UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

MESTRADO ACADÊMICO EM MATEMÁTICA

JOSAFÁ MARTINS GONÇALVES

O ANEL DOS INTEIROS ALGÉBRICOS DE UM CORPO DE NÚMEROS É UM DOMÍNIO DE DEDEKIND

FORTALEZA

2020

JOSAFÁ MARTINS GONÇALVES

O ANEL DOS INTEIROS ALGÉBRICOS DE UM CORPO DE NÚMEROS É UM DOMÍNIO DE DEDEKIND

Dissertação apresentada ao Curso de Mestrado Acadêmico em Matemática do Programa de Pós-Graduação em Matemática do Centro de Ciências da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Mestre em Matemática. Área de Concentração: Álgebra

Orientador: Prof. Dr. Antônio Caminha Muniz Neto

FORTALEZA

2020

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

G625a Gonçalves, Josafá Martins Gonçalves.
O anel dos inteiros algébricos de um corpo de números é um domínio de Dedekind / Josafá Martins Gonçalves Gonçalves. – 2020.
73 f.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Programa de Pós-Graduação em Matemática, Fortaleza, 2020.
Orientação: Prof. Dr. Antônio Caminha Muniz Neto.

1. Domínios de Dedekind. 2. Inteiros Algébricos. 3. Corpos de Números. 4. Corpos Ciclotômicos. I. Título.

CDD 510

JOSAFÁ MARTINS GONÇALVES

O ANEL DOS INTEIROS ALGÉBRICOS DE UM CORPO DE NÚMEROS É UM DOMÍNIO DE DEDEKIND

Dissertação apresentada ao Curso de Mestrado Acadêmico em Matemática do Programa de Pós-Graduação em Matemática do Centro de Ciências da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Mestre em Matemática. Área de Concentração: Álgebra

Aprovada em:

BANCA EXAMINADORA

Prof. Dr. Antônio Caminha Muniz Neto (Orientador)
Universidade Federal do Ceará (UFC) - Fortaleza

Prof. Dr. Francisco Yure Santos do Nascimento
Universidade Federal do Ceará (UFC) - Crateús

Prof. Dr. Ulisses Lima Parente
Universidade Estadual do Ceará (UECE)

Dedico este trabalho ao Professor Francisco José Bitu Feitosa, que foi a inspiração para esta caminhada do mestrado.

AGRADECIMENTOS

A Deus primeiramente pelo Dom da Vida.

Ao Prof.Dr. Antônio Caminha Muniz Neto por me orientar nesta dissertação, e por sempre acreditar no meu melhor.

A minha esposa Daucília Araújo Cardozo por sempre está ao meu lado em todos os momentos.

Aos meus Pais (Paulo Gonçalves Filho e Eliane Martins Gonçalves) por todo amor, e dedicação e paciência para comigo durate todos esses anos.

Ao Professor Francisco José Bitu Feitosa à quem dedico esta dissertação e que foi o primeiro a acreditar em meu sonho de concluir o mestrado.

Ao professor Edvalter da Silva Sena Filho por todas as grandes lições na matemática e na vida, e com certeza por ter sido um dos maiores responsáveis por minha entrada no mestrado.

Ao professor Nilton José Neves Cordeiro por cada aprendizado e por cada conselho que levarei por toda vida.

Ao meu nobre amigo Prof. Antônio Ramon Firmo da Costa por toda ajuda e dicas no LaTeXe pela ajuda na digitação do Trabalho.

Ao professor e Amigo Davi Ribeiro dos Santos por toda ajuda e apoio durante momentos difíceis do mestrado

Ao professor e amigo Elisafã Braga dos Santos por ter contribuído fortemente pela minha permanência no mestrado.

Aos Professores da Universidade Vale do Acaraú em nome do Professor Márcio Nascimento da Silva por todo Aprendizado que me Proporcionaram durante a graduação.

Ao programa "Pós graduação: Um sonho Possível"em nome do professor Edvalter da Silva Sena Filho e professor Daniel Brandão Menezes.

Aos docentes da Universidade Federal do Ceará em nome dos professoes Dr. Antônio Caminha Muniz Neto e Dr. Alexandre César Gurgel Fernandes.

A minha sogra (Luzimar Sousa Araújo) e ao meu sogro (Francisco Cardozo Araújo) pelo carinho e paciência.

A todos os meus Irmãos em nome do meu irmão mais velho Paulo Robson Martins Gonçalves e a todas as minhas cunhadas em nome de Taís Araújo Cardozo, a qual me deu grande ajuda no Inglês.

A todos os meus amigos em nome de Raimundo Pereira Barbosa Neto.

Ao CnPQ pelo apoio financeiro.

"O sonho é o que leva a gente para frente. Se a gente for seguir a razão, fica aquietado, acomodado."

