UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS VI - POETA PINTO DO MONTEIRO
CENTRO DE CIÊNCIAS HUMANAS E EXATAS
CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

JÚLIO FERNANDES DA SILVA

UMA INTRODUÇÃO À EXTENSÕES DE CORPOS FINITAS E ALGÉBRICAS

MONTEIRO - PB, BRASIL
Dezembro de 2018

JÚLIO FERNANDES DA SILVA

UMA INTRODUÇÃO À EXTENSÕES DE CORPOS FINITAS E ALGÉBRICAS

Trabalho de Conclusão do Curso apresentado à coordenação do curso de Licenciatura em Matemática do Centro de Ciências Humanas e Exatas da Universidade Estadual da Paraíba, em cumprimento às exigências legais para a obtenção do título de Graduado no Curso de Licenciatura Plena em Matemática.

Área de concentração: Matemática Pura.

Orientador: Me. Marciel Medeiros de Oliveira

MONTEIRO - PB, BRASIL
Dezembro de 2018

S586i Silva , Júlio Fernandes da.
Uma introdução à extensões de corpos finitas e algébricas [manuscrito] / Julio Fernandes da Silva . - 2018.
45 p.
Digitado.
Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências Humanas e Exatas , 2018.
"Orientação : Prof. Dr. Marciel Medeiros de Oliveira , Coordenação do Curso de Matemática - CCHE."
1. Extensões de corpos (Matemática) . 2. Anéis (Matemática) . 3. Corpos Finitos (Álgebra). 4. Polinômios. I. Título
21. ed. CDD 512.4

JÚLIO FERNANDES DA SILVA

UMA INTRODUÇÃO À EXTENSÕES DE CORPOS FINITAS E ALGÉBRICAS

Trabalho de Conclusão do Curso apresentado à coordenação do curso de Licenciatura em Matemática do Centro de Ciências Humanas e Exatas da Universidade Estadual da Paraíba, em cumprimento às exigências legais para a obtenção do título de Graduado no Curso de Licenciatura Plena em Matemática.

Área de concentração: Matemática pura

Aprovada em: 10/12/2018.

BANCA EXAMINADORA

Marciel Medeiros de Oliveira

Me. Marciel Medeiros de Oliveira
Orientador

Luiz Lima de Oliveira Júnior

Me. Luiz Lima de O. Júnior
Examinador interno (CCHE/UEPB)

José Marcos da Silva

Me. José Marcos da Silva
Examinador externo (IFPB/Monteiro)

Dedico este presente trabalho a todos que estiveram presentes durante a minha graduação, entre estes meus colegas e professores, foi muito importante todo apoio e incentivo que recebi, dedico a minha esposa Letícia Souza Rodrigues, aos meus pais José Francisco da Silva e Josenilda Maria da Silva e meu irmão Júnior Fernandes da Silva. Dedicar também ao meu avô Vanildo da Silva (ausente), lembro de ouvir ele sempre me dizer que um dos seus grandes desejos era ver um filho ou neto formado.

AGRADECIMENTOS

Eu gostaria de agradecer primeiramente a Deus por estar vivo e com saúde para finalizar mais essa etapa da minha vida. Agradecer aos meus professores, mestres e doutores, todos que contribuíram para minha formação intelectual e social. Muito obrigado meu amigo Professor, Mestre Marciel Medeiros, por ter me orientado e acima de tudo por ter me apresentado a fascinante Álgebra Matemática e seus resultados tão elegantes. Agora um agradecimento especial para minha esposa Letícia Rodrigues por ter desde o início me incentivado e me apoiado todos os dias para que eu obtivesse sucesso nesse desafio. Obrigado, toda minha família e colegas que sempre, sinceramente, me apoiaram.

"E se eu tiver o dom de profecia e entender todos os segredos sagrados e todo conhecimento, e se eu tiver toda a fé, a ponto de mover montanhas, mas não tiver amor, nada sou."

(1 Coríntios 13:2)

RESUMO

Este trabalho tem como objetivo apresentar alguns tópicos sobre extensões de corpos finitas e algébricas. Para tanto realizamos um trabalho, abordamos alguns dos conceitos iniciais sobre grupos abelianos e teoria dos anéis e corpos, resultados sobre extensões de corpos, os quais são fundamentais para o entendimento das extensões finitas e algébricas. Estas ultimas trazem resultados indispensáveis e elegantes para estudos aprofundados da teoria dos corpos. Por fim, apresentamos um exemplo atípico de uma extensão algébrica que não é finita.

Palavras-chave: Extensões de corpos. Extensões de Corpos Algébricas. Extensões de Corpos Finitas.

ABSTRACT

This paper aims to present some topics on extensions of finite and algebraic bodies. In order to do this, we will discuss some of the initial concepts about abelian groups and theory of rings and bodies, results on body extensions, which are fundamental for the understanding of finite and algebraic extensions. The latter provide indispensable and elegant results for in-depth studies of the theory of corpos. Finally, we present an atypical example of an algebraic extension that is not finite.

Key-words:Field extensions. Algebrica Fiel Extensions. Finite Field Extensions.

SUMÁRIO

INTRODUÇÃO

As Extensões de Corpos Finitas e Algébricas são importantes resultados dos estudos da Teoria dos Corpos, estudados pela subárea da Matemática chamada Álgebra Abstrata. Desse modo os resultados apresentados nos dão ferramentas para estudos mais aprofundados a respeito da Teoria de Galois.

O presente estudo é fruto de um trabalho bibliográfico e foi dividido em três capítulos, os quais são compostos por definições, exemplos e resultados fundamentais sobre anéis e corpos e extensões de copros.

O primeiro capítulo expõe conceitos e resultados preliminares sobre Grupos Abelianos e Teoria dos Anéis e Corpos. No segundo capítulo, apresentamos o estudo de Extensões de Corpos, o qual traz conceitos e resultados de grande importância para o entendimento do capítulo posterior. No terceiro capítulo apresentamos o estudo das Extensões de Corpos Finitas e Algébricas, o qual nos apresenta resultados indispensáveis e deverás elegantes para estudos aprofundados da Teoria dos Corpos. E por fim ainda no terceiro capítulo, apresentamos um exemplo atípico de uma exensão algébrica que não é finita.

1 TÓPICOS ELEMENTARES DE ANÉIS, HOMOMORFISMOS E IDEAIS

Esses tópicos iniciais são muito importantes para as construçoes futuras envolvendo as Extesões de Corpos. Iniciamente para entender a definição de um anel é necessario que conheçamos um grupo abeliano.

Nesse sentido, consideremos um conjunto não vazio G munido de uma operação * . Dizemos que $(G, *)$ é um **grupo** quando as propriedades a seguir são satisfeitas:
i) A operação é associativa, isto é,

$$a * (b * c) = (a * b) * c, \ \forall \ a, \ b \ c \in G.$$

ii) Existe elemento neutro para *, isto é,

$$\text{e} \ \in \ G \ \text{ tal que } \ a * e = e * a = a, \forall \ a \ \in G.$$

iii) Todo elemento em G é invertível segundo a operação *, isto é,

$$\forall \ a \in G, \ existe \ a^{'} \in G \ tal \ que \ a * a^{'} = a^{'} * a = e$$

Um grupo $(G, *)$ é **comutativo** ou **abeliano** quando

$$a * b = b * a, \forall a, b \in G.$$

ou seja, quando a operação em G for comutativa.
Chamamos normalmente a operação $*$ de produto. E neste caso, o grupo $(G, *)$ é chamado de grupo multiplicativo. Em alguns outros casos, a operação do grupo é indicada por $+$ e nesse caso os grupos $(G, +)$ são chamados grupos aditivos.

Então de posse da definição de um grupo abeliano, segue a preparação conceitual para os capítulos seguintes.

1.1 DEFINIÇÕES E EXEMPLOS DE ANÉIS, SUBANÉIS, CORPOS E SUBCORPOS

Definição 1.1. Um conjunto não vazio $\mathcal{A}$ munido de uma operação de adição "+"e de multiplicação "·", denotado por $(\mathcal{A}, +, \cdot)$, é chamado de **anel** quando as seguintes propriedades são satisfeitas:

i) $(\mathcal{A}, +)$ é um grupo abeliano.
ii) A multiplicação é associativa, ou seja, $x \cdot (y \cdot x) = (x \cdot y) \cdot z \ \ \forall x, y, z \in \mathcal{A}$.
iii) A multiplicação é distributiva sobre a adição, isto é,

$$x \cdot (y + z) \ = \ x \cdot y \ + \ x \cdot z \ \ e \ \ (x + y) \cdot z \ = \ x \cdot z \ + \ y \cdot z, \ \ \forall \ x, y, z \in \mathcal{A}.$$

Observação 1.1. Por questão de simplicidade, vamos denotar um anel $(\mathcal{A}, +, \cdot)$ simplesmente por $\mathcal{A}$, ficando subentendido as operações de soma e produto. Também escreveremos multiplicações do tipo ab ao invés de $a \cdot b$. Além disso, representamos o elemento neutro da adição de $\mathcal{A}$ por $0_{\mathcal{A}}$ ou simplesmente por 0, se não houver confusão de notação, de modo que para $a \in \mathcal{A}$ vale,

$$a + (-a) = 0_{\mathcal{A}}.$$

E também, dados $a, b \in \mathcal{A}$, a soma $a+(-b)$ será indicada por $a-b$. Com isso, $a-b = a+(-b)$.

Definição 1.2. Um anel $(\mathcal{A}, +, \cdot)$ é dito **comutativo** quando sua multiplicação for comutativa, ou seja, quando

$$ab = ba, \ \ \forall \ \ a, b \in \mathcal{A}.$$

Definição 1.3. Um anel $(\mathcal{A}, +, \cdot)$ é chamado **anel com unidade** quando sua multiplicação possui elememto neutro, isto é, quando existe $1_{\mathcal{A}} \in \mathcal{A}$ tal que

$$a \cdot 1_{\mathcal{A}} = 1_{\mathcal{A}} \cdot a = a, \qquad \forall \ a \in \mathcal{A}.$$

Se não houver confusão de notação, chamaremos $1_{\mathcal{A}}$ simplesmente de 1.

Definição 1.4. Um anel $(\mathcal{A}, +, \cdot)$ é dito anel **sem divisores de zero** se dados $a, b \in \mathcal{A}$, vale

$$a \cdot b = 0 \Rightarrow a = 0 \ \ ou \ \ b = 0.$$

Definição 1.5. Se $(\mathcal{A}, +, \cdot)$ é um anel comutativo, com unidade e sem divisores de zero, dizemos que $(\mathcal{A}, +, \cdot)$ é um **domínio de integridade**.

Definição 1.6. Se $(\mathcal{K}, +, \cdot)$ é um domínio de integridade e para $a \in \mathcal{K} - \{0\}$, existe $b \in \mathcal{K}$ tal que

$$ab = ba = 1,$$

dizemos que $(\mathcal{K}, +, \cdot)$ é um **corpo**.

Com efeito, considerando o conjunto $\mathcal{K}^*$ dos elementos não nulos de um corpo $\mathcal{K}$, temos que $\mathcal{K}^*$ é um grupo multiplicativo sob a multiplicação em $\mathcal{K}$. Isso se verifica, pois

$$U_{\bullet}(\mathcal{K}) = \{a \in \mathcal{K} \ : \ \text{existe } b \in \mathcal{K}, \text{com } a \cdot b = b \cdot a = 1\} = \mathcal{K}^*.$$

Portanto, um anel $\mathcal{K}$, comutativo com unidade, é um **corpo** quando $U_{\bullet}(\mathcal{K}) = \mathcal{K}^*$.

Exemplo 1.1. Os conjuntos $(\mathbb{Z},+,.),(\mathbb{Q},+,.),(\mathbb{R},+,.)$ *e* $(\mathbb{C},+,.)$ são anéis onde $+$ e $\cdot$ são a adição e multiplicação usuais. Em cada caso, a operação $\cdot$ é comutativa e 1 é o elemento neutro para esta operação. Destes são corpos $(\mathbb{Q},+,.),(\mathbb{R},+,.)$ *e* $(\mathbb{C},+,.)$.

Exemplo 1.2. O conjunto $\mathbb{Z}_n = \{\overline{0},\overline{1},\overline{2},...,\overline{n-1}\}$ é um anel munido da soma e produto a seguir

$$\begin{array}{rccc} + \ : & \mathbb{Z}_n \times \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & (\overline{m},\ \overline{n}) & \longmapsto & \overline{m+n} \end{array} \quad \text{e} \quad \begin{array}{rccc} \cdot \ : & \mathbb{Z}_n \times \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & (\overline{m},\ \overline{n}) & \longmapsto & \overline{m\cdot n} \end{array}.$$

Quando p é um número primo, os aneis $\mathbb{Z}_p$ são corpos.

Exemplo 1.3. Consideremos o conjunto $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} : a,\ b \in \mathbb{Z}\}$. Vamos definir as operações $+$ e $\cdot$ em $\mathbb{Z}[\sqrt{2}]$ da seguinte forma: dados os elementos $x = a_1 + b_1\sqrt{2}$ e $y = a_2 + b_2\sqrt{2}$, em que $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, então:

$$x + y = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$$

e

$$x \cdot y = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}.$$

Com essas operações, segue que $\mathcal{A} = \mathbb{Z}[\sqrt{2}]$ é um anel comutativo com unidade, sendo $0_A = 0 + 0\sqrt{2}$ (o número 0) e $1_A = 1 = 0\sqrt{2}$ (o número 1).

