \neq \{0\}$ . Considere então  $ker(\Psi) = K[x] \cdot p(x)$  um ideal em  $K[x]$ . Como  $p(x)$  é irredutível sobre  $K$ , pelo Teorema 1.7 temos que  $ker(\Psi) = K[x] \cdot p(x)$  é um ideal maximal em  $K[x]$

iv) Segue pelo item i) deste Teorema que  $Im\Psi = K[\alpha]$  e agora é imediato do Teorema 1.3 item (iii) que

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

■

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

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

ii) *Se  $\alpha$  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) Tomemos um homomorfismo nas condições do Teorema 3.1, ou seja,  $\Psi : K[x] \rightarrow L$  definido por  $\Psi(f(x)) = f(\alpha)$ . Suponha que  $\alpha$  é algébrico sobre  $K$  e seja  $p(x) = irr(\alpha, K) \in K[x]$ . Pelo item (iii) do Teorema 3.1 temos que  $ker(\Psi) = K[x] \cdot p(x)$  é um ideal maximal e portanto

$$\frac{K[x]}{ker(\Psi)},$$

é um corpo. Agora pelo item (iv) do Teorema 3.1 temos

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

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

ii) Para provar que  $K[\alpha]$  é um subdomínio de  $L$  precisamos mostrar que  $K[\alpha]$  é subanel e que não possui divisores de zero.

Vamos primeiro mostrar que  $K[\alpha]$  é subanel, para isto, considere  $f(\alpha), g(\alpha) \in K[\alpha]$ .

Note que,

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

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

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

$$f(\alpha) \cdot g(\alpha) = 0 \Rightarrow f(\alpha) = 0 \text{ ou } g(\alpha) = 0$$

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

$$f(\alpha) = 0(\alpha) \text{ ou } g(\alpha) = 0(\alpha)$$

■

**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,  $p(x) = \text{irr}(\alpha, K) = \text{irr}(\beta, K)$ . Agora, pelo item (iii) do Teorema 3.1, obtemos

$$J = K[x] \cdot p(x),$$

e por (iv) temos  $K[\alpha] \simeq \frac{K[x]}{J}$  e da mesma forma  $\frac{K[x]}{J} \simeq K[\beta]$ . Logo

$$K[\alpha] \simeq K[\beta].$$

são corpos isomorfos.

■

**Proposição 3.1** *Seja  $L$  uma extensão de  $K$  e  $\alpha \in L$  algébrico sobre  $K$ . Se o grau do polinômio  $\text{irr}(\alpha, K)$  é  $n$ , então:*

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

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

ii)  $K[\alpha] = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}; a_i \in K\}$  *é um subcorpo de  $L$  que contém  $K$ .*

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

**Demonstração:** Seja  $p(x) = \text{irr}(\alpha, K)$ . Por hipótese,  $\partial p(x) = n$ .

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

$$f(x) = q(x) \cdot p(x) + r(x), \text{ onde } r(x) = 0 \text{ ou } \partial r(x) < \partial p(x).$$



Assim  $r(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$  onde  $a_i \in K$ ,  $i = 0, 1, \dots, n-1$ .

Agora temos,

$$f(\alpha) = q(\alpha) \cdot p(\alpha) + r(\alpha)$$

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

Para demonstrar a unicidade da expressão temos

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

segue imediatamente que o polinômio  $q(x) \in K[x]$  onde

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

é tal que  $q(\alpha) = 0$  e  $\partial q(x) < n = \partial \text{irr}(\alpha, K)$  Assim  $q(x) = 0$  e daí segue

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

ii) Primeiro vamos mostrar que  $K[\alpha] = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} : a_i \in K\}$ . 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  $f(\alpha) = a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}$ , onde  $a_i \in K$ , daí temos

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

o fato de  $K[\alpha]$  ser um subcorpo de  $L$  que contém  $K$  segue diretamente do item i) do Corolário 3.1

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

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

Assim existe uma correspondência bijetiva entre  $\mathbb{Z}_p[\alpha]$  e o conjunto de todas as n-uplas  $(a_0, a_1, a_{n-1})$  onde cada  $a_i \in \mathbb{Z}_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$ . ■

**Exemplo 3.1** Considerando a Observação 2.2 por exemplo,

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] = \{a_0 + a_1\sqrt{2} : a_0, a_1 \in \mathbb{Q}\} \subset \mathbb{R}$$

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}] = \{a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 : a_0, a_1, a_2 \in \mathbb{Q}\} \subset \mathbb{R}$$

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt[4]{3}] = \{a_0 + a_1\sqrt[4]{3} + a_2(\sqrt[4]{3})^2 + a_3(\sqrt[4]{3})^3 : a_0, a_1, a_2, a_3 \in \mathbb{Q}\} \subset \mathbb{R}$$

Agora se  $\beta$  é uma raiz cúbica complexa de 2 e  $\beta \notin \mathbb{R}$ , temos que,

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

Mais ainda, pelo Corolário 3.2  $\mathbb{Q}[\sqrt[3]{2}] \simeq \mathbb{Q}[\beta]$  pois  $\sqrt[3]{2} \in \mathbb{R}$  e  $\beta \in \mathbb{C}$  são raízes do mesmo polinômio irredutível  $x^3 - 2$  sobre  $\mathbb{Q}$ .

### 3.2. Corpo de decomposição de um polinômio

Considere  $K$  um subcorpo de  $\mathbb{C}$ . Vamos também pensar em  $\mathbb{C}$  como um corpo algebricamente fechado, ou seja, qualquer  $f(x) \in \mathbb{C}[x]$  existe  $\alpha \in \mathbb{C}$  tal que  $f(\alpha) = 0$ . Assim, se  $f(x) \in K[x]$  é um polinômio de grau  $n \geq 1$  e  $\alpha_1, \alpha_2, \dots, \alpha_r$  são todas as distintas raízes de  $f(x)$  em  $\mathbb{C}$  temos que,

$$f(x) = c \cdot (x - \alpha_1)^{m_1} \dots (x - \alpha_r)^{m_r}$$

em  $\mathbb{C}[x]$  onde  $c \in K$  e  $r, m_1, \dots, m_r$  são inteiros positivos.