(Ariano Suassuna)

RESUMO

Do ponto de vista da Teoria Algébrica dos Números, um problema historicamente importante foi o de entender em detalhe as propriedades do anel dos inteiros algébricos de um corpo de números. Neste trabalho, que pode ser visto como uma introdução autocontida à Teoria Algébrica dos Números, demonstraremos que, se A for um domínio de Dedekind com corpo quociente K, se L for uma extensão separável e finita de K e B for o fecho inteiro de A em L, então B também será um domínio de Dedekind. Como consequência desse fato, concluímos que o anel dos inteiros algébricos de um corpo de números é um Domínio de Dedekind, o que, por sua vez, expõe a ubiquidade dos domínios de Dedekind. Concluímos o texto caracterizando o anel dos inteiros algébricos do n-ésimo corpo ciclotômico como o domínio de Dedekind dado pela adjunção de anéis das raízes complexas n-ésimas da unidade ao anel $\mathbb{Z}$ dos inteiros.

Palavras-chave: Domínio de Dedekind. Inteiros Algébricos. Corpos de números. Corpos ciclotômicos.

ABSTRACT

From the point of view of Algebraic Number Theory, a historically important problem was the one of understanding in detail the properties of the ring of algebraic integers of a number field. In this sense, in this work we show that, if A is a Dedekind domain with field of fractions K, if L is a finite separable extension of K and B is the algebraic closure of A in L, then B is also a Dedekind domain. As a consequence of this fact, we conclude that the ring of algebraic integers of a number field is a Dedekind domain, which, in turn, exposes the ubiquity of Dedekind domains. We close the text by characterizing the ring of algebraic integers of the n-th cyclotomic field as the Dedekind domain given by the ring adjunction of the n-th complex roots of unity to the ring $\mathbb{Z}$ of integers.

Keywords: Dedekind domain. Algebraic integers. Number fields. Cyclotomic fields.

SUMÁRIO

1 INTRODUÇÃO

Este trabalho teve como base principal o livro (ASH, 2013). Essencialmente, trabalhamos com o capítulo 7 do mesmo, no qual consta, de maneira breve, uma explanação introdutória da Teoria Algébrica dos Números.

Entende-se por um *número algébrico* qualquer $\alpha \in \mathbb{C}$ que é algébrico sobre $\mathbb{Q}$ isto é, que é raiz de um polinômio não nulo com coeficientes em $\mathbb{Q}$. Caso α seja raiz de um polinômio mônico com coeficentes em $\mathbb{Z}$, então chamaremos α de *inteiro algébrico*.

Os numeros algébricos surgiram como uma ferramentas para resoluções de equações diofantinas. Como exemplo podemos citar a equação associada ao Último Teorema de Fermat, que diz que, para $n > 2$ inteiro, a equação

$$X^n + Y^n = Z^n$$

não possui soluções inteiras não nulas. Representando a soma $X^n + Y^n$ por

$$(X+Y)(X+\zeta_n Y)\dots(X+\zeta_n^{n-1}Y)$$

onde ζ é uma raiz primitiva n-ésima da unidade, pode-se provar que o Último Teorema de Fermat é válido para n, desde que o domínio $\mathbb{Z}[\zeta]$ seja fatorial.

Outro exemplo importante surge quando tenta-se obter as soluções inteiras da Equação de Pell

$$X^2 - dY^2 = 1,$$

com $d \in \mathbb{Z}$ livre de quadrados. Escrevendo $X^2 - dY^2$ como

$$(X - \sqrt{d}Y)(X + \sqrt{d}Y),$$

verifica-se que as soluções inteiras (a,b) da Equação de Pell correspondem aos elementos invertíveis $a + b\sqrt{d}$ do anel $\mathbb{Z}[d]$.

Esses dois exemplos ilustram a importância, do ponto de vista da Teoria dos Números, do estudo algébrico dos anéis $\mathbb{Z}[\zeta]$ e $\mathbb{Z}[d]$, respectivamente, e isso se dá com ferramentas da Teoria Algébrica dos Números.

Um dos objetivos principais da Teoria do Números Algébricos é o estudo do conjunto de inteiros algébricos ou, mais geralmente, dos elementos "*inteiros*" de extensões de corpos do corpo de frações de um anel dado, o qual não necessariamente é um subconjunto de $\mathbb{C}$.

Nesse sentido, nosso principal objetivo nesta dissertação será provar que, se A é um domínio de Dedekind com corpo de frações K e L é uma extensão separável e finita de K, então o anel B dos elementos inteiros de L também é um domínio de Dedekind. Mostraremos, assim, um propriedade que é de forte ajuda para desenvolvimentos posteriores da teoria.

Adicionalmente, exemplificamos o resultado principal caracterizando o anel dos inteiros algébricos de extensões quadráticas e de extensões ciclotômicas de graus primos.

O trabalho encontra-se dividido da seguinte maneira: Nos capítulos 2 e 3 delineamos vários conceitos e resultados preliminares, tais como ideais primos e maximais, extensões de corpos e módulos. No capítulo 4, introduzimos alguns conceitos e resultados preliminares de Teoria Algébrica dos Números, para, no capítulo 5, apresentarmos a demonstração do teorema principal, juntamente com um exemplo interessante.