De forma geral se d é um inteiro que não é um quadrado perfeito, então o conjunto

$$\mathbb{Z}[\sqrt{d}] = \{a+b\sqrt{d} : a,\ b \in \mathbb{Z}\},$$

com operações análogas às do conjunto $\mathbb{Z}[\sqrt{2}]$, isto é, dados $x = a_1 + b_1\sqrt{d}$ e $y = a_2 + b_2\sqrt{d}$ em $\mathbb{Z}[\sqrt{d}]$,

$$x + y = (a_1 + a_2) + (b_1 + b_2)\sqrt{d} \quad e \quad x \cdot y = (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d},$$

é um anel comutativo com unidade.

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 $\mathbb{Z}[\sqrt{p}]$ e mais os anéis $\mathbb{Q}[\sqrt{p}]$ são exemplos de corpos.

Definição 1.7. Seja $\mathcal{A}$ um anel. Se existe $n \in \mathbb{N}$ tal que,

$$n \cdot a = 0_{\mathcal{A}}, \quad \forall\ a \in \mathcal{A},$$

então o menor número natural satisfazendo esta condição chama-se **característica** de $\mathcal{A}$. Caso não exista algum natural satisfazendo essa condição, então dizemos que $\mathcal{A}$ é de característica zero.

Indicaremos a característica m de um anel $\mathcal{A}$ por $car(\mathcal{A})$, isto é,

$$car(\mathcal{A}) = m.$$

Exemplo 1.4. Se $\mathcal{A}$ é qualquer um dos anéis $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, então $car(\mathcal{A}) = 0$. De fato, dado $a = 1$, temos:

$$n \cdot 1 = n \neq 0,$$

para qualquer $n \in \mathbb{N}$. Isto significa que não existe $m \in \mathbb{N}$ para o qual;

$$m \cdot a = 0,\ \forall\ a \in \mathcal{A}.$$

Definição 1.8. Seja $\mathcal{A}$ um anel e $\mathcal{B}$ um subconjunto não vazio de $\mathcal{A}$. Dizemos que $\mathcal{B}$ é um **subanel** de $\mathcal{A}$, se valem:
i) $x,\ y \in \mathcal{B} \Rightarrow x - y \in \mathcal{B}$.
ii) $x,\ y \in \mathcal{B} \Rightarrow x \cdot y \in \mathcal{B}$.

Exemplo 1.5. Temos que $n \cdot \mathbb{Z} = \{nk\ :\ k \in \mathbb{Z}\}$ 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 1.9. Um subanel $\mathcal{B}$ de um corpo $\mathcal{K}$ é chamado um **subcorpo** de $\mathcal{K}$ se dado $a \in \mathcal{B} - \{0\}$, existe $b \in \mathcal{B}$ tal que $ab = 1$.

Exemplo 1.6. 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 $\mathbb{R}$.

1.2 IDEAIS E ANÉIS QUOCIENTES

Definição 1.10. Seja $\mathcal{A}$ um anel. Um conjunto não vazio $\mathcal{I}$ de $\mathcal{A}$ é chamado **ideal** de $\mathcal{A}$ quando as seguintes condições são satisfeitas:

(a) $x - y \ \in \ \mathcal{I}, \quad \forall \ x, \ y \in \mathcal{I}.$

(b) $ax \in \mathcal{I}$ *e* $xa \in \mathcal{I}, \quad \forall \ a \in \mathcal{A} \ \ e \ \ \forall \ x \in \ \mathcal{I}.$

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

Seja $\mathcal{A}$ um anel comutativo. Consideremos os elementos fixos $a_1, \cdots, a_n \in \mathcal{A}$ e $\mathcal{I}$ o seguinte subconjunto de $\mathcal{A}$, construídos a partir desses elementos:

$$\mathcal{I} = \{x_1 \cdot a_1 + \cdots + x_n \cdot a_n : x_i \in \mathcal{A}, \ \forall \ i = 1, \cdots, n\}.$$

Vamos mostrar que $\mathcal{I}$ é um ideal de $\mathcal{A}$. Primeiro, notemos que $\mathcal{I}$ é não vazio, pois $0 = 0 \cdot a_1 + \cdots + 0 \cdot a_n \in \mathcal{I}$. Agora, sejam $x, \ y \in \mathcal{I}$, digamos

$$x = x_1 \cdot a_1 + \cdots + x_n \cdot a_n \quad \text{e} \quad y = y_1 \cdot a_1 + \cdots + y_n \cdot a_n,$$

em que $x_i, \ y_i \in \mathcal{I}$, para $i = 1, \cdots, n$. Desse modo,

$$x - y = (x_1 - y_1) \cdot a_1 + \cdots + (x_n - y_n) \cdot a_n \in \mathcal{I}.$$

Por fim, se $a \in \mathcal{A}$, então $ax = (ax_1) \cdot a_1 + \cdots + (ax_n) \cdot a_n \in \mathcal{I}$. Portanto, $\mathcal{I}$ é um ideal de $\mathcal{A}$, chamado ideal gerado por $a_1, \cdots, a_n$. Vamos indicar este ideal por: $< a_1, \cdots, a_n >$, ou seja,

$$< a_1, \cdots, a_n >= \{x_1 \cdot a_1 + \cdots + x_n \cdot a_n : x_i \in \mathcal{A}, \forall \ i = 1, \cdots, n\}.$$

Em particular, se $a \in \mathcal{A}$, o ideal

$$\mathcal{I} =< a >= \{x \cdot a : x \in \mathcal{A}\}$$

chama-se **ideal principal gerado** por a. É comum indicar também o ideal $\mathcal{I} =< a >$ por $a \cdot \mathcal{A}$.

Definição 1.11. Um domínio $\mathcal{D}$ é chamado **domínio de ideais principais** quando todos os ideais de $\mathcal{D}$ são principais.

O anel $\mathbb{Z}$ é um domínio de ideais principais.

Proposição 1.1. *Se $\mathcal{A}$ é um anel com unidade 1 e $\mathcal{J}$ é um ideal de $\mathcal{A}$ tal que $1 \in \mathcal{J}$, então $\mathcal{J} = \mathcal{A}$.*

Demonstração. De fato, primeiro note que $\mathcal{J} \subset \mathcal{A}$, pois $\mathcal{J}$ é ideal de A. Por outo lado, seja $x \in \mathcal{A}$. Como $\mathcal{J}$ é ideal e $1 \in \mathcal{J}$, então $x = x \cdot 1 \in \mathcal{J}$. Logo, $\mathcal{A} \subset \mathcal{J}$. Portanto $\mathcal{J} = \mathcal{A}$. ■

Definição 1.12. Sejam $\mathcal{A}$ um anel comutativo e $\mathcal{M}$ um ideal de $\mathcal{A}$, em que $\mathcal{M} \neq \mathcal{A}$. Diz-se que $\mathcal{M}$ é um **ideal maximal** quando os únicos ideais de $\mathcal{A}$ que contém $\mathcal{M}$ são $\mathcal{M}$ e $\mathcal{A}$. Equivalentemente, $\mathcal{M}$ é maximal quando para todo ideal $\mathcal{J}$ de $\mathcal{A}$ tal que $\mathcal{M} \subset \mathcal{J}$ *e* $\mathcal{M} \neq \mathcal{J}$, tem-se que $\mathcal{J} = \mathcal{A}$

Exemplo 1.7. O ideal $p \cdot \mathbb{Z} = \{pk \ : \ k \in \mathbb{Z}\}$ em $\mathbb{Z}$ com p primo é maximal. De fato, seja p primo e $\mathcal{J} = p \cdot \mathbb{Z}$. Vamos provar que $\mathcal{J}$ é um ideal maximal em $\mathbb{Z}$. Considere $\mathcal{I}$ um ideal de $\mathbb{Z}$ tal que

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

Pelo fato de todo ideal de $\mathbb{Z}$ ser principal, temos que existem inteiros n tais que $\mathcal{I} = n \cdot \mathbb{Z}$ Assim, $p \in p \cdot \mathbb{Z} \subset n \cdot \mathbb{Z}$, e daí segue $p = nk$ 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 $\mathcal{J} = \mathbb{Z}$ e se $n = \pm p$ vem que $\mathcal{I} = \mathcal{J}$.

Teorema 1.1. *Seja $\mathcal{K}$ um anel comutativo com unidade $1 \in \mathcal{K}$. Então as seguintes condições são equivalentes:*
i) $\mathcal{K}$ é um corpo;
ii) $\{0\}$ é um ideal maximal em $\mathcal{K}$;
iii) Os únicos ideais de $\mathcal{K}$ são os triviais.

Demonstração. i)⇒ ii). Seja $\mathcal{K}$ um corpo e seja $\mathcal{J}$ um ideal de $\mathcal{K}$ tal que $\{0\} \subset \mathcal{J} \subset \mathcal{K}$. Suponhamos $\mathcal{J} \neq \{0\}$. Assim existe $0 \neq a \in J$. Como K é um corpo existe $b \in K$ tal que $b \cdot a = 1$ e portanto $1 \in \mathcal{J}$. Da Proposição 1.1 segue que $\mathcal{J} = \mathcal{K}$.
ii) ⇒ iii). Segue imediatamente das definições.
iii) ⇒ i). Seja $0 \neq a \in \mathcal{K}$ e $\mathcal{I} = a \cdot \mathcal{K}$ o ideal principal de $\mathcal{K}$ gerado por a. Como $1 \in \mathcal{K}$, temos $a = 1.a \in \mathcal{I}$, nos diz que $\mathcal{I} \neq \{0\}$ e assim pela nossa hipótese, teremos $\mathcal{I} = \mathcal{K}$.
Daí segue, $1_{\mathcal{K}} \in \mathcal{K} = a \cdot \mathcal{K}$ donde existe $b \in \mathcal{K}$ tal que $1 = b \cdot a$. ■

Vamos agora definir a seguinte relação em $\mathcal{A}$:

$$\forall\ x,\ y \in \mathcal{A},\ x \equiv y (mod\ \mathcal{J}) \Leftrightarrow x - y \in \mathcal{J}.$$

Primeiramente vamos provar que $\equiv (mod\ \mathcal{J})$ define uma relação de equivalência em $\mathcal{A}$.
De fato, quaisquer que sejam $x,\ y,\ z \in \mathcal{A}$, temos
i) $x \equiv x (mod\ \mathcal{J})$ pois $0 = x - x \in \mathcal{J}$.
ii) $x \equiv y (mod\ J) \Rightarrow y \equiv x (mod\ \mathcal{J})$ pois se $x - y \in \mathcal{J}$ então $y - x = -(x - y) \in \mathcal{J}$.
iii) $x \equiv y (mod\ \mathcal{J})$ e $y \equiv z (mod\ \mathcal{J}) \Rightarrow x \equiv z (mod\ \mathcal{J})$ pois, $x - y \in \mathcal{J}$ e $y - z \in \mathcal{J} \Rightarrow$ $x - z = (x - y) + (y - z) \in \mathcal{J}$.

Denotaremos por $\overline{x}$ a **classe de equivalência de** $x \in A$ segundo a relação $\equiv (mod\ J)$. Assim,

$$\overline{x} = \{y \in \mathcal{A} \ : \ y \equiv x(mod\ \mathcal{J})\}.$$

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

Definiremos as seguintes operações em $\mathcal{A}/\mathcal{J}$

$$+ \ : \ \begin{array}{ccc} \mathcal{A}/\mathcal{J} \times \mathcal{A}/\mathcal{J} & \longrightarrow & \mathcal{A}/\mathcal{J} \\ (\overline{a},\ \overline{b}) & \longmapsto & \overline{a+b} \end{array} \text{ e } \cdot \ : \ \begin{array}{ccc} \mathcal{A}/\mathcal{J} \times \mathcal{A}/\mathcal{J} & \longrightarrow & \mathcal{A}/\mathcal{J} \\ (\overline{a},\ \overline{b}) & \longmapsto & \overline{a \cdot b} \end{array}.$$

Teorema 1.2. *Sejam $\mathcal{A}$ um anel e $\mathcal{I}$ um ideal de $\mathcal{A}$, e tomemos $x_1,\ x_2,\ y_1,\ y_2 \in \mathcal{A}$. Se $x_1 \equiv x_2\ (mod\ \mathcal{I})$ e $y_1 \equiv y_2\ (mod\ \mathcal{I})$, então:*

1. $\overline{x_1 + x_2} = \overline{x_2 + y_2}$ *ou* $(x_1 + y_1) + \mathcal{I} = (x_2 + y_2) + \mathcal{I}$.

2. $\overline{x_1 \cdot y_1} = \overline{x_2 \cdot y_2}$ *ou* $x_1 \cdot y_1 + \mathcal{I} = x_2 \cdot y_2 + \mathcal{I}$.