O inteiro  $m_i$  chama-se **multiplicidade** da raiz  $\alpha_i$ . Se  $m_i = 1$  dizemos que  $\alpha_i$  é uma raiz **simples** de  $f(x)$ . Se  $f(x) = a_0 + a_1x + \dots + a_nx^n \in K[x]$  definimos  $f'(x) = a_1 + 2a_2x + \dots + na_nx^{n-1} \in K[x]$  o qual chamamos de **derivada** de  $f(x)$ . Observe que se  $\partial f(x) = n \geq 1$  então  $f'(x) \neq 0$  e  $\partial f'(x) = n - 1$ .

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

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

$$(a \cdot f(x))' = a \cdot f'(x)$$

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

**Proposição 3.2** *Sejam  $f(x) \in K[x]$ ,  $\partial f(x) = n \geq 1$  e  $\alpha \in \mathbb{C}$  é uma raiz de  $f(x)$ . Então:*

i)  $\alpha$  é raiz simples de  $f(x)$  se, e somente se,  $f(\alpha) = 0$  e  $f'(\alpha) \neq 0$ .

ii) Se  $f(x)$  é irredutível sobre  $K$  então todas as raízes de  $f(x)$  são simples.

**Demonstração:** i) Se  $\alpha \in \mathbb{C}$  é uma raiz de  $f(x)$ , com multiplicidade  $m \geq 1$  temos que  $f(x)$  pode ser fatorado em  $\mathbb{C}[x]$  como,  $f(x) = (x - \alpha)^m \cdot g(x)$ , onde  $g(x) \in \mathbb{C}[x]$  e  $g(\alpha) \neq 0$ .

$$f'(x) = m(x - \alpha)^{m-1} \cdot g(x) + (x - \alpha)^m \cdot g'(x)$$

Assim para  $m = 1$ , temos que

$$f(x) = (x - \alpha)g(x) \Rightarrow f(\alpha) = (\alpha - \alpha)g(\alpha) \Rightarrow f(\alpha) = 0 \cdot g(\alpha) = 0.$$

Agora usando a regra da derivada do produto, temos

$$f'(x) = m \cdot (x - \alpha)^{m-1} \cdot g(x) + (x - \alpha)g'(x)$$

sendo  $m = 1$ , temos

$$f'(x) = m \cdot g(x) + (x - \alpha)g'(x)$$

$$f'(\alpha) = g(\alpha) + (\alpha - \alpha)g'(\alpha) = g(\alpha) \neq 0$$

Reciprocamente, sendo  $f(x) = (x - \alpha)^m \cdot g(x)$  e  $f'(x) = m(x - \alpha)^{m-1} \cdot g(x) + (x - \alpha)^m g'(x)$ .

Observe que  $f'(\alpha) = 0 \Leftrightarrow m \geq 2$

pois  $m = 2$

$$f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x)$$

$$f'(\alpha) = 2 \cdot 0 \cdot g(\alpha) + (\alpha - \alpha)^2 g'(\alpha) = 0$$

Mas por hipótese  $f'(\alpha) \neq 0$ . Logo,  $m = 1$ . Donde  $\alpha$  é raiz simples.

ii) Se  $f(x) \in K[x]$  é um polinômio irreduzível em  $K$  e  $\alpha \in \mathbb{C}$  é uma raiz de  $f(x)$ . Queremos provar que  $m = 1$ . Seja  $p(x) = \text{irr}(\alpha, K)$ , então pelo algoritmo da divisão existem polinômios  $q(x), r(x) \in K[x]$  tais que,  $f(x) = q(x) \cdot p(x) + r(x)$  com  $r(x) = 0$  ou  $\partial r(x) < \partial p(x)$ . Como  $\alpha$  é uma raiz de  $f(x)$  vem que,

$$0 = f(\alpha) = q(\alpha) \cdot p(\alpha) + r(\alpha)$$

ou

$$r(\alpha) = f(\alpha) - q(\alpha) \cdot p(\alpha) = 0 \Rightarrow r(\alpha) = 0.$$

Como  $p(x)$  é o menor polinômio que aplicando  $\alpha$  resulta em zero, temos que  $r(x) = 0$ . Daí,

$$f(x) = q(x) \cdot p(x).$$

Mas,  $f(x)$  é irreduzível, assim, tomemos  $a \in K$  tal que,

$$f(x) = a \cdot p(x).$$

Se  $m > 1$  pelo item (i) desta Proposição têm-se,

$$f'(\alpha) = a \cdot p'(\alpha) = 0 \Rightarrow p'(\alpha) = 0$$

Mas isso contradiz a minimalidade do grau de  $p(x)$ , já que

$$\partial p'(x) < \partial p(x).$$

Assim,  $m = 1$  e por definição  $\alpha$  é raiz simples de  $f(x)$ . ■

Chamamos **corpo de decomposição** de um polinômio  $f(x) \in K[x]$  sobre  $K$ , que denotaremos por  $L = Gal(f, K)$  ao menor subcorpo de  $\mathbb{C}$  que contém  $K$  e todas as raízes de  $f(x)$  em  $\mathbb{C}$ .

Observe que tal menor subcorpo existe e é igual a interseção de todos os subcorpos de  $\mathbb{C}$  contendo  $K$  e todas as raízes de  $f(x)$  em  $\mathbb{C}$ . Sejam  $f(x) \in K[x]$  e  $\alpha_1, \dots, \alpha_r$  as distintas raízes de  $f(x)$  em  $\mathbb{C}$ . Vejamos como definir de um modo construtivo o  $Gal(f, K)$ .