2 PRELIMINARES

Nossos primeiras definições serão baseadas nos livros (GONÇALVES, 1979) e (GARCIA; LEQUAIN, 2006). Muitos resultados não serão demonstrados, mas podem ser facilmente encontrados nessas duas bibliografias.

2.1 Anéis, Domínios de Integridade e Corpos

Seja A um conjunto não vazio onde estejam definidos duas operações, as quais chamaremos de soma e produto em A e denotaremos por $+$ e $\cdot$:

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

Chamaremos $(A,+,\cdot)$ um *anel* se as seis propriedades a seguir forem satisfeitas para quaisquer que sejam $a,b,c \in A$.

A_1) $(a+b)+c = a+(b+c)$ (associatividade da soma).

A_2) $\exists\ 0 \in A$ tal que $a+0 = 0+a = a$ (existência de elemento neutro para a soma).

A_3) $\forall x \in A$ existe um único $y \in A$, denotado por $y = -x$ tal que $x+y = y+x = 0$ (existência do inverso aditivo).

A_4) $a+b = b+a$ (comutatividade da soma).

A_5) $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ (associatividade do produto).

A_6) $a\cdot(b+c) = a\cdot b + a\cdot c$; $(a+b)\cdot c = a\cdot c + b\cdot c$ (distributividade à esquerda e à direita).

Adicionalmente, se $(A,+,\cdot)$ satisfizer a propriedade

A_7) $\exists\ 1 \in A; 0 \neq 1$ tal que $x\cdot 1 = 1\cdot x = x, \forall x \in A$,

diremos que $(A,+,\cdot)$ é um *anel com unidade* 1.

Caso A satisfaça a propriedade

A_8) $\forall x,y \in A, x\cdot y = y\cdot x$,

diremos que $(A,+,\cdot)$ é um *anel comutativo*.

Por fim, se o anel $(A,+,\cdot)$ satisfizer a propriedade

A_9) $x,y \in A; x\cdot y = 0 \Rightarrow x = 0$ ou $y = 0$,

diremos que $(A,+,\cdot)$ é um anel *sem divisores de zero*.

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

Finalmente, se um domínio de integridade $(A,+,\cdot)$ satisfizer a propriedade

A_{10}) $\forall\, x \in A, x \neq 0, \exists\, y \ \in A$ tal que $x \cdot y = y \cdot x = 1$,

diremos que $(A, +, \cdot)$ é um *corpo*.

No que segue, muitas vezes deixaremos de indicar as operações do anel, escrevendo simplesmente A para denotar um anel $(A, +, \cdot)$.

2.2 Subanéis

Seja $(A, +, \cdot)$ um anel e B um subconjunto não vazio de A. Suponha que B seja fechado para as operações $+$ e $\cdot$ de A, isto é:

a) $x, y \in B \Rightarrow x + y \in B$.

b) $x, y \in B \Rightarrow x \cdot y \in B$.

Desta forma, podemos considerar a soma e o produto como operações em B. Nesse caso, se $(B, +, \cdot)$ for um anel com as operações de A, diremos que B é um *subanel* de A.

Existe um critério simples para decidir quando um subconjunto não vazio de um anel é um subanel. Este é o conteúdo da seguinte

Proposição 2.2.1. *Sejam $(A, +, \cdot)$ um anel e B um subconjunto não vazio de A. Então, B é um subanel de A se, e somente se, as seguintes condições são verificadas.*

(i) $0 \in B$ *(o elemento neutro de A pertence a B).*

(ii) $x, y \in B \Rightarrow x - y \in B$ *(B é fechado para a diferença).*

(iii) $x, y \in B \Rightarrow x \cdot y \in B$ *(B é fechado para o produto).*

Como exemplo, vamos mostrar que $\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p};\ a, b \in \mathbb{Z}$ e p é um número primo$\}$ é um subanel de $\mathbb{R}$. De fato:

(i) $0 = 0 + 0\sqrt{p}, \in \mathbb{Z}[p]$.

(ii) $x = a + b\sqrt{p}, y = c + d\sqrt{p} \Rightarrow x - y = (a - c) + (b - d)\sqrt{p}$.

(iii) $x = a + b\sqrt{P}, y = c + d\sqrt{p} \Rightarrow x \cdot y = (a + b\sqrt{p}) \cdot (c + d\sqrt{p}) = (ac + pdb) + (bc + ad)\sqrt{p}$.

Portanto, $\mathbb{Z}[\sqrt{p}]$ é um subanel de $\mathbb{R}$.

2.3 Ideais e anéis quocientes

Uma classe muito importantes de subanéis de um anel é aquela formada por seus *ideais*, definidos a seguir.

Definição 2.3.1. *Seja A um anel e seja I um subanel de A. Dizemos que I é um ideal à esquerda de A se* $A \cdot I \subset I$*, isto é:*

$$a \cdot x \in I, \forall a \in A, \forall x \in I.$$

De maneira análoga, definimos um ideal à direita J de um anel A como sendo um subanel de A tal que $J \cdot A \subset J$, isto é:

$$x \cdot a \in J, \forall a \in A, \forall x \in J.$$

Caso I seja simultaneamente um ideal à esquerda e à direita de um anel A, diremos simplesmente que I é um *ideal* de A.