Demonstração. 1. Por hipótese, temos

$$x_1 = x_2 + a_1 \ \ e \ \ y_1 = y_2 + a_2$$

sendo $a_1,\ a_2 \ \in \mathcal{I}$. Portanto, somando membro a membro estas duas igualdades, segue que,

$$x_1 + y_1 = x_2 + y_2 + (a_1 + a_2).$$

Como $a_1 + a_2 \in \mathcal{I}$,

$$(x_1 + y_1) - (x_2 + y_2) \in \mathcal{I} \Leftrightarrow (x_1 + y_1) \equiv (x_2 + y_2)(mod\ \mathcal{I}) \Leftrightarrow \overline{x_1 + y_1} = \overline{x_2 + y_2}.$$

.

2. Usando as igualdades, obtemos

$$x_1 \cdot y_1 = (x_2 + a_1)(y_2 + a_2) = x_2y_2 + x_2a_2 + a_1y_2 + a_1a_2.$$

Como $\mathcal{I}$ é um ideal de $a_1,\ a_2 \in \mathcal{I}$, então $x_2a_2 + a_1y_2 + a_1a_2 \in \mathcal{I}$. Por isso,

$$x_1 \cdot y_1 \equiv (x_2y_2)(mod\mathcal{I}) \Leftrightarrow \overline{x_1 \cdot y_1} = \overline{x_2 \cdot y_2}.$$

■

Teorema 1.3. *Sejam $\mathcal{A}$ um anel e $\mathcal{I}$ um ideal de $\mathcal{A}$. Então*

$$+ : \mathcal{A}/\mathcal{I} \times \mathcal{A}/\mathcal{I} \to \mathcal{A}/\mathcal{I} \qquad \cdot : \mathcal{A}/\mathcal{I} \times \mathcal{A}/\mathcal{I} \to \mathcal{A}/\mathcal{I}.$$

$$e$$

$$(\overline{x}, \overline{y}) \mapsto \overline{x} + \overline{y} = \overline{x + y} \qquad (\overline{x}, \overline{y}) \mapsto \overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

Definem duas operações de adição e multiplicação sobre $\mathcal{A}/\mathcal{I}$. Além disso, $(\mathcal{A}/\mathcal{I}, +, \cdot)$ é um anel, chamado ***anel quociente*** *de $\mathcal{A}$ por $\mathcal{I}$.*

Demonstração. Primeiro vamos mostrar que os resultados destas operações independem dos representantes das classes. De fato, se $x_1,\ x_2,\ y_1,\ y_2 \in \mathcal{A}$ e $\overline{x_1} = \overline{x_2}$ e $\overline{y_1} = \overline{y_2}$, então $x_1 \equiv x_2 (mod\ \mathcal{I})$ e $y_1 \equiv y_2 (mod\ \mathcal{I})$. Pelo teorema anterior segue que

$$\overline{x_1 + y_1} = \overline{x_2 + y_2} \ \text{ e } \ \overline{x_1 \cdot y_1} = \overline{x_2 \cdot y_2}$$

Agora, vamos verificar apenas a existência do elemento neutro da adição de $\mathcal{A}/\mathcal{I}$, bem como a existência de inverso aditivo de cada $\overline{x} \in \mathcal{A}/\mathcal{I}$. Notemos que a classe $\overline{0}(0 = 0_{\mathcal{A}})$ é tal que,

$$\overline{x} + \overline{0} = \overline{0 + x} = \overline{x} = \overline{0} + \overline{x},\ \forall\ \overline{x} \in \mathcal{A}/\mathcal{I}$$

mas,

$$\overline{0} = 0 + \mathcal{I} = \mathcal{I}.$$

Por isso, o zero do anel $\mathcal{A}/\mathcal{I}$ é o próprio ideal $\mathcal{I}$. Agora, a classe $\overline{-x}$ satisfaz

$$\overline{x} + (\overline{-x}) = \overline{x + (-x)} = \overline{0} = \overline{(-x)} + \overline{x},$$

ou seja, $\overline{-x}$ é o inverso aditivo de $\overline{x}$ ■

Essas duas operações de adição e multiplicação sobre $\mathcal{A}/\mathcal{I}$ apresentadas neste teorema fazem de $(\mathcal{A}/\mathcal{I}, +, \cdot)$ um anel, chamado **anel quociente** de $\mathcal{A}$ por $\mathcal{I}$.

Teorema 1.4. *Sejam $\mathcal{A}$ um anel comutativo com unidade e $\mathcal{M}$ um ideal de $\mathcal{A}$. Então, $\mathcal{M}$ é maximal se, e somente se, $\mathcal{A}/\mathcal{M}$ é um corpo.*

Demonstração. Primeiro, suponhamos que $\mathcal{M}$ é maximal. Devemos mostrar que todo elemento não nulo $\overline{a} \in \mathcal{A}/\mathcal{M}$ é invertível (notemos que $\mathcal{A}/\mathcal{M}$ é comutativo com unidade). Seja $\overline{a} \in \mathcal{A}/\mathcal{M}$, com $\overline{a} \neq \overline{0}$, e tomemos o ideal $\mathcal{J} =< a >$. Assim, $\mathcal{M} + \mathcal{J}$ é um ideal de $\mathcal{A}$ que contém $\mathcal{M}$. Além disso, sendo $\overline{a} \neq \overline{0}$, então $a \notin \mathcal{M}$. Observe também que

$$\overline{a} = \mathcal{M} \Leftrightarrow a \in \mathcal{M}.$$

Como $a = a \cdot 1 \in \mathcal{J} \subset \mathcal{J} + \mathcal{M}$, segue que $\mathcal{J} + \mathcal{M} \neq \mathcal{M}$. Por isso, sendo $\mathcal{M}$ maximal e $\mathcal{M} \subset \mathcal{J} + \mathcal{M}$, concluímos que

$$\mathcal{J} + \mathcal{M} = \mathcal{A}.$$

Com isso, existem $x \in \mathcal{J}$ *e* $y \in \mathcal{M}$ tais que

$$1 = x + y,$$

pois $1 \in \mathcal{A}$. Mas, $x \in \mathcal{J}$ implica que $x = a \cdot b$, para algum $b \in \mathcal{A}$. Portanto,

$$\overline{1} = \overline{ab} + \overline{y} = \overline{ab} = \overline{0} = \overline{ab},$$

desde que $y \in \mathcal{M}$. A igualdade $1 = \overline{ab}$ nos diz que $\overline{a}$ é invertível e, por isso, $\mathcal{A}/\mathcal{M}$ é corpo. Reciprocamente, tomemos um ideal $\mathcal{J}$ de $\mathcal{A}$ tal que $\mathcal{M} \subset \mathcal{J}$ e $\mathcal{M} \neq \mathcal{J}$. Logo, existe $a \in \mathcal{J}$, com $a \notin \mathcal{M}$, de maneira que $\overline{a} \neq \overline{0}$. Como $\mathcal{A}/\mathcal{M}$ é um corpo, existe $\overline{b} \in \mathcal{A}/\mathcal{M}$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$. Daí,

$$\overline{a} \cdot \overline{b} = \overline{1} \Leftrightarrow ab \equiv 1(mod\ \mathcal{M}) \Leftrightarrow ab = 1 + m_0,$$

com $m_0 \in \mathcal{M}$, isto é,

$$1 = ab - m_0$$

Como $a \in \mathcal{J}$, então $ab \in \mathcal{J}$. Também, $m_0 \in \mathcal{M}$ implica que m_0 pertence a $\mathcal{J}$, pois $\mathcal{M} \subset \mathcal{J}$. Portanto, $1 \in \mathcal{J}$, ou seja, $\mathcal{J} = \mathcal{A}$. ■

1.3 HOMOMORFISMO DE ANÉIS

Definição 1.13. Sejam $\mathcal{A}$ *e* $\mathcal{B}$ anéis. Uma função $f : \mathcal{A} \longrightarrow \mathcal{B}$ chama-se **homomorfismo** de $\mathcal{A}$ *em* $\mathcal{B}$, quando as seguintes condições são satisfeitas:
i) $f(a + b) = f(a) + f(b), \ \ \forall\ a,\ b \in \mathcal{A}$.
ii) $f(a \cdot b) = f(a) \cdot f(b), \ \ \forall\ a,\ b \in \mathcal{A}$.

Sejam $\mathcal{A}$ e $\mathcal{B}$ dois anéis. Um homomorfismo $f : \mathcal{A} \longrightarrow \mathcal{B}$ bijetivo chama-se **isomorfismo**. Em particular, um isomorfismo $f : \mathcal{A} \longrightarrow \mathcal{A}$ é dito um automorfismo de $\mathcal{A}$. Quando existe um isomorfismo entre dois anéis $\mathcal{A}$ e $\mathcal{B}$, dizemos que estes são isomorfos e denotamos por $\mathcal{A} \simeq \mathcal{B}$.

Teorema 1.5. *Sejam $\mathcal{A}$ e $\mathcal{B}$ anéis e $f : \mathcal{A} \to \mathcal{B}$ um homomorfismo. Então:*
i) $Im(f) = \{f(a) \ : \ a \in \mathcal{A}\}$ é um subanel de $\mathcal{B}$.
ii) $ker(f) = \{a \in \mathcal{A} \ : \ f(a) = 0_{\mathcal{B}}\}$ é um ideal de $\mathcal{A}$ e f é injetiva se, e somente se, $ker(f) = \{0_{\mathcal{A}}\}$.
iii) Os anéis $\mathcal{A}/ker(f)$ e $Im\ (f)$ são isomorfos.

Demonstração. Vamos demonstrar o item *iii*). Para isso seja $f : \mathcal{A} \to \mathcal{B}$ um homomorfismo de anéis.Tomemos

$$\begin{gathered}\Psi : \mathcal{A}/Ker(f) \to Im(f).\\ x + Ker(f) \mapsto f(x)\end{gathered}$$

Observemos que Ψ está bem definida. De fato, se $\overline{x}, \overline{y} \in \mathcal{A}/Ker(f)$ são tais que $\overline{x} = \overline{y}$, então

$$x \equiv y(mod\ Ker(f)),$$

ou seja $x = y + a$, em que $a \in Ker(f)$. Assim, $f(a) = 0_{\mathcal{B}}$, de modo que

$$\begin{aligned}\Psi(\overline{x}) &= f(x) = f(y + a)\\ &= f(y) + f(a)\\ &= f(y)\\ &= \Psi(\overline{y}).\end{aligned}$$

Assim, Ψ está bem definida. Agora,

$$\Psi(\overline{x}) = \Psi(\overline{y}) \Rightarrow f(x) = f(y) \Rightarrow f(x - y) = 0_{\mathcal{B}}.$$

Portanto, $x - y \in Ker(f)$, isto é, $x = y + a$, para algum $a \in Ker(f)$. Com isso,

$$\overline{x} = \overline{y + a} = \overline{y} + \overline{a} = \overline{y},$$

pois $\overline{a} = \overline{0}$. Assim, Ψ é injetora. A função é claramente sobrejetora. Para finalizar, dados, $\overline{x}, \overline{y} \in \mathcal{A}/Ker(f)$, temos;

$$\begin{aligned}\Psi(\overline{x} + \overline{y}) &= \Psi(\overline{x + y})\\ &= f(x + y)\\ &= f(x) + f(y)\end{aligned}$$

$$\begin{aligned} &= \Psi(\overline{x}) + \Psi(\overline{y}) \\ e & \\ \Psi(\overline{x} \cdot \overline{y}) &= \Psi(\overline{x \cdot y}) \\ &= f(x \cdot y) \\ &= f(x) \cdot f(y) \\ &= \Psi(\overline{x}) \cdot \Psi(\overline{y}). \end{aligned}$$

Portanto, Ψ é um homomorfismo. Concluímos que Ψ é um isomorfismo e $\mathcal{A}/Ker(f) \simeq Im(f)$. ■

1.4 ANÉIS DE POLINÔMIOS

Definição 1.14. Seja $\mathcal{A}$ um anel qualquer. Um **polinômio sobre** $\mathcal{A}$ em uma variável X é uma soma infinita informal

$$f(X) = \sum_{i=0}^{\infty} a_i X_i = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n + \cdots,$$

em que $a_i \in \mathcal{A}$, para todo $i \in \mathbb{N} \cup \{0\}$ e $a_i \neq 0$ apenas para um número finito de valores de i, ou seja, existe $m \in \mathbb{N}$ tal que $a_j = 0$ para qualquer $j \geq m$. Os elementos $a_i \in \mathcal{A}$ do polinômio $f(X)$ são ditos **coeficientes** de $f(X)$.

O conjunto de todos os polinômios sobre o anel $\mathcal{A}$ será denotado por $\mathcal{A}[X]$.

Dados dois polinômios

$$p(X) = a_0 + a_1 X + ... + a_m X^m + ... \quad e \quad q(X) = b_0 + b_1 X + ... + b_k X^k + ...$$

em $\mathcal{A}[X]$, dizemos que $p(X)$ e $q(X)$ são **iguais** se, e somente se, $a_i = b_i$ em $\mathcal{A}$, $\forall\ i \in \mathbb{N}$.

Se $p(X) = 0 + 0X + ... + 0X^m + ...$, indicaremos $p(X)$ por 0 e o chamaremos de polinômio **identicamente nulo** sobre $\mathcal{A}$. Assim um polinômio

$$p(X) = a_0 + a_1 X + ... + a_m X^m + ...$$

sobre $\mathcal{A}$ é identicamente nulo se, e somente se, $a_i = 0 \in \mathcal{A},\ \forall \in \mathbb{N}$.