Consideremos,

$$K_0 = K \subset K_1 = K[\alpha_1] \subset K_2 = K_1[\alpha_2] \subset \dots \subset K_r = K_{r-1}[\alpha_r].$$

$K_r$  é o menor subcorpo de  $\mathbb{C}$  contendo  $K$  e  $\alpha_1, \dots, \alpha_r$  e portanto  $K_r = Gal(f, K)$ . Denotando  $K_r = K[\alpha_1, \dots, \alpha_r]$  temos  $Gal(f, K) = K[\alpha_1, \dots, \alpha_r]$ . É imediato que qualquer que seja a ordem em que pegamos as raízes  $\alpha_1, \dots, \alpha_r$  ainda assim esse processo nos levaria ao  $Gal(f, K)$ . A esse processo chamamos de **adjunção de raízes**.

**Exemplo 3.2** Vamos construir o corpo de decomposição de  $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ .

Primeiramente note que  $\alpha = \sqrt[3]{2} \in \mathbb{R}$  é raiz de  $f(x)$ , pois

$$f(\sqrt[3]{2}) = (\sqrt[3]{2})^3 - 2 = 2 - 2 = 0.$$

Agora observe que

$$\beta = \sqrt[3]{2} \cdot \left( -\frac{1}{2} + \frac{\sqrt{3}}{2}i \right) \in \mathbb{C}$$

é raiz complexa de  $f(x)$ , onde  $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$  é uma raiz cúbica complexa da unidade. De fato,

$$\beta = -\frac{\sqrt[3]{2}}{2} + \frac{\sqrt[3]{2} \cdot \sqrt{3}}{2}i$$

daí,

$$\begin{aligned} f\left(-\frac{\sqrt[3]{2}}{2} + \frac{\sqrt[3]{2} \cdot \sqrt{3}}{2}i\right) &= \left(-\frac{\sqrt[3]{2}}{2} + \frac{\sqrt[3]{2} \cdot \sqrt{3}}{2}i\right)^3 - 2 = \\ &= \left(-\frac{\sqrt[3]{2}}{2} + \frac{\sqrt[3]{2} \cdot \sqrt{3}}{2}i\right) \left(-\frac{\sqrt[3]{2}}{2} + \frac{\sqrt[3]{2} \cdot \sqrt{3}}{2}i\right)^2 - 2 = \\ &= \left(-\frac{\sqrt[3]{2}}{2} + \frac{\sqrt[3]{2} \cdot \sqrt{3}}{2}i\right) \left(\frac{(\sqrt[3]{2})^2}{4} + 2\left(-\frac{\sqrt[3]{2}}{2} \cdot \frac{\sqrt[3]{2} \cdot \sqrt{3}}{2}i\right) + \left(-\frac{(\sqrt[3]{2})^2(\sqrt{3})^2}{4}\right)\right) - 2 = \end{aligned}$$

$$\begin{aligned}
& \left( -\frac{\sqrt[3]{2}}{2} + \frac{\sqrt[3]{2} \cdot \sqrt{3}}{2} i \right) \left( \frac{\sqrt[3]{4}}{4} - \frac{\sqrt[3]{4} \cdot 3}{4} - \frac{\sqrt[3]{4} \cdot \sqrt{3} i}{2} \right) - 2 = \\
& = \left( -\frac{\sqrt[3]{2}}{2} + \frac{\sqrt[3]{2} \cdot \sqrt{3}}{2} i \right) \left( -\frac{\sqrt[3]{4}}{2} - \frac{\sqrt[3]{4} \sqrt{3} i}{2} \right) - 2 = \\
& = \frac{\sqrt[3]{8}}{4} + \frac{\sqrt[3]{8} \cdot \sqrt{3} i}{4} - \frac{\sqrt[3]{8} \cdot \sqrt{3} i}{4} - \frac{\sqrt[3]{8} \cdot 3 i^2}{4} - 2 = \\
& = \frac{\sqrt[3]{8}}{4} - \frac{\sqrt[3]{8} \cdot 3 i^2}{4} - 2 = \\
& = \frac{1}{2} + \frac{6}{4} - 2 = \frac{2+6-8}{4} = 0
\end{aligned}$$

E mais  $\bar{\beta} = \sqrt[3]{2} \left( -\frac{1}{2} - \frac{\sqrt{3}}{2} i \right)$  é raiz de  $f$ .

Logo, as três raízes distintas de  $f(x) = x^3 - 2$  em  $\mathbb{C}$  são  $\alpha = \sqrt[3]{2}$ ,  $\beta = \sqrt[3]{2} \left( -\frac{1}{2} + \frac{\sqrt{3}}{2} i \right)$  e  $\bar{\beta} = \sqrt[3]{2} \left( -\frac{1}{2} - \frac{\sqrt{3}}{2} i \right)$ . Então

$$\text{Gal}(x^3 - 2, \mathbb{Q}) = \mathbb{Q}[\alpha, \beta, \bar{\beta}] = \mathbb{Q}[\alpha, \beta].$$

**Definição 3.1** Seja  $K$  um corpo. Um **automorfismo** de  $K$  é um isomorfismo  $f : K \rightarrow K$ . O conjunto dos automorfismos de  $K$  será denotado por  $\text{Aut}K$

**Proposição 3.3** Seja  $L \supset K$  é uma extensão de  $K$ , onde  $K$  é um subcorpo de  $\mathbb{C}$ . Considere o seguinte conjunto:

$$\text{Aut}_K L = \{ \sigma \in \text{Aut}L : \sigma(a) = a, \forall a \in K \}.$$

Seja  $f(x) \in K[x]$  e  $\alpha \in L$  uma raiz de  $f(x)$  em  $L$ , então  $\sigma(\alpha)$  é também uma raiz de  $f(x)$  em  $L$ ,  $\forall \sigma \in \text{Aut}_K L$ .