Vale observar que, se o anel A for comutativo, então as condições para que um subanel seja ideal à esquerda ou à direita coincidem.

Exemplo 1. *Se A é um anel, então A e { 0 } são claramente ideias de A. Estes ideais são chamados triviais. Caso um ideal seja não trivial, diremos que ele é próprio.*

Exemplo 2. *Seja A um anel. O conjunto (Denotado e definido por)*

$$Ax_1 + Ax_2 + \cdots + Ax_n = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n;\ a_n\ \in A\}.$$

É de fácil verificação que este conjunto é um ideal à esquerda de A, o qual chamaremos ideal à esquerda gerado por $x_1, \cdots, x_n \in A$*. Se* $I = Ax_1$*, então I será chamado ideal principal (à esquerda) gerado por* $x_1 \in A$*. Analogamente, pode-se definir ideal à direita gerado por* $x_1 \cdots, x_n \in A$ *e também ideal (à direita) gerado por* $x_1 \in A$ *.*

Agora, trabalharemos a noção de anéis quocientes. Para tanto, sejam A um anel e J um ideal de A. É fácil ver que a relação $\equiv (mod\ J)$ em A, tal que

$$x \equiv x'(mod\ J) \Leftrightarrow x - x' \in\ J,$$

é de equivalência.

Denotaremos por $\bar{x}$ ou $x + J$ a classe de equivalência de x relativamente a $\equiv (mod\ J)$:

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

Também, chamaremos de *conjunto quociente* de A pelo ideal J ao conjunto

$$A/J = \{x + J, x \in A\}.$$

Através da seguinte proposição é possível tornar A/J um anel:

Proposição 2.3.1. *Sejam um anel A e J um ideal em A. Se* $x \equiv x'(mod\ J)$ *e* $y \equiv y'(mod\ J)$*, então:*

(a) $x+y \equiv (x'+y')(mod\ J)$.

(b) $x \cdot y \equiv x' \cdot y'(mod\ J)$.

Como corolário imediato da proposição anterior, temos o próximo resultado.

Proposição 2.3.2. *Sejam A um anel e J um ideal de A. Se* $\overline{x} = \overline{x'}$ *e* $\overline{y} = \overline{y'}$*, então:*

(a) $\overline{x+y} = \overline{x'+y'}$.

(b) $\overline{x \cdot y} = \overline{x' \cdot y'}$.

Desta forma, o Teorema seguinte mostra que A/J admite uma estrutura natural de anel.

Teorema 2.3.3. *Sejam A um anel e J um ideal de A. Se* $\overline{x} = x+J$ *e* $A/J = \{\overline{x}, x \in A\}$*, então:*

(a) As operações

$$\begin{array}{rccc} +: & A/J \times A/J & \longrightarrow & A/J \\ & (\overline{x},\overline{y}) & \longmapsto & \overline{x+y} = \overline{x}+\overline{y} \end{array} \quad \text{e} \quad \begin{array}{rccc} \cdot: & A/J \times A/J & \longrightarrow & A/J \\ & (\overline{x},\overline{y}) & \longmapsto & \overline{x \cdot y} = \overline{x} \cdot \overline{y} \end{array}$$

estão bem definidas, sendo denominadas adição e produto em A/J.

(b) $A/J, +\cdot$ é um anel, chamado o anel quociente de A por J.

(c) Se 1 é a unidade de A, então $\overline{1}$ é a unidade de A/J.

(d) Se A é comutativo, então A/J é comutativo.

2.4 Ideais primos e maximais

A seguir, definiremos os importantes conceitos de ideial primo e ideal maximal, os quais são essencias em qualquer estudo envolvendo anéis comutativos.

Definição 2.4.1. *Seja* $(A,+,\cdot)$ *um anel comutativo com unidade. Um ideal P de A é primo se* $P \subsetneq A$ *e se* $x,y \in A$ *com* $x \cdot y \in P$ *implicar* $x \in P$ *ou* $y \in P$.

Definição 2.4.2. *Seja* $(A,+,\cdot)$ *um anel comutativo com unidade. Um ideal M de A é maximal se* $M \subsetneq A$ *e se não existe ideal de A propriamente contido entre M e A.*

Os resultados a seguir são verdadeiros.

Teorema 2.4.1. *Seja A um anel comutativo com unidade e seja J um ideal de A. Então:*

J é um ideal maximal de $A \Leftrightarrow A/J$ é um corpo.

Teorema 2.4.2 (Krull)**.** *Todo ideal $J \subsetneq A$ está contido em um ideal maximal.*

2.5 Homomorfimos de anéis

Sejam A e A' dois anéis. Por comodidade de notação, vamos denotar as operações desses anéis pelos mesmo símbolos $+$ e $\cdot$; porém, denotaremos por 0_A o elemento neutro de A e por $0_{A'}$ o elemento neutro de A'. Caso os anéis A e A' possuam unidade, denotaremos por 1_A a unidade A e $1_{A'}$ a unidade de A'.