Se $a \in \mathcal{A}$, indicaremos por a ao polinômio $p(X) = a_0 + a_1 X + ... + a_n X^n + ...$ onde $a_0 = a$, e $a_i = 0,\ \forall\ i \geq 1$. Chamaremos ao polinômio $p(X) = a,\ a \in \mathcal{A}$, de **polinômio constante** a.

Se $p(X) = a_0 + a_1 X + ... + a_n X^n + ...$ 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 indicaremos por $\partial p(X) = n$. O coeficiente a_n é

chamado de **coeficiente líder** de $p(X)$. Além disso, se $\mathcal{A}$ tem unidade 1 e $a_n = 1$, então $p(X)$ é dito **polinômio mônico**.

Por exemplo, se $p(X) = 2 + x - x^3 + x^4 \in \mathbb{Z}[X]$, então $\partial p(X) = 4$, temos também que $p(X)$ é mônico, pois $a_4 = 1$.

Consideremos agora $f(X)$ e $g(X)$, digamos

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n + \cdots$$
e
$$g(X) = b_0 + b_1X + b_2X^2 + \cdots + b_mX^m + \cdots$$

dois polinômios em $\mathcal{A}[X]$. Define-se **soma** de $f(X)$ e $g(X)$ indicada por $f(X) + g(X)$ da seguinte forma:

$$f(X) + g(X) = \sum_{i=0}^{\infty} c_iX^i$$

em que $c_i = a_i + b_i$, para todos os valores de i.

A **multiplicação** de $f(X)$ e $g(X)$, denotada por $f(X) \cdot g(X)$, é definida por

$$f(X) \cdot g(X) = \sum_{i=0}^{\infty} d_iX_i,$$

sendo

$$d_i = \sum_{j=0}^{\infty} a_j \cdot b_{i-j} = \sum_{j+l=i \atop j,l\geq 0} a_j \cdot b_l,$$

Com as operações de soma e multiplicação denifidas, $(\mathcal{A}[X], +, \cdot)$ é um anel, o anel de polinômios sobre $\mathcal{A}$. De fato, é imediato verificar que $(\mathcal{A}[X], +, \cdot)$ é um grupo abeliano, no qual o elemento neutro da soma é o polinômio nulo $0 = \sum_{i\geq 0} 0X^i$, enquanto o inverso aditivo de $f(X) = \sum_{i=o}^{n} a_iX_i \in \mathcal{A}[X]$ é o polinômio $-f(X) = \sum_{i=0}^{n}(-a_i)X^i \in \mathcal{A}[X]$. A propriedade que demostraremos agora é associatividade da multiplicação, o que se exige um pouco de habilidade com as propriedades se somatório. Sejam $f(X),\ g(X),\ h(X) \in \mathcal{A}[X]$, digamos:

$$f(X) = \sum_{i=0}^{\infty} a_iX^i,\ g(X) = \sum_{i=0}^{\infty} b_jX^j \quad \text{e} \quad h(X) = \sum_{i=0}^{\infty} c_kX^k.$$

Então,

$$\begin{aligned}
[f(X)\cdot g(X)]\cdot h(X) &= \left[\left(\sum_{i=0}^{\infty} a_i X^i\right)\cdot\left(\sum_{i=0}^{\infty} b_j X^j\right)\right]\cdot\left(\sum_{i=0}^{\infty} c_k X^k\right)\\
&= \left[\left(\sum_{i=0}^{n} a_i b_{n-i}\right) X^n\right]\cdot\left(\sum_{i=0}^{\infty} c_k X^k\right)\\
&= \sum_{s=0}^{\infty}\left[\sum_{n}^{s}\left(\sum_{i=0}^{n} a_i b_{n-i}\right) c_{s-n}\right] X^s\\
&= \sum_{s=0}^{\infty}\left(\sum_{i+j+k=s} a_i b_j c_k\right) X^s\\
&= \sum_{s=0}^{\infty}\left[\sum_{m=0}^{s} a_{s-m}\left(\sum_{i=0}^{m} b_j c_{m-j}\right)\right] X^s\\
&= \left(\sum_{i=0}^{\infty} a_i X^i\right)\cdot\left[\sum_{m=0}^{\infty}\left(\sum_{j=0}^{m} b_j c_{m-j}\right)\right] X^m\\
&= \left(\sum_{i=0}^{\infty} a_i X^i\right)\cdot\left[\left(\sum_{j=0}^{\infty} b_j X^j\right)\cdot\left(\sum_{k=0}^{\infty} c_k X^k\right)\right]\\
&= f(X)\cdot[g(X)\cdot h(X)].
\end{aligned}$$

Assim, a multiplicação é associativa. E portanto, temos o anel $(\mathcal{A}[X], +, \cdot)$ dos polinômios com coeficientes em $\mathcal{A}[X]$ e na variável X.

Definição 1.15. Seja $\mathcal{A}$ um anel comutativo com unidade e sejam $f(X),\ g(X) \in \mathcal{A}[X]$. Dizemos que $g(X)$ **divide** $f(X)$ ou que $f(X)$ é **divisível** por $g(X)$, denotado por $g(X) \mid f(X)$, quando existe $q(X) \in \mathcal{A}[X]$ tal que

$$f(X) = g(X)\cdot q(X).$$

Caso contrário, dizemos que $g(X)$ não divide $f(X)$ em $\mathcal{A}[X]$ e denotamos por $g(X) \not| f(X)$.

Por exemplo, em $\mathbb{Z}[X]$, temos que o polinômio $g(X) = 1 + 3X + X^3$ divide $f(X) = 3 + 10X + 3X^2 + 3^3 + X^4$, pois

$$f(X) = (3 + x)\cdot(1 + 3X + X^3).$$

Proposição 1.2. *Para quaisquer $f(X),\ g(X)$ e $h(X)$ em $\mathcal{A}[X]$, valem as propriedades:*

(1) $f(X)|f(X)$;

(2) Se $g(X)|h(X)$ e $h(X)|f(X)$, então $g(X)|f(X)$;

(3) Se $g(X)|f(X)$, então $g(X)|f(X)\cdot h(X)$;

(4) Se $g(X)|f(X)$ e $g(X)|h(X)$, então $g(X)|(f(X)\cdot h_1(X)+h(X)\cdot h_2(X))$, $\forall\, h_1(X),\ h_2(X) \in \mathcal{A}[X]$.

Demonstração. Vamos demonstrar apenas a propriedade (4). Por hipótese, temos que:

$$f(X) = g(X) \cdot q_1(X) \text{ e } h(X) = g(X) \cdot q_2(X),$$

em que $q_1(X),\ q_2(X) \in \mathcal{A}[X]$. Logo, se $h_1(X),\ h_2(X) \in \mathcal{A}[X]$, então

$$f(X) \cdot h_1(X) = g(X) \cdot (h_1(X) \cdot q_1(X)) \text{ e}$$
$$h(X) \cdot h_2(X) = g(X) \cdot (h_2(X) \cdot q_2(X)).$$

Somando membro a membro estas duas últimas igualdades obtemos

$$f(X) \cdot h_1(X) + h(X) \cdot h_2(X) = g(X) \cdot (h_1(X) \cdot q_1(X) + h_2(X) \cdot q_2(X)).$$

Como

$$h_1(X) \cdot q_1(X) + h(X) \cdot h_2(X) \cdot q_2(X) \in \mathcal{A}[X], \text{ segue que}$$
$$g(X) | f(X) \cdot h_1(X) + h(X) \cdot h_2(X).$$

■

Teorema 1.6. *(Algoritmo da Divisão) Sejam $f(X),\ g(X) \in \mathcal{A}[X]$ e $g(X) \neq 0$. Então existem únicos $q(X),\ r(X) \in \mathcal{A}[X]$ tais que:*

$$f(X) = q(X) \cdot g(X) + r(X),$$

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

Demonstração. Sejam $f(X) = a_0 + a_1X + ... + a_nX^n$ e $g(X) = b_0 + b_1X + ... + b_mX^m$, com $\partial g(X) = m$.
(Existência):
Se $f(X) = 0$, basta tomar $q(X) = r(X) = 0$. Suponhamos $f(X) \neq 0$. Assim $\partial f(X) = n$. 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

$$f(X) = a_n b_m^{-1} X^{n-m} \cdot g(X) + f_1(X).$$

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

$$f(X) = a_0 b_0^{-1} g(X)$$

e basta tomar $q(X) = a_0 b_0^{-1}$ e $r(X) = 0$. Pela igualdade $f_1(X) = f(X) - a_n b_m^{-1} X^{n-m} g(X)$ 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:

$$f(X) = (q_1(X) + a_n b_m^{-1} X^{n-m}) g(X) + r_1(X)$$

e portanto tomando $q(X) = q_1(X) + a_n b_m^{-1} X^{n-m}$ 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 $\partial r(X) < \partial g(X)$.
(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,

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

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 segue que

$$r_1(X) = f(X) - q_1(X) g(X) = f(X) - q_2(X) g(X) = r_2(X).$$

■

Teorema 1.7. *Se $\mathcal{K}$ é um corpo, então $\mathcal{K}[X]$ é um domínio de ideais principais.*

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

Definição 1.16. Sejam $\mathcal{K}$ um corpo e $f(X),\ g(X) \in \mathcal{K}[X]$, com $f(X) \neq 0$ ou $g(X) \neq 0$. Dizemos que um polinômio $d(X) \in \mathcal{K}[X]$ é um **máximo divisor comum** de $f(X)$ e $g(X)$ quando as condições seguintes são satisfeitas:

(a) $d(X) \mid f(X)$ e $d(X) \mid g(X)$.

(b) Se $h(X) \in \mathcal{K}[X]$ é tal que $h(X)|f(X)$ e $h(X) \mid h(X)$, então $h(X) \mid d(X)$.

Teorema 1.8. *(Existência de MDC) Sejam $\mathcal{K}$ um corpo e $f(X),\ g(X) \in \mathcal{K}[X]$, com $f(X) \neq 0$ ou $g(X) \neq 0$. Então, existe máximo divisor comum $d(X)$ de $f(X)$ e $g(X)$. Além disso, existem $h_1(X),\ h_2(X)\ \in \mathcal{K}[X]$, tais que:*

$$d(X) = f(X) \cdot h_1(X) + g(X) \cdot h_2(X).$$

Demonstração. Tomemos o ideal $\mathcal{I}$ em $\mathcal{K}[X]$ gerado por $f(X)$ e $g(X)$, isto é,

$$\mathcal{I} =< f(X), g(X) >= \{f(X) \cdot h_1(X) + g(X) \cdot h_2(X) :\ h_1(X),\ h_2(X) \in \mathcal{K}[X]\}.$$

Sendo $\mathcal{K}[X]$ um domínio de ideais principais, existe $d(X) \in \mathcal{K}$ de modo que $\mathcal{I} =< d(X) >$. Além disso, como $f(X) \in \mathcal{I} =< d(X) >$, pois $\mathcal{K}[X]$ tem unidade, então $f(X) = d(X) \cdot q(X)$ para algum $q(X) \in \mathcal{K}[X]$. Logo, $d(X)$ divide $f(X)$. Da mesma forma, $d(X)$ divide $g(X)$. Para outra parte, notemos primeiramente que $d(X) \in < d(X) >=< f(X),\ g(X) >$. Assim, existem $h_1(X), h_2(X) \in \mathcal{K}[X]$ de maneira que

$$d(X) = f(X) \cdot h_1(X) + g(X) \cdot h_2(X).$$

Supondo agora $h(X) \in \mathcal{K}[X]$ divisor de $f(X)$ e $g(X)$, então a igualdade acima nos mostra que $h(X)$ dividirá $d(X)$. Logo $d(X)$ é um MDC de $f(X)$ e $g(X)$. ■

Definição 1.17. Sejam $\mathcal{K}$ um corpo e $p(X) \in \mathcal{K}[X]$. Dizemos que $p(X)$ é um **polinômio irredutível** em $\mathcal{K}[X]$ ou **irredutível** em $\mathcal{K}$ quando as seguintes condições são satisfeitas:

(a) $\partial p(X) \geq 1$ (p(X) não é um polinômio constante).

(b) Se $f(X),\ g(X) \in \mathcal{K}[X]$ são tais que

$$p(X) = f(X) \cdot g(X),$$

então $\partial f(X) = 0$ ou $\partial g(X) = 0$, isto é, $f(X)$ ou $g(X)$ é um polinômio constante. Um polinômio $f(X) \in \mathcal{K}[X]$, com $\partial p(X) \geq 1$, que não é irredutível em $\mathcal{K}[X]$, é chamado **redutível** em $\mathcal{K}[X]$ ou **redutível** sobre $\mathcal{K}$.

Um polinômio $p(X) \in \mathcal{F}[X]$ pode ser irredutível sobre um corpo $\mathcal{F}$, mas redutível sobre uma extensão $\mathcal{K}$ de $\mathcal{F}$, isto é, sobre um corpo $\mathcal{K}$, com $\mathcal{F} \subset \mathcal{K}$.