**Demonstração:** Seja  $\alpha \in L$  é uma raiz de  $f(x)$ , têm-se que  $f(\alpha) = 0$ . Note que,

$$\sigma(\alpha) = \alpha, \text{ pois } \sigma(\alpha) \in \text{Aut}_K L$$

e mais ainda,

$$f(\sigma(\alpha)) = f(\alpha) = 0 \Rightarrow f(\sigma(\alpha)) = 0$$

Isto nos diz que  $\sigma(\alpha)$  é uma raiz de  $f(x) \in K[x]$ . ■

### 3.3. Grau de uma Extensão

**Proposição 3.4** Seja  $K$  um corpo e  $L \supset K$  uma extensão de  $K$ . Então:

a) Se  $L \supset K$  é finita, então  $L \supset K$  é algébrica;

- b) Se  $\alpha \in L \supset K$  é um elemento algébrico sobre  $K$  e o grau de  $\text{irr}(\alpha, K)$  é igual a  $n$  então  $1, \alpha, \dots, \alpha^{n-1}$  é uma base do espaço vetorial  $K[\alpha]$  sobre  $K$  e  $[K[\alpha] : K] = n < \infty$ ;
- c) Se  $\alpha \in L \supset K$  é um elemento transcendente sobre  $K$ , então  $K[\alpha] \supset K$  é uma extensão infinita.

**Demonstração:** a) Suponha  $[L : K] = m < \infty$  e  $\alpha \in L \supset K$  como  $K[\alpha]$  um subespaço de  $L$  segue que  $[K[\alpha] : K] \leq m < \infty$ . Se  $[K[\alpha] : K] = n$  então o conjunto  $1, \alpha, \dots, \alpha^n$  é L.D., pois  $n$  é o número máximo de elementos de L.I., e portanto existem escalares  $a_0, a_1, \dots, a_n$  não nulos tais que

$$a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$$

e isso significa que  $\alpha$  é algébrico sobre  $K$ , pois basta considerar  $p(x) = a_0 + a_1x + \dots + a_nx^n$

b) Seja  $\alpha \in L \supset K$  um elemento algébrico sobre  $K$  tal que grau de  $\text{irr}(\alpha, K) = n$ . Mas pela Proposição 3.1 todo elemento de  $K[\alpha]$  pode ser escrito de modo único como combinação linear sobre  $K$  de  $1, \alpha, \dots, \alpha^{n-1}$ . Assim,  $1, \alpha, \dots, \alpha^{n-1}$  é uma base de  $K[\alpha]$  sobre  $K$ . Logo,  $[K[\alpha] : K] = n$ .

c) Segue de imediato do item (a)

■

Vejamos um corolário que decorre desta proposição

**Corolário 3.3** *Seja  $\alpha \in L \supset K$ . Então, as seguintes afirmações são equivalentes:*

- i)  $\alpha$  é algébrico sobre  $K$ ;
- ii)  $[K[\alpha] : K] < \infty$ ;
- iii)  $K[\alpha]$  é uma extensão algébrica de  $K$ .

**Demonstração:** *i)  $\Rightarrow$  ii)* Note que se  $\alpha \in L \supset K$  é algébrico sobre  $K$ , então existe  $p(x) \in K[x]$  implica que  $p(\alpha) = 0$ . Seja  $f(x) = \text{irr}(\alpha, K)$ , com  $\partial f(x) = n$  pela minimalidade do grau de  $f(x)$  e por resultado da Proposição 3.4, item (b) temos que,  $1, \alpha, \dots, \alpha^{n-1}$  é uma base de  $K[x]$  e  $[K[\alpha] : K] = n < \infty$ .

*ii)  $\Rightarrow$  iii)* Suponha  $[K[\alpha] : K] = n < \infty$ . Então pela Proposição 3.4 item (a) temos que  $K[\alpha]$  é uma extensão algébrica de  $K$ .

*iii)  $\Rightarrow$  (i)* Sendo  $K[\alpha]$  uma extensão algébrica sobre  $K$ , por definição  $\alpha$  é algébrico sobre  $K$ .

■

**Proposição 3.5** *Sejam  $M \supset L \supset K$  corpos tais que  $[M : L]$  e  $[L : K]$  são finitos então  $[M : K]$  é finito e  $[M : K] = [M : L] \cdot [L : K]$ .*

**Demonstração:** Suponha  $M$  sobre  $K$  finita. Temos que  $L$  é um subespaço do  $K$ -espaço vetorial  $M$ . Logo,  $[L : K]$  é finita. Considere  $\beta$  uma base de  $M$  sobre  $K$ . Temos que  $\beta$  é finita e

que  $\beta$  gera  $M$  também como  $L$ -espaço vetorial. Logo,  $[M : L]$  é finita. Suponha agora  $[M : L]$  e  $[L : K]$  finitas. Sendo  $[M : L] = m$  e  $[L : K] = n$ ,  $\alpha = \{\alpha_1, \dots, \alpha_m\}$  é base de  $M$  sobre  $L$  e  $\gamma = \{\beta_1, \dots, \beta_n\}$  é base de  $L$  sobre  $K$ . Tomemos

$$\delta = \{\beta_i \alpha_j : i = 1, \dots, n; j = 1, \dots, m\}$$

$\delta$  é base de  $M$  sobre  $K$ . De fato, suponha  $x \in M$ , temos

$$x = a_1 \alpha_1 + \dots + a_m \alpha_m, \text{ com } a_j \in L$$

$\gamma$  é base de  $L$  sobre  $K$ , temos  $\lambda_{ij} = \lambda_{ij} \beta_1 + \dots + \lambda_{nj} \beta_n$  com  $\lambda_{ij} \in K$  para  $i = 1, \dots, n$  e  $j = 1, \dots, m$ . Logo,  $x$  é combinação linear dos elementos de  $\delta$  com coeficientes em  $K$ . Assim,  $\delta$  gera o  $K$ -espaço vetorial  $M$ .