Definição 2.5.1. *Uma função $f : A \longrightarrow A'$ é denominada um homomorfismo (de anéis) de A em A' se satisfizer as seguintes condições:*

(i) $f(x+y) = f(x) + f(y), \forall x, y \in A$.

(ii) $f(x \cdot y) = f(x) \cdot f(y), \forall x, y \in A$.

Se $f : A \longrightarrow A'$ é um homomorfismo bijetivo, dizemos que f é um *isomorfismo* de A sobre A'.

A próxima proposição lista algumas propriedades elementares de homomorfismos:

Proposição 2.5.1. *Sejam A e A' anéis e $f : A \longrightarrow A'$ um homomorfismo. Então:*

a) $f(0_A) = 0_{A'}$.

b) $f(-a) = -f(a), \forall\ a\ \in A$.

c) Se A e A' são domínios de integridade, então ou f é a função constante e igual a $0_{A'}$ ou $f(1_A) = 1_{A'}$.

d) Se A e A' são corpos, então ou f é a função constante e igual a $0_{A'}$ ou f é injetiva.

Exemplo 3. *Seja A e A' anéis. Claramente, a função constante e igual a $0_{A'}$ é um homomorfismo de A em A'. É também imediato que a função identidade $I_A : A \longrightarrow A$ é um isomorfismo de A em si mesmo.*

Exemplo 4. *Sejam J um ideal de A e $\overline{A} = A/J$. A projeção canônica $\pi : A \longrightarrow \overline{A}$, definida por $\pi(x) = \overline{x}$ para todo $x \in A$, é tal que*

$$\pi(x+y) = \overline{x+y} = \pi(x) + \pi(y)$$

e

$$\pi(x \cdot y) = \overline{x \cdot y} = \overline{x} \cdot \overline{y} = \overline{x} \cdot \overline{y} = \pi(x) \cdot \pi(y).$$

Assim, π é um homomorfismo de A sobre A/J.

O próximo resultado terá importância fundamental na demonstração de alguns teoremas importantes ao longo dessa dissertação. Seu item (iii) é conhecido como o Primeiro Teorema dos Isomorfismos.

Teorema 2.5.2. *Sejam A e A' anéis e $f : A \longrightarrow A'$ um homomorfismo. Então:*
(i) $Im(f) = \{f(a); a \in A\}$ é um subanel de A'.
(ii) $N(f) = \{a \in A; f(a) = 0_{A'}\}$ é um ideal de A e f é injetiva se, e somente se, $N(f) = \{0\}$.
(iii) Os anéis $A/N(f)$ e $Im(f)$ são naturalmente isomorfos.

Provamos, agora, um resultado que servirá de lema para a demonstração do teorema principal dessa dissertação:

Proposição 2.5.3. *Sejam A e B anéis comutativos e $f : A \to B$ um homomorfismo. Se P é um ideal primo de B, então $f^{-1}(P)$ é um ideal primo de A.*

Demonstração. Usando a definição em 2.4.1, devemos mostrar que se $a, b \in A$ são tais que $a \cdot b \in f^{-1}(P)$, então $a \in f^{-1}(P)$ ou $b \in f^{-1}(P)$. Ora, como $a \cdot b \in f^{-1}(P)$, temos que $f(a \cdot b) = f(a) \cdot f(b) \in P$. A partir daí, como P é um ideal primo de B, segue que $f(a) \in P$ ou $f(b) \in P$. Assim, $a \in f^{-1}(P)$ ou $b \in f^{-1}(P)$. □

2.6 Domínios de fatoração única, de ideais principais e anéis noetherianos

Ao longo desta seção, estendemos a anéis algumas definições e resultados próprios da Teoria dos Números elementar.

Em tudo o que segue, D é um anel comutativo, com zero 0 e unidade 1.

Definição 2.6.1. *Seja $a \in D$. Um elemento $b \in D$ é um divisor ou fator de a (em D) se existe $c \in D$ tal que $a = b \cdot c$. Nesse caso, dizemos também que b divide a, ou que a é múltiplo de b.*

Definição 2.6.2. *Um elemento $a \in D$ é invertível (em D) se existe $b \in D$ tal que $a \cdot b = 1$. Denotamos por $D^\times$ o conjunto dos elementos invertíveis de D.*

Definição 2.6.3. *Dois elementos a e b de D são associados (em D) se existe $u \in D^\times$ tal que $a = u \cdot b$.*

Definição 2.6.4. *Deja D um anel. Um elemento $a \in D \setminus (D^\times \cup \{0\})$ é irredutível (em D) se a possui apenas a fatoração trivial em D, isto é, se $a = b \cdot c$, com $b, c \in D$, então $b \in D^\times$ ou $c \in D^\times$.*

Ainda em relação à definição anterior, observe que os únicos divisores de um elemento irredutível a de D são os elementos associados a a em D e os elementos invertíveis de D.