Exemplo 1.8. O polinômio $p(X) = -3X + X^2 \in \mathbb{Q}[X]$ é irredutível sobre $\mathbb{Q}$. De fato, primeiro, temos que $\partial p(X) \geq 1$. Agora, supondo que

$$-3 + x^2 = (a_0 + a_1X) \cdot (b_0 + b_1X),$$

com $a_0,\ a_1,\ b_0, b_1 \in \mathbb{Q},\ a_1 \neq 0$ e $b_1 \neq 0$. Assim, $\alpha = \dfrac{-a_0}{a_1}$ é raiz de $h_1(X) = a_0 + a_1X$. Por isso, $p(\alpha) = 0$, isto é,

$$\frac{a_0}{a_1} = \pm\sqrt{3}$$

o que é uma contradição, pois $\sqrt{3}$ é irracional. Entretanto, $p(X) = -3 + X^2$ é redutível sobre $\mathbb{R}$, desde que

$$p(X) = (X - \sqrt{3}) \cdot (X + \sqrt{3}).$$

Mais geralmente, se $p > 0$ é um número primo, então $p(X) = -p + X^2$ é irredutível sobre $\mathbb{Q}$, mas sempre redutível sobre $\mathbb{R}$.

Exemplo 1.9. Todo polinômio $p(X) \in \mathcal{K}[X]$, com $\partial p(X) = 1$, é irredutível sobre $\mathcal{K}$. De fato, tomemos $p(X) = a_0 + a_1X \in \mathcal{K}[X]$, em que $a_1 \neq 0$, e $f(X),\ g(X) \in \mathcal{K}[X]$ tais que $p(X) = f(X) \cdot g(X)$. Logo,

$$1 = \partial f(X) + \partial g(X),$$

de modo que $\partial f(X) = 0$ ou $\partial g(X) = 0$. Por isso, $p(X)$ é irredutível.

Vamos agora considerar o conceito de polinômio irredutível em $\mathcal{K}[X]$, para um corpo $\mathcal{K}$, e estudar sua relação com ideais maximais.

Teorema 1.9. *Sejam $\mathcal{K}$ um corpo e $p(X) \in \mathcal{K}[X]$. Então, as seguintes afirmações são equivalentes:*

(1) $p(X)$ é irredutível.

(2) $< p(X) >$ é um ideal maximal em $\mathcal{K}[X]$.

(3) $\dfrac{\mathcal{K}[\mathcal{X}]}{< p(X) >}$ é um corpo.

Demonstração. Primeiro é fácil notar que as implicações (2) $\Leftrightarrow$ (3) seguem diretamente do Teorema 1.4. Por isso, vamos provar as equivalências (1) $\Leftrightarrow$ (2).
(1) $\Rightarrow$ (2) Suponhamos que $p(X)$ é irredutível sobre $\mathcal{K}$. Por definição,

$$< p(X) >= \{f(X) \cdot p(X) : f(X) \in \mathcal{K}[X]\}.$$

Primeiro, observemos que $\partial p(X) \geq 1$. Então $< p(X) > \neq \mathcal{K}[X]$. Agora, seja $\mathcal{I}$ um ideal de $\mathcal{K}[X]$ tal que $< p(X) > \subset \mathcal{I}$. Provemos que $\mathcal{I} =< p(X) >$ ou $\mathcal{I} = \mathcal{K}[X]$. Como $\mathcal{K}[X]$ é um

domínio de ideias principais, então existe $h(X) \in \mathcal{K}[X]$ de maneira que $\mathcal{I} =< h(X) >$. Assim, desde que $p(X) \in < p(X) > \subset \mathcal{I}$ (note que $p(X) = 1 \cdot p(X)$), existe $g(X) \in \mathcal{K}[X]$ tal que

$$p(X) = g(X) \cdot h(X).$$

Como $p(X)$ é irredutível, então $\partial g(X) = 0$ ou $\partial h(X) = 0$, isto é, $g(X) = a \in \mathcal{K}^*$ ou $h(X) = b \in \mathcal{K}^*$, se $g(X) = a \in \mathcal{K}^*$. Então, segue que

$$h(X) = a^{-1} \cdot p(X),$$

de modo que todo múltiplo de $h(X)$ é também múltiplo de $p(X)$. Formalmente,

$$\mathcal{I} =< h(X) > \subset < p(X) >,$$

o que mostra que $\mathcal{I} =< p(X) >$.

Se $h(X) = b \in \mathcal{K}^*$, então $h(X) \in U_\bullet(\mathcal{K}[X])$, de maneira que $< h(X) > = \mathcal{K}[X]$. Portanto, $< p(X) >$ é maximal.

(2) $\Rightarrow$ (1) Consideremos $< p(X) >$ um ideal maximal em $\mathcal{K}[X]$. Logo, $< p(X) > \neq \mathcal{K}[X]$ e, por conseguinete, $\partial p(X) \geq 1$. Tomemos $g(X),\ h(X) \in \mathcal{K}[X]$ tais que

$$p(X) = g(X) \cdot h(X).$$

Vamos mostrar que $g(X) = a \in \mathcal{K}^*$ ou $h(X) = b \in \mathcal{K}^*$. Obtemos de forma imediata que

$$< p(X) > \subset < h(X) > .$$

Mas, como $p(X)$ é maximal, segue que $< p(X) > = < h(X) >$ ou $< h(X) >= \mathcal{K}[X]$. Se $< p(X) > = < h(X) >$, então $h(X) \in < p(X) >$, ou seja, existe $f(X) \in \mathcal{K}[X]$, com

$$h(X) = f(X) \cdot p(X).$$

Logo,

$$p(X) = g(X) \cdot f(X) \cdot p(X).$$

Como $p(X) \neq 0$ e $\mathcal{K}[X]$ é um domínio, segue que:

$$1 = g(X) \cdot f(X),$$

ou seja, $g(X) \in U_\bullet(\mathcal{K}[X])$, de modo que $g(X) = a \in \mathcal{K}^*$ é um polinômio constante.

Se $< h(X) > = \mathcal{K}[X]$, segue imediato que $h(X) = b \in \mathcal{K}^*$, pois existe $q(X) \in \mathcal{K}[X]$ tal que

$$1 = h(X) \cdot q(X).$$

Portanto, $p(X)$ é irredutível. ■

Teorema 1.10. *(Fatoração Única) Se $\mathcal{K}$ é um corpo, então todo polinômio não constante em $\mathcal{K}[X]$ se escreve de maneira única, a menos da ordem dos fatores e de um invertível em $\mathcal{K}$, como produto de polinômios irredutíveis em $\mathcal{K}[X]$.*

Demonstração. Seja $f(X) \in \mathcal{K}[X]$ um polinômio não constante.
(Existência da fatoração): Se $f(X)$ é irredutível, o resultado segue imediato. Consideremos, pois, $f(X)$ redutível e provemos o resultado por indução sobre $\partial f(X) = n$.

Se $n = 1$, então $f(X)$ é claramente irredutível, conforme o exemplo apresentado. Suponhamos por hipótese de indução, que o resultado seja válido para todo polinômio de grau até $n-1$. Sendo $f(X)$ redutível, existem $g(X),\ h(X) \in \mathcal{K}[X]$ tais que

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

em que $0 < \partial g(X),\ \partial h(X) < n$. Logo, por hipótese de indução, existem polinômios irredutíveis

$$p_1(X), p_2(X), \cdots, p_t(X), p_{t+1}(X), \cdots, p_r(X) \in \mathcal{K}[X]$$

para os quais

$$g(X) = p_1(X) \cdots p_t(X) \quad \text{e} \quad h(X) = p_{t+1}(X) \cdots p_r(X).$$

Desse modo, obtemos

$$f(X) = p_1(X) \cdots p_r(X).$$

Isso mostra a existência da fatoração.
(Unicidade da fatoração): Suponhamos que

$$f(X) = p_1(X) \cdots p_r(X) = q_1(X) \cdots q_s(X),$$

sendo $p_i(X)$ e $q_j(X)$ polinômios irredutíveis em $\mathcal{K}[X]$. Para cada $i = 1, \cdots, r$ e cada $j = 1, \cdots, s$, temos

$$p_1(X) \mid q_1(X) \cdots q_s(X),$$

e como $p_1(X)$ é irredutível, segue que $p_1(X) \mid q_j(X)$ para algum j. Sem perda de generalidade, podemos supor que $p_1(X) \mid q_1(X)$. Como $q_1(X)$ é também irredutível, então

$$q_1(X) = \mu_1 \cdot p_1(X),$$

em que $\mu_1 \in \mathcal{K}^*$. E assim fazendo as devidas substituições, obtemos

$$p_1(X) \cdot p_2(X) \cdots p_r(X) = \mu_1 \cdot p_1(X) \cdot q_2(X) \cdots q_s(X),$$

de modo que

$$p_2(X) \cdots p_r(X) = \mu_1 \cdot q_2(X) \cdots q_s(X),$$

pois $\mathcal{K}[X]$ é um domínio. Da mesma forma, podemos supor que $q_2(X) = \mu_2 \cdot p_2(X)$ com $\mu_2 \in \mathcal{K}^*$, o que implica em

$$p_3(X) \cdots p_r(X) = \mu_1 \cdot \mu_2 \cdot q_3(X) \cdots q_s(X).$$

Continuando este processo e supondo que $s \geq r$, então

$$1 = \mu_1 \cdot \mu_2 \cdots \mu_r \cdot q_{r+1}(X) \cdots q_s(X).$$

Mas isso só é possível quando $r = s$, de maneira que

$$1 = \mu_1 \cdot \mu_2 \cdots \mu_r.$$

Assim, os irredutíveis $p_i(X)$ e $g_j(X)$ são os mesmos, diferentes possilvelmente pela ordem surgem nas fatorações e por um invertível em $\mathcal{K}$. ■

Definição 1.18. Um corpo $\mathcal{K}$ é dito **algebricamente fechado** se todo polinômio $f(X) \in \mathcal{K}[X]$, com $\partial f(X) \geq 1$, tem uma raiz em $\mathcal{K}$.

Exemplo 1.10. O corpo dos números reais $\mathbb{R}$ não é algebricamente fechado, pois o polinômio $f(X) = 1 + X^2 \in \mathbb{R}[X]$ não possui raiz em $\mathbb{R}$.

2 EXTENSÕES DE CORPOS

Neste capítulo apresentamos alguns resultados sobre Extensões de Corpos os quais são fundamentais para o entendimento do capítulo posteior.

Definição 2.1. Um corpo $\mathcal{K}$ é dito uma **extensão** de $\mathcal{F}$ quando $\mathcal{F}$ é um subcorpo de $\mathcal{K}$.

Vamos usar os símbolos $\mathcal{K} \supset \mathcal{F}$ ou $\mathcal{F} \subset \mathcal{K}$ para indicar que $\mathcal{K}$ é uma extensão de $\mathcal{F}$.

Por exemplo, $\mathbb{R}$ é uma extensão de $\mathbb{Q}$ e $\mathbb{C}$ é uma extensão de $\mathbb{R}$.

Teorema 2.1. *(Kronecker) Sejam $\mathcal{F}$ um corpo e $f(X)$ um polinômio em $\mathcal{F}[X]$, com $\partial f(X) \geq 1$. Então, existem uma extensão $\mathcal{K}$ de $\mathcal{F}$ e um elemento $\alpha \in \mathcal{K}$ tais que $f(\alpha) = 0$.*

Demonstração. De acordo com o Teorema 1.10, existe um polinômio irredutível $p(X)$ em $\mathcal{F}[X]$ tal que $p(X)$ divide $f(X)$. Pelo Teorema 1.9, o anel quociente $\frac{\mathcal{F}[X]}{<p(X)>}$ é um corpo. Consideramos agora a função

$$\begin{array}{c} \varphi : \mathcal{F} \to \dfrac{\mathcal{F}[X]}{< p(X) >} \\ a \mapsto a + < p(X) > . \end{array}$$

É imediato verificar que φ é um homomorfismo de corpos. Agora, se $a,\ b \in \mathcal{F}$ são tais que $\varphi(a) = \varphi(b)$, então

$$a + < p(X) > = b + < p(X) >,$$

isto é, $a - b \in < p(X) >$. Assim, $a - b \in \mathcal{F}$, então devemos necessariamente ter $a - b = 0$ ou seja, $a = b$, de modo que φ é injetora. Dessa forma,

$$\mathcal{F} \simeq \varphi(\mathcal{F}),$$

ou seja, o corpo $\mathcal{F}$ é isomorfo ao subcorpo $\varphi(\mathcal{F})$ de $\frac{\mathcal{F}[X]}{<p(X)>}$. Logo, por meio do homomorfismo φ, identificamos $\mathcal{F}$ como o subcorpo

$$Im(\varphi) = \mathcal{K}_1 = \{a + < p(X) > : a \in \mathcal{F}\}$$

de $\frac{\mathcal{F}[X]}{<p(X)>}$. Desse modo, podemos considerar $\frac{\mathcal{F}[X]}{<p(X)>}$ como uma extensão de $\mathcal{F}$.