Suponha agora,  $\lambda_{ij} \in K$ ,  $i = 1, \dots, n$  e  $j = 1, \dots, m$  tais que

$$\sum_{j=1}^m \sum_{i=1}^n \lambda_{ij} \beta_i \alpha_j = 0$$

Temos que

$$(\lambda_{11} \beta_1 + \dots + \lambda_{n1} \beta_n) \alpha_1 + \dots + (\lambda_{1m} \beta_1 + \dots + \lambda_{nm} \beta_n) \alpha_m = 0$$

como  $\alpha$  é L.I sobre  $L$ , devemos ter  $(\lambda_{1j} \beta_1 + \dots + \lambda_{nj} \beta_n) = 0$  para todo  $j = 1, \dots, m$ . Como  $\gamma$  é L.I sobre  $K$ , devemos ter  $\lambda_{ij} = 0$ . Assim,

$$[M : K] = m \cdot n = [M : L][L : K]$$

■

**Corolário 3.4** a) Se  $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ algébrico sobre } \mathbb{Q}\}$  então  $\overline{\mathbb{Q}}$  é subcorpo de  $\mathbb{C}$  e é uma extensão algébrica infinita de  $\mathbb{Q}$ ;

b) Se  $\overline{\mathbb{Q}_{\mathbb{R}}} = \{\alpha \in \mathbb{R} : \alpha \text{ algébrico sobre } \mathbb{Q}\}$  então é um subcorpo de  $\mathbb{R}$  e é uma extensão algébrica infinita de  $\mathbb{Q}$ .

**Demonstração:** a) Por definição  $\overline{\mathbb{Q}}$  é um subconjunto de  $\mathbb{C}$  e contém  $\mathbb{Q}$ . Mostremos que  $\overline{\mathbb{Q}}$  é um subcorpo de  $\mathbb{C}$ . Para isso é suficiente provarmos as seguintes três propriedades:

i)  $\alpha, \beta \in \overline{\mathbb{Q}_c} \Rightarrow \alpha - \beta \in \overline{\mathbb{Q}_c}$

ii)  $\alpha, \beta \in \overline{\mathbb{Q}_c} \Rightarrow \alpha \cdot \beta \in \overline{\mathbb{Q}_c}$

iii)  $0 \neq \alpha \in \overline{\mathbb{Q}_c} \Rightarrow \frac{1}{\alpha} \in \overline{\mathbb{Q}_c}$

Vamos demonstrar simultaneamente i), ii), e iii). De fato, seja  $K = \mathbb{Q}[\alpha]$  e  $L = K[\beta]$ . Como  $\alpha$  é algébrico sobre  $\mathbb{Q}$  segue pelo Corolário 1 que  $[K : \mathbb{Q}] < \infty$ . Agora sendo  $\beta$  algébrico

sobre  $\mathbb{Q}$ ,  $\beta$  também é algébrico sobre  $K$  e daí pelo mesmo Corolário segue que  $[L : K] < \infty$ . Pela Proposição 3.5, temos que

$$[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}],$$

segue que  $[L : \mathbb{Q}] < \infty$  e pela Proposição 3.4 temos que  $L \supset \mathbb{Q}$  é uma extensão algébrica. Agora o resultado sai imediatamente  $\alpha \pm \beta \in L$ ,  $\alpha \cdot \beta \in L$  e  $\frac{1}{\alpha} \in L$  se  $\alpha \neq 0$ . Imediatamente segue que  $\overline{\mathbb{Q}_c}$  é uma extensão algébrica sobre  $\mathbb{Q}$ . Agora se  $\alpha_i = \sqrt[i]{2}$  e  $K_0 = \mathbb{Q}$ ,  $K_1 = \mathbb{Q}[\alpha_1], \dots, K_i = K_{i-1}[\alpha_i]$  temos que  $M = \bigcup_{i=0}^{\infty} K_i$  é uma extensão algébrica infinita de  $\mathbb{Q}$  e  $M \subset \overline{\mathbb{Q}_c} \subset \overline{\mathbb{Q}}$ .

b) Basta observar que  $\overline{\mathbb{Q}_R} = \overline{\mathbb{Q}} \cap \mathbb{R}$ . De fato  $\overline{\mathbb{Q}_R} = \{\alpha \in \mathbb{R} : \alpha \text{ algébrico sobre } \mathbb{Q}\}$  temos  $\beta \in \overline{\mathbb{Q}_c} \cap \mathbb{R} \Rightarrow \beta \in \overline{\mathbb{Q}_c} = \{\beta \in \mathbb{C} : \beta \text{ é algébrico sobre } \mathbb{Q}\}$  e  $\beta \in \mathbb{R}$  implica que  $\beta \in \mathbb{R}$  e  $\beta$  é algébrico sobre  $\mathbb{Q}$ , assim,  $\beta \in \overline{\mathbb{Q}_R}$ , ou seja,  $\beta \in \mathbb{R}$  e  $\beta$  é algébrico sobre  $\mathbb{Q}$ . Como  $\mathbb{R} \subset \mathbb{C}$ , podemos tomar  $\beta \in \overline{\mathbb{Q}_c}$  e daí segue  $\beta \in \overline{\mathbb{Q}_c} \cap \mathbb{R}$  e também  $M = \bigcup_{i=0}^{\infty} K_i \subset \overline{\mathbb{Q}_R}$ . ■