Definição 2.6.5. *Um elemento $p \in D \setminus D^\times$ é primo se o ideal gerado por ele for primo. Em termos da noção de divisibilidade em D, temos que p é primo se a seguinte condição for satisfeita:*

$$\forall a, b \in D,\ p | a \cdot b \Longrightarrow p \mid a \text{ ou } p \mid b.$$

Definição 2.6.6. *Dados elementos $a_1, \cdots, a_n \in D$ não todos nulos, um elemento $d \in D$ é um maior divisor comum (abreviamos MDC) de $a_1, \cdots, a_n$ se d divide $a_1, \cdots, a_n$ e se todo elemento de D que divide $a_1, \cdots, a_n$ também divide d.*

Lema 2.6.1. *Sejam D um domínio e $a_1, \cdots, a_n \in D$, não todos nulos. Então, dois MDC$'$s para $a_1, \cdots, a_n$ são, necessariamente, associados em D.*

Demonstração. Sejam d_1 e d_2 dois *MDC*$'$*s* de $a_1, \cdots, a_n$. Pela definição 2.6.6, temos que $d_1 | a_i$ para cada $i \in \{1, \ldots, n\}$. Ainda pela mesma definição, segue que $d_1 | d_2$ e, portanto, existe $k_1 \in D$ tal que $d_2 = d_1 \cdot k_1$. Analogamente, seguindo os mesmos passos anteriores, existe $k_2 \in D$ tal que $d_1 = k_2 \cdot d_2$. Consequentemente, $d_2 = d_1 \cdot k_1 = (k_2 \cdot k_1) \cdot d_2$. Mas, como D é um domínio e $d_2 \neq 0$, segue que $k_2 \cdot k_1 = 1$, de sorte que d_1 é associado a d_2. □

O lema anterior ensina que, em um domínio, temos a unicidade, a menos de multiplicação por elementos invertíveis, do *MDC*. Em um anel comutativo qualquer não temos a unicidade, em geral. Por isso, consideraremos a noção de *MDC* apenas em domínios, de forma que poderemos falar (a menos da multiplicação por elementos invertíveis) do *MDC* de $a_1, \cdots, a_n$, o qual denotaremos por

$$MDC\{a_1, \cdots, a_n\}.$$

Definição 2.6.7. *Os elementos não todos nulos $a_1, \cdots, a_n$ de um domínio D são dito primos entre si ou relativamente primos se $MDC\{a_1, \cdots, a_n\}$ existe e é igual a* 1.

Definição 2.6.8. *O domínio D é um domínio fatorial ou domínio de fatoração única (abreviamos DFU) se todo elemento não nulo e não invertível de D se escreve de maneira única (a menos de reordenação e multiplicação por invertíveis) como produto de elementos irredutíveis de D. Em símbolos:*

(i) Todo elemento não nulo e não invertível de D pode ser escrito como um produto de fatores irredutíveis.

(ii) Se $\{p_i\}_{1 \leq i \leq s}$ *e* $\{q_j\}_{1 \leq j \leq t}$ *são famílias finitas de elementos irredutíveis de D, tais que* $p_1 \cdot p_2 \cdot \ldots \cdot p_s = q_1 \cdot q_2 \cdot \ldots \cdot q_t$*, então:*

- $s = t$.
- *a menos de ordenação,* p_i *é associado a* q_i *para* $i = 1, \ldots, s$ *(isto é, existe uma bijeção* σ *de* $\{1, \cdots, s\}$ *em si mesmo tal que* p_i *é associado a* $q_{\sigma(i)}$ *para* $i = 1, 2 \ldots, s$.

Proposição 2.6.1. *Seja D um DFU. Se* $a, b \in D$ *não são ambos nulos, então* $MDC\{a, b\}$ *existe.*

Demonstração. Podemos supor que $a, b \neq 0$. Também, é claro que $MDC\{a, b\} = a$ se a for invertível ou $MDC\{a, b\} = b$ se b for invertível.

Se a e b não são invertíveis, sejam $a = p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$ e $b = p_1^{l_1} \cdot \ldots \cdot p_n^{l_n}$, com $p_1, \ldots, p_n$ irredutíveis dois a dois não associados e $k_1, \ldots, k_n$, $l_1, \ldots, l_m$ inteiros não negativos. Como na Teoria dos Números elementar, definimos

$$d = p_1^{a_1} \cdot \ldots \cdot p_n^{a_n},$$

com $a_i = \min\{k_i, l_i\}$ para $1 \leq i \leq n$. Também como lá, é imediato verificar que d é o MDC de a e b. □

Note que essencialmente a mesma demonstração anterior mostra que, em um DFU, existe o MDC de uma quantidade qualquer finita de elementos $a_1, \cdots, a_n \in D$, não todos nulos.