Falta mostrar agora que esiste $\alpha \in \mathcal{K}$ tal que $p(\alpha) = 0$. Sabemos que em $\mathcal{K}$ a classe $\overline{p(X)}$ é tal que $\overline{p(X)} = \overline{0}$. Logo, sendo $p(X) = a_0 + a_1 X + \cdots + a_n X^n$, temos

$$\overline{p(X)} = \overline{a_0 + a_1X + \cdots + a_nX^n} = \overline{0}$$

isto é,

$$\overline{a_0} + \overline{a_1}\overline{X} + \cdots + \overline{a_n}\overline{X^n} = \overline{0},$$

em que $\overline{X} = X + < p(X) > \in \mathcal{K}$. Isso mostra que $\alpha = X + < p(X) >$ pertencente a $\mathcal{K}$ é uma raíz de $p(X) \in \mathcal{F}[X]$. ■

Definição 2.2. Um elemento $\alpha \in \mathcal{K} \supset \mathcal{F}$ é dito **algébrico sobre** $\mathcal{F}$ quando existe $f(X) \in \mathcal{F}[X] - \{0\}$ tal que $f(\alpha) = 0$. Ao contrário disso, α é dito **transcedente sobre** $\mathcal{F}$.

Definição 2.3. Um elemento $\alpha \in \mathbb{C}$ algébrico sobre $\mathbb{Q}$ é dito número algébrico. Caso contrário, α é dito número transcedente.

Exemplo 2.1. Como todo corpo é um extensão si próprio, então todo elemento $\alpha \in \mathcal{F}$ é algébrico sobre $\mathcal{F}$, desde que α é raiz de $f(X) = X - \alpha \in \mathcal{F}[X]$.

Exemplo 2.2. Desde que $\mathbb{R}$ é uma extensão de $\mathbb{Q}$, então para um número primo $p > 0$, temos que $\alpha = \sqrt{p} \in \mathbb{R}$ é algébrico sobre $\mathbb{Q}$, pois α é raiz do polinômio $f(X) = x^2 - p \in \mathbb{Q}[X]$. Também, $\mathbb{C}$ é uma extensão de $\mathbb{Q}$ e $\beta = i$ é algébrico sobre $\mathbb{Q}$, pois β é raiz de $g(X) = X^2 + 1 \in \mathbb{Q}[X]$.

Exemplo 2.3. O elemento $\alpha = \sqrt{1 + \sqrt{5}} \in \mathbb{R}$ é tal que $\alpha^2 - 1 = \sqrt{5}$, ou seja,

$$\alpha^4 - 2\alpha - 4 = 0$$

Por isso, α é raiz do polinômio $f(X) = -4 - 2X + X^4 \in \mathbb{Q}[X]$. Logo, α é algébrico sobre $\mathbb{Q}$.

Exemplo 2.4. O número π é um elemento transcedente. O número de Euller $e \approx 2,718281...$, também é um elemento transcedente.

Exemplo 2.5. Números de Liouville.
Um número real x, é dito número de Liouville se, para todo inteiro positivo n existirem inteiros p e q tais que:

$$0 < \left| x - \frac{p}{q} \right| < \frac{1}{q^n},\ q > 1.$$

Todos os número de Liouville são elementos transcedentes.

Observação 2.1. Sendo $\alpha \in \mathcal{K} \supset \mathcal{F}$ algébrico sobre $\mathcal{F}$, então existe $f(X) \in \mathcal{F}[X] - \{0\}$ tal que $f(\alpha) = 0$. Com efeito, considere pois

$$f(X) = a_0 + a_1X + ... + a_{n-1}X^{n-1} + a_nX^n,$$

com $a_n \neq 0$. Assim, $a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} + a_n\alpha^n = 0$. Como $\mathcal{F}$ é um corpo, então dividindo a ultima igualdade por a_n obtemos:

$$\frac{a_0}{a_n} + \frac{a_1}{a_n}\alpha + ... + \frac{a_{n-1}}{a_n}\alpha^{n-1} + \alpha^n = 0.$$

Assim, podemos dizer que α também é raiz do polinômio mônico

$$g(X) = \frac{a_0}{a_n} + \frac{a_1}{a_n}X + ... + \frac{a_{n-1}}{a_n}X^{n-1} + X^n.$$

Ademais, observe que o grau de $F(X)$ e de $g(X)$ são iguais.

Teorema 2.2. *Sejam $\alpha \in \mathcal{K} \supset \mathcal{F}$ algébrico sobre $\mathcal{F}$. Então, existe um único polinômio irredutível $p(X)$ em $\mathcal{F}[X]$ de menor grau tal que $p(\alpha) = 0$.*

Demonstração. Sendo α algébrico sobre $\mathcal{F}$, então pela obeservação acima, existe um polinômio mônico $g(X) \in \mathcal{F}[X]$ tal que $g(\alpha) = 0$. Agora, seja $p(X) \in \mathcal{F}[X]$ mônico de menor grau, com $p(\alpha) = 0$. Assim, é notório que $p(X)$ é irredutível,pois caso contrário, existem polinômios mônicos $h(X),\ q(X) \in \mathcal{F}[X]$ tais que

$$p(X) = h(X) \cdot q(X) \text{ com } 0 < \partial h(X),\ \partial q(X) < \partial p(X).$$

Desse modo, $h(\alpha) = 0$ ou $q(\alpha) = 0$, o que contradiz a minimalidade do grau de $p(X)$. Vamos agora mostrar a unicidade de $p(X)$. Para isso, tomemos $g(X) \in \mathcal{F}[X]$ mônico irredutível, com $g(\alpha) = 0$ e $\partial\alpha g(X) = \partial\alpha p(X) = n$. Pelo algorítmo da divisão, existem únicos $q(X),\ r(X) \in \mathcal{F}[X]$ tais que

$$p(X) = g(X) \cdot q(X) + r(X), \text{ com } r(X) = 0 \text{ ou } \partial r(X) < \partial g(X).$$

Suponhamos que $r(X) \neq 0$. Desde que

$$r(\alpha) = p(\alpha) - g(\alpha) \cdot q(\alpha) = 0 - 0 \cdot q(\alpha) = 0,$$

então α é uma raiz de $r(X)$ e sendo $\partial r(X) < \partial p(X)$, contradizendo a minimalidade do grau de $p(X)$. Portanto, $r(X) = 0$, resultando que

$$p(X) = g(X) \cdot q(X).$$

Mas se $p(X)$ e $g(X)$ são irredutíveis, então a última igualdade indica $q(X) = a \in \mathcal{F}^*$. E mais, como estes polinômios são mônicos, então necessariamente $a = 1$. Portanto, $p(X) = g(X)$. ■

Definição 2.4. O polinômio $p(X)$, nas condições do teorema anterior, é chamado **polinômio minimal de** α **sobre** $\mathcal{F}$, o qual será indicado por $irr(\alpha,\ \mathcal{F})$. O grau de $irr(\alpha, \mathcal{F})$ é **o grau de** α **sobre** $\mathcal{F}$, denotado por $\partial(\alpha, \mathcal{F})$.

Sendo $\alpha \in \mathcal{K} \supset \mathcal{F}$, vamos indicar por $\mathcal{F}[\alpha]$ o seguinte subconjunto de $\mathcal{K}$:

$$\mathcal{F}[\alpha] = \{f(\alpha) : f(X) \in \mathcal{F}[X]\}.$$

Inicialmente pode-se constar que $\mathcal{F}[\alpha]$ é um subdomínio de $\mathcal{K}$ que contém $\mathcal{F}$.

Vamos descrever a forma dos elementos de $\mathcal{F}[\alpha]$ considerando que α é algébrico sobre $\mathcal{F}$. Seja $p(X) = irr(\alpha, \mathcal{F})$, com $\partial p(X) = n$. Dado $f(X) \in \mathcal{F}[X]$, existem pelo algoritmo da divisão, $q(X),\ r(X) \in \mathcal{F}[X]$ tais que

$$f(X) = p(X) \cdot q(X) + r(X),$$

em que $r(X) = 0$ ou $\partial r(X) < \partial p(X)$. Para qualquer um dos casos, podemos considerar $r(X) = r_0 + r_1X + \cdots + r_{n-1}X^{n-1}$, com $r_i \in \mathcal{F}$ para $i = 0, 1, \cdots, n-1$. Como

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

e $p(\alpha) = 0$, então

$$f(\alpha) = r(\alpha) = r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1}.$$

Portanto, $\mathcal{F}[\alpha]$ consiste de expressões polinomiais como acima, isto é,

$$\mathcal{F}[\alpha] = \{r_0 + r_1\alpha + r_{n-1}\alpha^{n-1} : r_i \in \mathcal{F}\}.$$

É imediato verificar que se $\alpha \in \mathcal{F}$, então $\mathcal{F}[\alpha] = \mathcal{F}$.
Uma sugestão para verificar a igualdade é tomar
$r_o = 0,\ r_1 = 1,\ r_2 = 0, \cdots, r_{n-1} = 0$
Daí, obtemos

$$0 + 1\alpha + \cdots + 0\alpha^{n-1} = \alpha$$

Como $0 + 1\alpha + \cdots + 0\alpha^{n-1} \in \mathcal{F}[\alpha]$ e $\alpha \in \mathcal{F} \Rightarrow \mathcal{F}[\alpha] = \mathcal{F}$.

Exemplo 2.6. Consideremos $\mathcal{F} = \mathbb{Q},\ \mathcal{K} = \mathbb{R}$ e $\alpha = \sqrt{2}$. Neste caso, temos

$$p(X) = irr(\sqrt{2},\ \mathbb{Q}) = X^2 - 2.$$

Assim,

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

No geral, se p é um número primo, então $irr(\sqrt{p},\ \mathbb{Q}) = X^2 - p$ e

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

Lema 2.2.1. *Se $\alpha \in \mathcal{K} \supset \mathcal{F}$, então a aplicação $\phi_\alpha : \mathcal{F}[X] \to \mathcal{K}$ dada por*

$$\phi_\alpha(f(X)) = f(\alpha)$$

é um homomorfismo de anéis.

Demonstração. Tomemos

$$f(X) = a_0 + a_1X + \cdots + a_nX^n \quad \text{e} \quad g(X) = b_0 + b_1X + \cdots + b_mX^m.$$

Então somando $f(X)$ com $g(X)$, obtemos:

$$f(X) + g(X) = c_0 + c_1X + \cdots + c_rX^r,$$

em que $c_i = a_i + b_i,\ i \in \mathbb{N}$.
Assim,

$$\phi_\alpha(f(X) + g(X)) = c_0 + c_1\alpha + \cdots + c_r\alpha^r$$

$$\phi_\alpha(f(X) + \phi_\alpha(g(X)) = (a_0 + a_1\alpha + \cdots + a\alpha^n) + (b_0 + b_1\alpha + \cdots + b_m\alpha^m).$$

$$= \phi_\alpha(f(X) + \phi_\alpha(g(X)).$$

Já para a multiplicação, consideremos

$$f(X) \cdot g(X) = d_0 + d_1X + \cdots + d_sX^s,$$

em que $d_j = \sum_{i=0}^{j} a_ib_{j-i},\ j \in \mathbb{N}$.
logo,

$$\phi(f(X) \cdot g(X)) = d_0 + d_1\alpha + \cdots + d_s\alpha^s$$

e

$$\phi_\alpha(f(X)) \cdot \phi_\alpha(g(X)) = (a_0 + a_1\alpha + \cdots + a_n\alpha^n) \cdot (b_0 + b_1\alpha + \cdots + b_m\alpha^m).$$

$$= \phi_\alpha(f(X) \cdot \phi_\alpha(g(X))$$

Assim, concluímos que ϕ_α é um homomorfismo de anéis.

■

Teorema 2.3. *Sejam $\alpha \in \mathcal{K} \supset \mathcal{F}$ e ϕ_α o homomorfismo do lema anterior. Então:*

(1) $Im(\phi_\alpha) = \mathcal{F}[\alpha]$.

(2) α é transcedente sobre $\mathcal{F}$ se, e somente se, $Ker(\phi_\alpha) = \{0\}$.

(3) Se α é algébrico sobre $\mathcal{F}$ e $p(X) = irr(\alpha,\ \mathcal{F})$, então $Ker(\phi_\alpha) =< p(X) >$ é um ideal maximal de $\mathcal{F}[X]$.

(4) $\dfrac{\mathcal{F}[x]}{Ker(\phi_\alpha)} \simeq \mathcal{F}[\alpha]$.

Demonstração.

(1) Este item segue diretamente das definições do homomorfismo ϕ_α e do conjunto $\mathcal{F}[X]$.

(2) Suponha que α é transcedente sobre $\mathcal{F}$. Se $Ker(\phi_\alpha) \neq \{0\}$, então existe $f(X) \in \mathcal{F}[X] - \{0\}$ tal que $\phi_\alpha(f(X)) = 0$, isto é,

$$f(\alpha) = \phi_\alpha(f(X)) = 0,$$

ou seja, α é algébrico sobre $\mathcal{F}$, o que é uma contradição. Portanto, $Ker(\phi_\alpha) = \{0\}$. Reciprocamente, se $Ker(\phi_\alpha) = \{0\}$, então para qualquer $f(X) \in \mathcal{F}[X] - \{0\}$ temos que $\phi_\alpha(f(X)) \neq 0$, ou seja, $f(\alpha) \neq 0$. Assim, α é transcedente sobre $\mathcal{F}$.