**Corolário 3.5** *Seja  $K \supset \mathbb{Q}$  tal que  $[K : \mathbb{Q}] = m$  e  $p(x) \in \mathbb{Q}[x]$  um polinômio irredutível sobre  $\mathbb{Q}$  tal que  $\partial p(x) = n$ . Se  $M.D.C.\{m, n\} = 1$  então  $p(x)$  é um polinômio irredutível sobre  $K$ .*

**Demonstração:** Seja  $\alpha \in \mathbb{C}$  uma raiz de  $p(x)$ . Considere agora os corpos  $\mathbb{Q} \subset K[\alpha]$  e suponhamos que  $[K[\alpha] : K] = r$  e  $[K[\alpha] : \mathbb{Q}[\alpha]] = s$ . como  $\partial p(x) = n$  e  $p(x)$  é irredutível e  $p(x) \in \mathbb{Q}[x]$  sobre  $\mathbb{Q}$  segue que  $[\mathbb{Q}[\alpha] : \mathbb{Q}] = n$  e  $[K[\alpha] : K] = r = n$ . De fato, pela Proposição 3.5 segue que  $n \cdot s = m \cdot r$  e como  $M.D.C.\{n, m\} = 1$  vem que  $n|r$ . Mas  $r \leq n$  nos diz que  $n = r$  e assim  $p(x)$  é também irredutível sobre  $K$ . ■

**Corolário 3.6** *Seja  $L = Gal(x^p - 2, \mathbb{Q})$ . Então  $[L : \mathbb{Q}] = p \cdot (p - 1)$ .*

**Demonstração:** De fato, sabemos que  $L = Gal(x^p - 2, \mathbb{Q}) = \mathbb{Q}[\alpha, u]$  onde

$$\alpha = \sqrt[p]{2} \in \mathbb{R} \text{ e } u = \left( \cos \frac{2\pi}{p} + i \operatorname{sen} \frac{2\pi}{p} \right) \in \mathbb{C}$$

é uma raiz  $p$ -ésima da unidade tal que  $1, u, u^2, \dots, u^{p-1}$  nos dão todas as distintas raízes  $p$ -ésimas da unidade em  $\mathbb{C}$  (por isso  $u$  diz-se uma raiz primitiva da unidade). Agora pela Proposição 3.5,

$$[L : \mathbb{Q}] = [L : \mathbb{Q}[\alpha]] \cdot [\mathbb{Q}[\alpha] : \mathbb{Q}]$$

Pelo critério de Eisenstein temos  $[\mathbb{Q}[\alpha] : \mathbb{Q}] = p$ . Agora se  $K = \mathbb{Q}[\alpha]$  temos  $L = K[u] \supset K \supset \mathbb{Q}$ . Ainda por Eisenstein temos que  $u$  é a raiz de  $x^{p-1} + x^{p-2} + \dots + x + 1$  que é polinômio irredutível de grau  $p - 1$  sobre  $\mathbb{Q}$ . Como  $[K : \mathbb{Q}] = p$  e  $M.D.C.\{p, p - 1\} = 1$



temos pelo Corolário anterior que  $x^{p-1} + x^{p-2} + \dots + x + 1$  é ainda irredutível sobre  $K$  tendo  $u$  como raiz. Portanto  $[K[u] : K] = p - 1$  e isto demonstra o nosso Corolário pois

$$L = K[u] \text{ e } K = \mathbb{Q}[\alpha].$$

■

**Teorema 3.2** *Seja  $L \supset K \supset \mathbb{Q}$  tal que  $[L : K] < \infty$ . Então, existe  $u \in L$  tal que  $L = K[u]$ .*

**Corolário 3.7** *Seja  $L \supset K \supset \mathbb{Q}$  tal que  $[L : K] < \infty$ . Então,  $[L : K] \geq |Aut_K L|$  (onde  $|Aut_K L|$  denota o número de elementos do conjunto  $Aut_K L = \{f \in Aut L; f(\lambda) = \lambda, \forall \lambda \in K\}$ )*

**Demonstração:** Seja  $L \supset K \supset \mathbb{Q}$  com  $[L : K] < \infty$ . Então pelo Teorema 3.2 existe,  $u \in L$  tal que  $L = K[u]$ .

Sendo  $\alpha \in Aut_K L$  e  $p(x) = irr(\alpha, K)$  segue da Proposição 3.3 que  $u' = \sigma(u)$  é também raiz de  $p(x)$ , com  $u \in L$ . Ora  $K[u'] \subset L$  e  $[K[u'] : K] = [L : K] = \partial p(x)$  nos diz que  $L = K[u] = K[u']$ . Como  $\sigma(a) = a, \forall a \in K$ ,  $\sigma$  fica completamente determinado pelo valor  $u' = \sigma(u)$ . Assim o número  $|Aut_K L|$  é no máximo igual ao número de raízes  $u'$  de  $p(x)$  que pertencem a  $L$ . Certamente esse número é no máximo o grau do polinômio  $p(x) = irr(u, K)$ , em que  $\partial p(x) = [L : K]$  ■

**Demonstração:** (Teorema 3.2) A demonstração será por indução sobre o grau  $[L : K] < \infty$ . Se  $[L : K] = 1$  segue que  $L = K$  e o teorema é válido trivialmente.

Suponhamos  $[L : K] > 1$ . Assim, existe  $\alpha_1 \in L, \alpha_1 \notin K$  Seja  $K_1 = K[\alpha_1]$ . Se  $K_1 = L$  o teorema está demonstrado. Assim, existe  $\alpha_2 \in L, \alpha_2 \notin K_1$ .