Definição 2.6.9. *Um domínio no qual todo ideal é principal é chamado um domínio principal ou domínio de ideais principais (abreviamos DIP).*

É possível provar (veja a bibliografia citada no início deste capítulo) que todo DIP é um DFU.

Mais geralmente que os DIP, temos a importante classe dos *anéis noetherianos*.

Definição 2.6.10. *Um anel no qual todo ideal é finitamente gerado é dito noetheriano.*

Definição 2.6.11. *Uma cadeia ascendente*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \cdots$$

de ideais de um anel é estacionária se existe $n \in \mathbb{N}$ tal que $I_k = I_n$ para todo $k \geq n$.

Teorema 2.6.2. *Seja A um anel. Então A é Noetheriano se e somente se toda cadeia ascendente de ideais de A é estacionária.*

Demonstração. Suponha A noetheriano. Mostraremos que toda cadeia ascendente de ideais de A é estacionária. Desta forma , seja $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ uma cadeia ascendente de ideais de A. Prova-se facilmente que $I = \bigcup_{n\geq 1} I_n$ é um ideal de A e portanto, por hipótese ,finitamente gerado. Seja assim $\alpha_1, \ldots, \alpha_n$ os geradores de I em A, isto é, $I = (\alpha_1, \ldots, \alpha_n)$. Claramente temos $\alpha_1 \in I_{m_1}$,$\alpha_2 \in I_{m_2}$,...,$\alpha_m \in I_{m_n}$ e denotando $t = max\{ m_1, m_2, \ldots, m_n\}$ temos

$$I = (\alpha_1, \ldots, \alpha_m) \subseteq I_t \subseteq I_k \subseteq I$$

para cada $k \in \mathbb{N}$ com $k \geq t$. Isto mostra que $I_k = I_t$ para $k \geq t$ e , portanto , a cadeia ascedente é estacionária.Suponha agora que toda cadeia ascendente de A é estacionária e que A não seja noetheriano.Segue então que existe um ideal I de A que não é finitamente gerado.Construiremos assim uma cadeia ascedente de ideais que não é estacionária gerando um absurdo e provando que A é noetheriano . Tomemos assim $\alpha_1 \in I$; $\alpha_2 \in I \backslash (\alpha_1)$;$\alpha_3 \in I \backslash (\alpha_1, \alpha_2)$ e assim sucessivamente. Notemos que sempre exitse $\alpha_n \in I \backslash (\alpha_1, \alpha_2, \cdots, \alpha_{n-1})$ uma vez que o ideal I não é finitamente gerado, e em particular, temos que $I \underset{\neq}{\supset} (\alpha_1, \alpha_2, \cdots, \alpha_{n-1})$. Desta maneira obtemos a cadeia ascendente não-estacionária abaixo

$$(\alpha_1) \underset{\neq}{\subset} (\alpha_1, \alpha_2) \underset{\neq}{\subset} (\alpha_1, \alpha_2, \alpha_3), \cdots, \underset{\neq}{\subset} (\alpha_1, \alpha_2, \cdots, \alpha_n), \cdots$$

□

2.7 Característica de um anel e corpo de frações de um domínio

Nesta seção, trazemos algumas definições e teoremas relativos à noção de característica de um anel, bem como tecemos alguns comentários sobre o corpo de frações de um domínio. Começaremos definindo a ordem de um elemento de um anel. As demonstrações omitidas podem ser encontradas na bibliografia (ENDLER, 1972).

Em tudo o que segue, A é um anel comutativo com unidade.

Definição 2.7.1. *Seja $a \in A$. Se o conjunto $\{m \in \mathbb{N} \setminus \{0\}; m \cdot z = O_A\}$ for não vazio, definimos a ordem de z, denotada por $o(a)$, como sendo seu menor elemento. Caso contrário, definimos $o(a) = \infty$.*

Alguns resultados simples que são válidos em um anel A são que:

a) $o(a) = 1$ se, e somente se, $a = 0_A$.

b) Se $n \cdot a = 0$, então $o(a)$ divide n.

c) Se $o(1_A) \neq \infty$, então $o(a)$ divide $o(1_A)$.

d) Se $o(a) \neq o(1_A)$, então a é um divisor de zero de A.

Agora, definiremos a característica de um anel comutativo com unidade.

Definição 2.7.2. *Seja A um anel comutativo com unidade 1_A. Definimos a característica de A, denotada $car(A)$, por :*

$$car(A) = \begin{cases} 0, \text{ se } o(1_A) = \infty \\ n, \text{ se } o(1_A) = n \neq \infty \end{cases}$$

Se $car(A) = 0$, diremos que A tem característica zero; se $car(A) = n \neq \infty$, diremos que A tem característica finita.

É obvio que todo subanel de A tem a mesma característica que A. Em particular, a característica depende apenas do *subanel primo* de A, isto é, da interseção de todos os subanéis não nulos de A.

Proposição 2.7.1. *Se A é um anel comutativo com unidade, então temos que:*

(a) $car(A) = 1$ se, e somente se, A for trivial.