(3) Consideremos α algébrico sobre $\mathcal{F}$ e seja $p(X) = irr(\alpha,\ \mathcal{F})$. Primeiro mostremos que $Ker(\phi_\alpha) =< p(X) >$. Suponha que $f(X) \in < p(X) >$, então direto pela definição do ideal $< p(x) >$, existe $g(X) \in \mathcal{F}[X]$ tal que $f(X) = p(X) \cdot g(X)$. Desse modo,

$$f(\alpha) = p(\alpha) \cdot g(\alpha) = 0 \cdot g(\alpha) = 0,$$

ou seja, $\phi_\alpha\ (f(X)) = 0$, de modo que $f(X) \in Ker(\phi_\alpha)$, mostrando com isso que $< p(X) > \subset Ker(\phi_\alpha)$. Por outro lado, seja $h(X) \in Ker(\phi_\alpha)$, então $\phi_\alpha(h(X) = 0$, assim, $h(\alpha) = 0$, implicando que α é raiz de $h(X)$. Do algoritmo da divisão, tomemos $q(X),\ r(X) \in \mathcal{F}[X]$ tais que

$$h(X) = p(X) \cdot q(X) + r(X), \text{ com } r(X) = 0 \textit{ ou } \partial r(X) < \partial p(X).$$

Assim,

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

Mas, pela definição do polinômio $p(X)$, não podemos ter $\partial r(X) < \partial p(X)$. Dessa forma $r(X) = 0$, e por conseguinte, $h(X) = p(X) \cdot q(X)$. Com isso, $h(X) \in < p(X) >$ e temos a outra inclusão, ou seja, $Ker(\phi_\alpha) \subset < p(X) >$. Portanto, $Ker(\phi_\alpha) =< p(X) >$. A maximilidade do ideal $< p(X) >$ decorre diretamente do Teorema 1.9.

(4) Pelo item (1), sabemos que $Im(\phi_\alpha) = \mathcal{F}[\alpha]$. Logo, pelo Teorema 1.5, obtemos;

$$\frac{\mathcal{F}[X]}{Ker(\phi_\alpha)} \simeq \mathcal{F}[\alpha].$$

■

Corolário 2.1. Dado $\alpha \in \mathcal{K} \supset \mathcal{F}$, valem as propriedades:

(1) Se α é algébrico sobre $\mathcal{F}$, então $\mathcal{F}[\alpha]$ é um subcorpo de $\mathcal{K}$.

(2) Se α é transcedente sobre $\mathcal{F}$, então $\mathcal{F}[X]$ é um subdomínio de $\mathcal{K}$ isomorfo ao domínio de integridade $\mathcal{F}[X]$.

Demonstração.

(1) Se α é algébrico sobre $\mathcal{F}$, então pelo item (3) do Teorema 2.3, podemos afirmar que $Ker(\phi_\alpha) =< p(X) >$, com $p(X) = irr(\alpha,\ \mathcal{F})$, é um ideal maximal de $\mathcal{F}[X]$. Por outro lado pelo item (4) do mesmo teorema

$$\frac{\mathcal{F}[X]}{< p(X) >} \simeq \mathcal{F}[\alpha].$$

Com efeito, sendo, $< p(X) >$ maximal, segue do Teorema 1.9 que o anel quociente $\dfrac{\mathcal{F}[X]}{< p(X) >}$ é um corpo. Portanto, do isomorfismo acima, $\mathcal{F}[\alpha]$ também é um corpo.

(2) Pelo item (2) do Teorema 2.3, sendo α transcedente sobre $\mathcal{F}$, segue que $Ker(\phi_\alpha) = \{0\}$ e pelo item (4) do mesmo teorema, concluims que

$$\frac{\mathcal{F}[X]}{\{0\}} \simeq \mathcal{F}[X].$$

Assim,

$$\mathcal{F}[X] \simeq \frac{\mathcal{F}[X]}{\{0\}} \simeq \mathcal{F}[\alpha],$$

isto é, $\mathcal{F}[X] \simeq \mathcal{F}[X]$. Disso concluímos que $\mathcal{F}[\alpha]$ é um subdomínio de $\mathcal{K}$. ■

3 EXTENSÕES FINITAS E ALGÉBRICAS

Este Capítulo é destinado a apresentar o principal momento de nosso trabalho, o qual versa sobre Extensões de Corpos Finitas e Algébricas e traz resultados indispensáveis e elegantes para estudos aprofundados da Teoria dos Corpos.

Então vamos aos conceitos e resultados.

Definição 3.1. Seja $\mathcal{F}$ um corpo qualquer e seja $\mathcal{V}$ um conjunto não vazio onde está definida uma operação soma. Suponhamos também que esteja definida, uma operação de elementos de $\mathcal{F}$ por elementos de $\mathcal{V}$, assim definidas:

$$\begin{array}{rccc} + & : & \mathcal{V}\times\mathcal{V} & \longrightarrow & V \\ & & (u,v) & \longmapsto & u+v \end{array} \quad \text{e} \quad \begin{array}{rccc} \cdot & : & \mathcal{F}\times\mathcal{V} & \longrightarrow & V. \\ & & (\lambda,v) & \longmapsto & \lambda\cdot v \end{array}$$

Dizemos que V munido dessas operações é um **espaço vetorial** sobre o corpo $\mathcal{F}$ se as seguintes propriedades são verificadas quaisquer que sejam $u,\ v\ \in \mathcal{V}$ e $\alpha,\ \beta \in \mathcal{F}$:
i) $(\mathcal{V},+)$ é um grupo abeliano.
ii) $1\cdot v = v$. (1 é a unidade do corpo $\mathcal{F}$)
iii) $\alpha\cdot(u+v) = \alpha\cdot u + \alpha\cdot v$.
iv) $(\alpha+\beta)\cdot u = \alpha\cdot u + \beta\cdot u$.
v) $\alpha\cdot(\beta\cdot v) = \alpha\cdot(\beta\cdot v) = (\alpha\beta)\cdot v$.

Exemplo 3.1. Sejam $\mathcal{F}$ um corpo qualquer, $\mathcal{K}$ uma extensão de $\mathcal{F}$ e $\alpha \in \mathcal{K}$. É de fácil verificação que podemos definir operações sobre $\mathcal{K}[X]$(respectivamente $\mathcal{K}[\alpha]$) de modo que $\mathcal{K}[X]$ (respectivamente $\mathcal{K}[\alpha]$) torna-se um espaço vetorial sobre $\mathcal{K}$. Para isso basta considerar em $\mathcal{K}[X]$ ($\mathcal{K}[\alpha]$ segue analogamente) as seguintes operações:

$$\begin{array}{rccc} + & : & \mathcal{K}[X]\times\mathcal{K}[X] & \longrightarrow & \mathcal{K}[X] \\ & & (f(X),g(X)) & \longmapsto & f(X)+g(X) \end{array} \quad \text{e} \quad \begin{array}{rccc} \cdot & : & K\times\mathcal{K}[X] & \longrightarrow & \mathcal{K}[X] \\ & & (\lambda,f(X)) & \longmapsto & \lambda\cdot f(X). \end{array}$$

Com estas operações $\mathcal{K}[X]$ é um espaço vetorial sobre $\mathcal{K}$.

Exemplo 3.2. Seja $\mathcal{K}$ uma extensão de $\mathcal{F}$, então $\mathcal{K}$ pode ser visto como espaço vetorial sobre o corpo $\mathcal{F}$. De fato, as operações

$$\begin{array}{rccc} + & : & \mathcal{K}\times\mathcal{K} & \longrightarrow & \mathcal{K} \\ & & (u,v) & \longmapsto & u+v \end{array} \quad \text{e} \quad \begin{array}{rccc} \cdot & : & \mathcal{F}\times\mathcal{K} & \longrightarrow & \mathcal{K} \\ & & (\lambda,u) & \longmapsto & \lambda\cdot u \end{array}$$

já existem de modo natural no corpo $\mathcal{K}$.

Definição 3.2. Um subconjunto não vazio $\mathcal{W}$ do espaço vetorial $\mathcal{V}$ sobre $\mathcal{K}$ é dito um **subespaço vetorial** de $\mathcal{V}$ se as seguintes condições são satisfeitas:

a) Se $w_1,\ w_2 \in \mathcal{W}$ então $w_1 + w_2 \in \mathcal{W}$.
b) Se $\lambda \in \mathcal{K}$ e $\ w \in \mathcal{W}$, então $\lambda \cdot w \in \mathcal{W}$.

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

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

Se $u_1,\ u_2, ..., u_r \in \mathcal{V}$, então é fácil verificar que $\mathcal{W} = \{\sum_{i=1}^{r} \alpha_i u_i : \alpha_i \in K, i = 1, ..., r\}$ é um subespaço vetorial de $\mathcal{V}$, o qual chamaremos de **subespaço gerado** por $u_1, ..., u_r$ e denotaremos esse espaço por

$$\mathcal{W} = [u_1, ..., u_r].$$

Se um conjunto (ordenado) $\{v_1, ..., v_n\} \subset \mathcal{V}$ for L.I. e tal que $[v_1, ..., v_n] = \mathcal{V}$, dizemos que $\{v_1, ..., v_n\}$ é uma **base** de $\mathcal{V}$. Por exemplo, $\{e_1, ..., e_n\}$ é uma base de $\mathcal{K}^n$.

Teorema 3.1. *a) Todo espaço vetorial $\mathcal{V}$ sobre um corpo $\mathcal{K}$ possui uma base.*
b) Se um espaço vetorial $\mathcal{V}$ sobre um corpo $\mathcal{K}$ possui uma base com n elementos, então toda base de $\mathcal{V}$ possui n elementos.

Demonstração. Ver demonstração no livro de Flávio Ulhôa

■

Se β é uma base para $\mathcal{V}$, então o número de elementos de β é chamado de **dimensão** de $\mathcal{V}$ e denotamos por $dim\ \mathcal{V}$. Assim, se $\beta = \{u_1, ..., u_r\}$ é base para $\mathcal{V}$, então $dim\ \mathcal{V} = n$.

3.1 EXTENSÕES FINITAS E ALGÉBRICAS

Seja $\mathcal{K}$ uma extensão de $\mathcal{F}$ e consideremos as seguintes operações

$$\begin{array}{ll} + : \mathcal{K} \times \mathcal{K} \to \mathcal{K} & \cdot : \mathcal{F} \times \mathcal{K} \to \mathcal{K} \\ (a,\ b) \mapsto a + b & (\lambda,\ a) \mapsto \lambda \cdot a \end{array}$$

É simples verificar que $\mathcal{K}$, com estas operações, é um espaço vetorial sobre $\mathcal{F}$, isto nos permite apresentar o conceito de grau de uma extensão.

Definição 3.3. Definimos o **grau** ou **índice** de uma extensão $\mathcal{K} \supset \mathcal{F}$, indicado por $[\mathcal{K} : \mathcal{F}]$ como sendo a dimensão de $\mathcal{K}$, visto como espaço vetorial sobre $\mathcal{F}$. A extensão $\mathcal{K}$ é dita **finita** se $[\mathcal{K} : \mathcal{F}]$ é finito. Caso contrário a extensão é dita **infinita**.

Exemplo 3.3. O corpo $\mathbb{C}$ é uma extensão de grau 2 sobre $\mathbb{R}$, isto é, $[\mathbb{C} : \mathbb{R}] = 2$, pois $\mathcal{B} = \{1, i\}$ é base de $\mathbb{C}$ sobre $\mathbb{R}$.