Seja  $K_2 = K_1[\alpha_2] = K[\alpha_1, \alpha_2]$ . Como  $[L : K] < \infty$  conseguimos  $\alpha_1, \alpha_2, \dots, \alpha_r, r \geq 2$ , elementos de  $L$  tais que,  $L = K[\alpha_1, \alpha_2, \dots, \alpha_r]$  e  $\alpha_i \notin K[\alpha_1, \alpha_2, \dots, \alpha_{i-1}] = K_{i-1}$ ,  $K_r = L \supseteq K_{r-1} = K[\alpha_1, \alpha_2, \dots, \alpha_{r-1}] \supset, \dots, \supset K_1 = K[\alpha_1] \supset K_0 = K$  como  $[K_{r-1} : K] < \infty$  temos pela hipótese de indução que existe  $\alpha \in K_{r-1} = K[\alpha]$  e daí segue imediatamente que  $L = K_r = K[\alpha, \alpha_r]$ . Chamando  $\alpha_r = \beta \in L$  temos  $L = K[\alpha, \beta]$ . Agora vamos supor que existe  $u \in L$  tal que  $L = K[u]$ .

Sejam  $p(x) = irr(\alpha, K)$  e  $q(x) = irr(\beta, K)$  tais que  $\partial p(x) = m$  e  $\partial q(x) = n$ . Pela Proposição 3.2 item *iii*) segue que todas as raízes de  $p(x)$  (respectivamente  $q(x)$ ) são distintas em  $\mathbb{C}$ .

Sejam  $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_m$  as raízes de  $p(x)$  em  $\mathbb{C}$  e sejam  $\beta_1 = \beta, \beta_2, \dots, \beta_n$  as raízes de  $q(x)$  em  $\mathbb{C}$ . Vamos definir para  $j \neq i$  os seguintes números complexos,

$$j \neq i, \lambda_{ij} = \frac{\alpha_i - \alpha}{\beta - \beta_j} \in \mathbb{C}$$

Como  $K$  é um corpo infinito então existe  $\lambda \in K$  tal que  $\lambda \notin \left\{ \lambda_{ij} : \begin{array}{l} 1 \leq i \leq m \\ 2 \leq j \leq n \end{array} \right\}$ .

Agora seja  $u = \alpha + \lambda\beta \in L$  e assim  $K[u] \subset L$ , vamos provar que de fato  $L = K[u]$ . Para isso vamos provar que  $\alpha, \beta \in K[u]$ .

Seja  $F = K[u]$  e seja  $h(x) = p(u - \lambda x) \in F[x]$ , observe que

$$h(\beta) = p(u - \lambda\beta) = p(\alpha + \lambda\beta - \lambda\beta) = p(\alpha) = 0.$$

Mas  $\beta$  também é raiz de  $q(x) \in K[x] \subset F[x]$ . Portanto pelo Teorema 1.6  $(x - \beta)$  é um divisor de  $d(x) = M.D.C\{q(x), h(x)\}$  em  $\mathbb{C}[x]$ . Vamos de fato provar que  $d(x) = (x - \beta)$ , e para isso é suficiente provarmos que se  $d(\beta_j) = 0$  então  $j = 1$  já que  $d(x)|q(x)$ , e  $q(x)$  só possui raízes simples.

Se  $d(\beta_j) = 0$  e  $j \neq 1$  teremos  $h(\beta_j) = 0$ , ou seja,  $p(u - \lambda\beta_j) = 0$  o que nos diz que existe  $i$ ,  $1 \leq i \leq m$  tal que  $\alpha_i = u - \lambda\beta_j = \alpha + \lambda\beta - \lambda\beta_j$  e daí segue que  $\lambda = \lambda_{ij}$  contradizendo a nossa escolha de  $\lambda$ . Portanto  $x - \beta = d(x)$ .

Agora se  $d_1x = M.D.C\{q(x), h(x)\}$  em  $F[x]$ , então temos por  $F \subset \mathbb{C}$  que grau de  $d_1x$  é menor ou igual ao grau  $d(x)$ . Portanto se  $d_1x \neq d(x)$  teríamos que  $1 = M.D.C\{q(x), h(x)\}$  em  $F[x]$  mas então sugeriria que  $d(x) = 1$  o que é um absurdo. Logo  $d(x) = x - \beta = M.D.C\{q(x), h(x)\}$  em  $F[x]$  e isto nos diz que  $\beta \in F$ . Agora,  $\alpha = u - \lambda\beta \in F$  pois  $u \in F = K[u]$ ,  $\beta \in F$ ,  $\lambda \in K \subset F$  demonstrando nosso teorema. ■

## Referências

COELHO, F. Ulhoa. **Um Curso de Álgebra Linear**, 2<sup>o</sup>ed. São Paulo: IMPA, 2005.

FRALEIGH, J. B. **A First Course in Abstract Algebra**, 7th Edition, Seventh Edition, 2002.

HYGINO, D.; GELSON, I. **Álgebra Moderna**, São Paulo: editora atual, 2003.

GARCIA, A.; YVES, L. **Álgebra: um curso de introdução**, Rio de Janeiro: IMPA, 1988.

GONÇALVES, A. **Introdução à Álgebra**, 5<sup>o</sup>. Rio de Janeiro: IMPA, 2011.

# A Algumas noções básicas de Álgebra Linear

Nesta seção relembremos algumas noções básicas de álgebra linear, como espaço vetorial e base.