Teorema 3.2. *Sejam $\mathcal{K}_1$, $\mathcal{K}_2$ e $\mathcal{K}_3$ corpos, tais que $\mathcal{K}_1 \supset \mathcal{K}_2 \supset \mathcal{K}_3$. Se $[\mathcal{K}_1 : \mathcal{K}_2]$ e $[\mathcal{K}_2 : \mathcal{K}_3]$ são finitos, então $[\mathcal{K}_1 : \mathcal{K}_3]$ é finito. Além disso,*

$$[\mathcal{K}_1 : \mathcal{K}_3] = [\mathcal{K}_1 : \mathcal{K}_2] \cdot [K_2 : \mathcal{K}_3].$$

Demonstração. Sejam $\{v_1, \cdots, v_m\}$ uma base de $\mathcal{K}_1$ sobre $\mathcal{K}_2$ e $\{u_1, \cdots, u_n\}$ uma base de $\mathcal{K}_2$ sobre $\mathcal{K}_3$. Vamos mostrar que

$$\mathcal{B} = \{v_i \cdot u_j : 1 \leq i \leq m \ e \ 1 \leq j \leq n\}$$

é uma base de $\mathcal{K}_1$ sobre $\mathcal{K}_3$. Mostremos que $\mathcal{B}$ gera $\mathcal{K}_1$ como espaço vetorial sobre $\mathcal{K}_3$. De fato, se $u \in \mathcal{K}_1$, então podemos escrever

$$u = \sum_{i=1}^{m} \alpha_1 v_i, \ \alpha_i \in \mathcal{K}_2. \qquad \text{(I)}$$

Por outro lado, como $\alpha_i \in \mathcal{K}_2$ e $\{u_1, \cdots, u_n\}$ é uma base de $\mathcal{K}_2$ sobre $\mathcal{K}_3$, segue que

$$\alpha_i = \sum_{j=1}^{n} \beta_{ij} u_j, \quad \beta_{ij} \in \mathcal{K}_3. \qquad \text{(II)}$$

Substituindo os valores dos $\alpha_i s$ dados por (II) em (I), obtemos

$$u = \sum_{i=1}^{m} \sum_{j=1}^{n} \beta_{ij} v_i u_j, \quad \beta_{ij} \in \mathcal{K}_3. \qquad \text{(III)}$$

Mas a igualdade (III) mostra que $\mathcal{B}$ gera o espaço $\mathcal{K}_1$ sobre $\mathcal{K}_3$. Agora, vamos mostrar que $\mathcal{B}$ é L.I sobre $\mathcal{K}_3$. Para isso, consideremos a equação

$$\sum_{i=1}^{m} \sum_{j=1}^{n} \beta_{ij} v_i u_j = 0, \quad \beta_{ij} \in \mathcal{K}_3.$$

Esta igualdade pode ser escrita da forma

$$\sum_{i=1}^{m} \lambda_i v_i = 0, \qquad \text{(IV)}$$

em que $\lambda_i = \sum_{j=1}^{n} \beta_{ij} u_j$ para cada $i = 1, \cdots, m$. Desde que $\{v_1, \cdots, v_m\}$ é L.I sobre $\mathcal{K}_2$, então da igualdade (IV) segue que os escalares $\lambda_i = 0$, com $i = 1, \cdots, m$. Por isso,

$$\sum_{j=1}^{n} \beta_{ij} u_j = 0, \quad i = 1, \cdots, m.$$

Analogamente, como $\{u_1, \cdots, u_n\}$ é L.I sobre $\mathcal{K}_3$, então dessa última igualdade obtemos que

$$\beta_{ij} = 0,$$

para $i = 1, \cdots, m$ e $j = 1, \cdots, n$, donde concluímos que $\mathcal{B}$ é L.I. Portanto, segue que $\mathcal{B}$ é uma base de $\mathcal{K}_1$ sobre $\mathcal{K}_3$ e temos que $[\mathcal{K}_1 : \mathcal{K}_3] = mn$. Assim, chegamos que

$$[\mathcal{K}_1 : \mathcal{K}_3] = [\mathcal{K}_1 : \mathcal{K}_2] \cdot [\mathcal{K}_2 : \mathcal{K}_3].$$

■

Corolário 3.1. Se $\mathcal{K}_i$ é um corpo para cada $i = 1, \cdots, r$ e $\mathcal{K}_{i+1}$ é uma extensão finita de $\mathcal{K}_i$, então $\mathcal{K}_r$ é uma extensão finita de $\mathcal{K}_1$. Além disso,

$$[\mathcal{K}_r : \mathcal{K}_1] = [\mathcal{K}_r : \mathcal{K}_{r-1}] \cdot [\mathcal{K}_{r-1} : \mathcal{K}_{r-2}] \cdots [\mathcal{K}_2 : \mathcal{K}_1].$$

Demonstração. Indução sobre r. ■

Definição 3.4. Uma extensão $\mathcal{K}$ é dita **extensão algébrica de** $\mathcal{F}$ se todo elemento $\alpha \in \mathcal{K} \supset \mathcal{F}$ é algébrico sobre $\mathcal{F}$.

A seguir vamos mostrar que toda extensão finita é também extensão algébrica. Antes,vejamos o seguinte resultado.

Lema 3.2.1. *Seja $\mathcal{V}$ um espaço vetorial gerado pelos vetores $v_1,\ v_2, \cdots, v_n$. Então, qualquer subconjunto de $\mathcal{V}$ com mais de n vetores é L.D. Por conseguinte, qualquer subconjunto L.I de $\mathcal{V}$ tem o máximo n vetores.*

Teorema 3.3. *Se $\mathcal{K}$ é uma extensão finita de $\mathcal{F}$, então $\mathcal{K}$ é uma extensão algébrica de $\mathcal{F}$.*

Demonstração. Mostremos que cada $\alpha \in \mathcal{K}$ é algébrico sobre $\mathcal{F}$. Como $\mathcal{K}$ é uma extensão finita de $\mathcal{F}$, digamos, $[\mathcal{K} : \mathcal{F}] = n$, segue do Lema 3.2.1 que os elementos $1, \alpha, \cdots, \alpha^n$ não podem ser L.I. Logo, por definição, existem $a_0, a_1, \cdots, a_n \in \mathcal{F}$ não todos nulos tais que

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0.$$

Isso significa que α é raiz do polinômio não nulo $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathcal{F}[X]$. Portanto, α é algébrico sobre $\mathcal{F}$. ■

O Teorema 3.3 acima afirma que toda extensão algébrica é finita. Uma pergunta natural é a seguinte: toda extensão finita é algébrica, ou seja, vale a recíproca do Teorema 3.3 ? A resposta é não. E isso será feito mais adiante através de um contraexemplo.

Antes, porém, temos que apresentar alguns resultados que preparam para apresentação deste contarexemplo.

Teorema 3.4. *Seja $\alpha \in \mathcal{K} \supset \mathcal{F}$ algébrico sobre $\mathcal{F}$ e $p(X) = irr(\alpha, \mathcal{F})$, com $\partial\, p(X) = n$. Então $\beta = \{1, \alpha, ..., \alpha^{n-1}\}$ é uma base para o espaço $\mathcal{F}[\alpha]$ sobre $\mathcal{F}$. Em particular, $[\mathcal{F}[\alpha] : \mathcal{F}] = n$ e $\mathcal{F}[\alpha]$ é uma extensão algébrica de $\mathcal{F}$.*

Demonstração. Em primeiro lugar, como $\partial\, p(X) = n$, então temos que

$$\mathcal{F}[\alpha] = \{r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1} : r_i \in \mathcal{F}\}.$$

Por isso, se $\beta \in \mathcal{F}[\alpha]$, então

$$\beta = r_0 \cdot 1 + r_1 \cdot \alpha + \cdots + r_{n-1} \cdot \alpha^{n-1} \in [1 \cdot \alpha, \cdots, \alpha^{n-1}].$$

Portanto, $[\mathcal{B}] = \mathcal{F}[\alpha]$. Por outro lado, cada $\beta \in \mathcal{F}[\alpha]$ pode ser escrito de forma única com combinação linear dos elementos de $\mathcal{B}$. Por isso, se

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0,$$

para $a_i \in \mathcal{F}$, então, como

$$0 = 0 + 0\alpha + \cdots + 0\alpha^{n-1},$$

segue que

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0 + 0\alpha + \cdots + 0\alpha^{n-1}.$$

Logo, pela unicidade da expressão de cada elemento de $\mathcal{F}[\alpha]$, concluímos que $a_1 = a_2 = \cdots = a_{n-1} = 0$. Portanto, $\mathcal{B}$ é L.I, e assim é uma base de $\mathcal{F}[\alpha]$. Por conseguinte, $[\mathcal{F}[\alpha] : \mathcal{F}] = n$. Para finalizar, segue do Teorema 3.3 que $\mathcal{F}[\alpha]$ é uma expressão algébrica de $\mathcal{F}$. ■

Corolário 3.2. Seja $\alpha \in \mathcal{K} \supset \mathcal{F}$. Então, as seguintes afirmações são equivalentes:

(1) α é algébrico sobre $\mathcal{F}$.

(2) $\mathcal{K}[\alpha]$ é uma extensão finita de $\mathcal{F}$.

(3) $\mathcal{K}[\alpha]$ é uma extensão algébrica de $\mathcal{F}$.

Exemplo 3.4. Para $\alpha = \sqrt{5} \in \mathbb{Q}[\sqrt{5}] \supset \mathbb{Q}$, temos $irr(\alpha, \mathbb{Q}) = X^2 - 5$. Desse modo $\{1, \sqrt{5}\}$ é uma base de $\mathbb{Q}\sqrt{5}$ sobre $\mathbb{Q}$.

3.2 EXEMPLO DE UMA EXTENSÃO ALGÉBRICA QUE NÃO É FINITA

Encerramos este último capítulo com um exemplo atípico, com o intuito de mostrar que nem toda extensão algébrica é finita. Iremos considerar o contrário do que foi feito

anteriormente, com uma cadeia infinita de subcorpos de $\mathbb{Q}$, porém, seguindo o mesmo princípio.

Consideremos $\mathcal{K} = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \cdots, \sqrt{p}, \cdots]$ o menor subcorpo de $\mathbb{R}$ que contém $\mathbb{Q}$ e todas raízes quadráticas $\sqrt{p}$ para cada número primo positivo p. Mostremos primeiramente que

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}] \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}] \subset \cdots$$

é uma cadeia infinita. Para tanto, considere $p_1, p_2, \cdots, p_n$ os n números primos positivos e $q > 0$ um número primo tal que[1] $q \neq p_i$ para cada $i = 1, \cdots, n$.

Vamos mostrar por indução que $\sqrt{q} \notin \mathcal{F} = \mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}, \cdots, \sqrt{p_n}]$. Se $n = 0$, então $\mathcal{F} = \mathbb{Q}$, e como já sabemos, $\sqrt{q} \notin \mathbb{Q}$. Suponhamos que o resultado seja válido para $n - 1$ primeiros primos e façamos

$$\mathcal{F} = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \cdots, \sqrt{p_{n-1}}, \sqrt{p_n}].$$

Logo, $\mathcal{F} = \mathcal{F}_1[\sqrt{p_n}]$ em que $\mathcal{F}_1 = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \cdots, \sqrt{p_{n-1}}]$. Por hipótese, o resultado é válido para $n - 1$. Por absurdo, suponhamos que $\sqrt{q} \in \mathcal{F}$. Como $\mathcal{F}$ é uma extensão de $\mathcal{F}_1$ de grau 2 pois$\sqrt{p_n}^2 - p_n = 0$, então podemos escrever $\sqrt{p}$ da forma

$$\sqrt{q} = a + b\sqrt{p_n}, \quad \text{com } a,\ b \in \mathcal{F}_1.$$

Elevando ao quadrado ambos os lados desta igualdade, obtemos

$$q = a^2 + b^2 p_n + 2ab\sqrt{p_n}.$$

Notemos que se $b = 0$, então da última igualdade temos que $\sqrt{q} \in \mathcal{F}_1$, o que é um absurdo. Da mesma forma, para $a = 0$ chega-se que

$$\frac{\sqrt{q}}{\sqrt{p}} \in \mathcal{F}_1,$$

o que não acontece. Por fim, se $a \neq 0$ e $b \neq 0$, então

$$\sqrt{p_n} = \frac{q - a^2 - b^2 p_n}{2ab},$$

ou seja, $\sqrt{p_n} \in \mathcal{F}_1$, o que não é possível. Por isso,

$$\sqrt{q} \notin \mathcal{F} = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \cdots, \sqrt{p_{n-1}}, \sqrt{p_n}].$$

Isso significa que

[1] Isso é possível, desde que o conjunto dos números primos é infinito.

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}] \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}] \subset \cdots$$

é uma cadeia infinita de corpos. Portanto, por construção, $\mathcal{K} = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \cdots, \sqrt{p}, \cdots]$ é uma extensão infinita de $\mathbb{Q}$. Por fim, notemos que se $\alpha \in \mathcal{K}$, então existe $r \in \mathbb{N}$ tal que $\alpha \in \mathbb{Q}[\sqrt{2}, \sqrt{3}, \cdots, \sqrt{p_r}]$. Mas pelo Corolário 3.1,

$$[\mathbb{Q}[\sqrt{2}, \sqrt{3}, \cdots, \sqrt{p_r}] : \mathbb{Q}] = 2^r,$$

pois $[\mathbb{Q}[\sqrt{p_i}] : \mathbb{Q}] = 2$ para cada $i = 1, \cdots, r$. Por isso, pelo Teorema 3.3, segue que α é algébrico sobre $\mathbb{Q}$. Portanto, $\mathcal{K} = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \cdots, \sqrt{p}, \cdots]$ é uma extensão algébrica de $\mathbb{Q}$, porém é uma extensão infinita. Portanto, apresentamos uma extensão de corpos algébrica que não é finita.

REFERÊNCIAS

BHATTACHARIA, P.; JAIN, S.; NAGPAUL, S. **Basic Abstract Algebra**. 2. ed. New York, EUA: Cambridge University Press, 1995.

FAZZIO, A.; WATARI, K. **Introdução à Teoria de Grupos aplicada em moléculas e sólidos**. 2. ed. Santa Maria, RS: UFSM, 2009.

GARCIA, A.; LEQUAIN, Y. **Elementos de Álgebra**. 6. ed. Rio de Janeiro, RJ: IMPA, 2012.

MILIES, C. P. Grupos Nilpotentes: Uma Introdução. **Matemática Universitária**, n. 34, p. 55 – 100, 2003.

SILVEIRA, D. S. Grupos solúveis e nilpotentes. UFMG, Minas GeraisMG, 2010.

VIEIRA, V. L. **Álgebra Abstrata para Licenciatura**. 2. ed. Campina Grande, PB: EDUEPB, 2015.