**Definição A.1** *Seja  $K$  um corpo qualquer e seja  $V$  um conjunto não vazio onde está definida uma operação soma. Suponhamos também que esteja definida, uma operação de elementos de  $K$  por elementos de  $V$ . Assim, estão definidas:*

$$+ : V \times V \longrightarrow V \quad e \quad \cdot : K \times V \longrightarrow V$$

$$(u, v) \longmapsto u + v \quad (\lambda, v) \longmapsto \lambda \cdot v$$

*Dizemos que  $V$  munido dessas operações é um **espaço vetorial** sobre o corpo  $K$  se as seguintes proposições são verificadas quaisquer que sejam  $u, v, w \in V$  e  $\lambda, \mu \in K$ :*

- i)  $u + (v + w) = (u + v) + w$*
- ii)  $\exists 0 \in V$  tal que  $u + 0 = 0 + u = u$*
- iii)  $\forall x \in V \exists y \in V$  tal que  $x + y = y + x = 0$*
- iv)  $u + v = v + u$*
- v)  $1v = v$  onde  $1$  é a unidade do corpo  $K$*
- vi)  $\lambda(u + v) = \lambda u + \lambda v$  e  $(\mu + \lambda)u = \mu u + \lambda u$*
- vii)  $\lambda(\mu v) = \mu(\lambda v) = (\lambda\mu)v$*

**Exemplo A.1** *Sejam  $K$  um corpo qualquer,  $L \supset K$  um extensão e  $\alpha \in L$ . É de fácil verificação que pode se definir operações sobre  $K[x]$  (respectivamente  $K[\alpha]$ ) de modo que  $K[x]$  (respectivamente  $K[\alpha]$ ) torna-se um espaço vetorial sobre  $K$ . Para isso cons basta considerar em  $K[x]$  e  $K[\alpha]$  segue analogamente. Considere as seguintes operações:*

$$+ : K[x] \times K[x] \longrightarrow K[x] \quad e \quad \cdot : K \times K[x] \longrightarrow K[x]$$

$$(f(x), g(x)) \longmapsto f(x) + g(x) \quad (\lambda, f(x)) \longmapsto \lambda \cdot f(x)$$

*Agora Sejam  $f(x), g(x), e h(x) \in K[x]$  e  $\lambda, \mu \in K$ .*

- i)  $f(x) + (g(x) + h(x)) = (f(x) + g(x)) + h(x)$ ;*
- ii)  $\exists 0(x) \in K[x]$  tal que  $0(x) + f(x) = f(x) + 0(x) = f(x)$*

- iii)  $\forall f(x) \in K[x] \exists -f(x) \in K[x]$  tal que  $f(x) + (-f(x)) = -f(x) + f(x) = 0 = 0(x)$ ;  
 iv)  $f(x) + g(x) = g(x) + f(x)$ ;  
 v)  $1f(x) = f(x)$  onde 1 é a unidade do corpo  $K$ ;  
 vi)  $\lambda(f(x) + g(x)) = \lambda f(x) + \lambda g(x)$  e  $(\mu + \lambda)f(x) = \mu f(x) + \lambda f(x)$ ;  
 vii)  $\lambda(\mu f(x)) = \mu(\lambda f(x)) = (\lambda\mu)f(x)$ .

Portanto  $K[x]$  com estas operações é um espaço vetorial sobre  $K$ .

**Exemplo A.2** Finalmente  $L \supset K$  é uma extensão de corpos  $L$  pode ser visto como espaço vetorial sobre o corpo  $K$ . De fato, as operações  $+$  :  $L \times L \rightarrow L$  e  $\cdot$  :  $K \times L \rightarrow L$  já existem de modo natural no corpo  $L$ . A verificação das propriedades que definem espaço vetorial é similar ao que foi feito no exemplo anterior.

Até o fim desta seção  $K$  representa um corpo de  $V$  um espaço vetorial sobre  $K$ .

Um subconjunto não vazio  $W$  de  $V$  diz-se um subespaço vetorial de  $V$  se as seguintes condições são satisfeitas:

- a)  $w_1, w_2 \in W \Rightarrow w_1 + w_2 \in W$ ;  
 b)  $\lambda \in K, w \in W \Rightarrow \lambda w \in W$ .

Observe que pelas condições acima as operações do espaço vetorial  $V$  induzem operações em  $W$  e o próprio  $W$  é um espaço vetorial com as operações induzidas.

Se  $v_1, \dots, v_n \in V$  dizemos que  $v_1, \dots, v_n$  são linearmente independentes se a equação vetorial  $\sum_{i=1}^n \alpha_i v_i = 0$ ,  $\alpha_i \in K$  é satisfeita apenas para os escalares  $\alpha_1 = \alpha_2 = \dots = \alpha_n = 0$ . Caso contrário dizemos que  $v_1, \dots, v_n$  são linearmente dependentes. Usamos simbolicamente L.I para linearmente independentes e L.D para linearmente dependentes. Por exemplo,  $e_1 = (1, 0, \dots, 0)$ ,  $e_2 = (0, 1, \dots, 0)$ , ...,  $e_n = (0, 0, \dots, 1)$  são L.I em  $K^n$ .

Se  $u_1, u_2, \dots, u_r \in V$  então é fácil verificar que

$$W = \left\{ \sum_{i=1}^r \alpha_i u_i : \alpha_i \in K, i = 1, \dots, r \right\}$$

é um subespaço vetorial de  $V$ , o qual chamaremos de subespaço gerado por  $u_1, \dots, u_r$ . Denotaremos esse espaço por,

$$W = \langle u_1, \dots, u_r \rangle.$$

Se um conjunto (ordenado)  $v_1, \dots, v_n \in V$  for L.I. e tal que  $\langle v_1, \dots, v_n \rangle = V$  dizemos que  $v_1, \dots, v_n$  é uma base de  $V$ . Por exemplo,  $e_1, \dots, e_n$  é uma base de  $K^n$ .

**Teorema A.1** *a) Todo espaço vetorial  $V$  sobre um corpo  $K$  possui uma base.*  
*b) Se um espaço vetorial  $V$  sobre um corpo  $K$  possui uma base com  $n$  elementos então toda base de  $V$  possui  $n$  elementos.*

**Demonstração:** Ver demonstração no livro de Flávio Ulhôa

■