(b) Se A for um domínio, então $car(A) = 0$ ou p, um número primo. Neste caso, temos $o(a) = \infty$, respectivamente p, para todo $a \in A \setminus \{0\}$.

Agora, falaremos brevemente sobre o corpo de frações de um domínio. Um subanel de um corpo é, obviamente, um domínio. Por outro lado, todo domínio A é um subanel de um corpo, a saber seu *corpo de frações*, o qual é construído de maneira análoga à construção de $\mathbb{Q}$ a partir de $\mathbb{Z}$. Precisamente, como conjunto, $cf(A)$ é definido como o quociente do conjunto $A \times (A \setminus \{0\})$ pela relação (de equivalência)

$$(x, y) \sim (x', y') \Leftrightarrow x \cdot y' = x' \cdot y$$

(aqui, $x,x' \in A$ e $y,y' \in A \setminus \{0\}$). As classes de equivalência são chamadas "*frações*"; para $(x,y) \in A \times (A\setminus\{0\})$, denotamos a classe correspondente por $\frac{x}{y}$.

Tornamos $cf(A)$ um corpo com as operações (bem definidas) de adição e multiplicação dadas por

$$\frac{x}{y}+\frac{w}{z}=\frac{xz+wy}{yz};\ \ \frac{x}{y}\cdot\frac{w}{z}=\frac{xw}{yz}.$$

Por fim, o anel A pode ser considerado como subanel de $cf(A)$ pela identificação $x \approx \frac{x}{1}$, a qual tem sentido pelo fato de que a aplicação $x \mapsto \frac{x}{1}$, de A em $cf(A)$, é um homomorfismo injetor de anéis.

3 EXTENSÕES DE CORPOS E MÓDULOS

Neste capítulo, continuamos a expor conceitos e resultados preliminares, desta vez relativos a extensões de corpos e módulos. Optamos por separar estes conteúdos daqueles do capítulo anterior por entender que várias partes do que segue são bem menos elementares do que fizemos até agora.

3.1 Extensões de Corpos

A partir de agora trataremos de extensões de corpos. Todas as demonstrações das afirmações não provadas podem ser encontradas no capítulo 3 de (ASH, 2013).

Definição 3.1.1. *Se F e E são corpos, e $F \subseteq E$; dizemos que E é uma extensão de F, e escrevemos $F \leq E$ ou $E|F$.*

Se E é uma extensão de F, então, em particular, podemos ver E como um grupo abeliano em relação à adição. Multiplicando o "vetor" $x \in E$ pelo "escalar" $\lambda \in F$ utilizando a multiplicação de E, vemos facilmente que todos os axiomas da definição de espaço vetorial são satisfeitos. Assim, podemos considerar E como um espaço vetorial sobre F. A dimensão deste espaço vetorial é o *grau* da extensão e será denotado por $[E : F]$. Caso $[E : F] < \infty$, dizemos que E é uma *extensão finita* de F, que a extensão $E|F$ é finita ou, ainda, que E é de grau n sobre F, onde $n = [E : F]$.

O resultado a seguir é utilizado na demonstração do importante Teorema 3.1.1.

Lema 3.1.1. *Seja $f : F \longrightarrow E$ um homomorfismo de corpos com $f(1_F) = 1_E$, então f é um monomorfismo, isto é, é injetivo.*

Teorema 3.1.1. *Seja f um polinômio não constante sobre o corpo F. Então, existe uma extensão finita $E|F$ e um elemento $\alpha \in E$ tal que $f(\alpha) = 0$.*

Definição 3.1.2. *Se E é uma extensão de F, um elemento $\alpha \in E$ é algébrico sobre F se existir um polinômio não nulo $f \in F[x]$ tal que $f(\alpha) = 0$. Se α não for algébrico sobre F, dizemos que α é transcendente sobre F.*

Definição 3.1.3. *Se E é uma extensão de F e cada elemento de E é algébrico sobre F, dizemos que E é uma extensão algébrica de F, ou simplesmente que $E|F$ é algébrica.*

O resultado a seguir é uma decorrência imediata do fato de que, em todo espaço vetorial de dimensão finita sobre um corpo, um conjunto de vetores com mais elementos do que a dimensão é LD.

Teorema 3.1.2. *Se $E|F$ é uma extensão finita, então $E|F$ é uma extensão algébrica.*

A seguir, centramos nossa atenção num elemento da extensão E de F.

Definição 3.1.4. *Seja $E|F$ uma extensão de corpos e $\alpha \in E$ algébrico sobre F. Um polinômio mônico $m(x)$ sobre F é um polinômio minimal de α sobre F se $I = (m(x))$, onde $I = \{g \in F[x]; g(\alpha) = 0\}$.*

Nas notações da definição anterior, um polinômio minimal $m(x)$ de α sobre F tem as seguintes propriedades:

1) Se $g \in F[x]$, então $g(\alpha) = 0$ se, e somente se, $m(x)$ divide $g(x)$.

2) $m(x)$ é o polinômio mônico de menor grau tal que $m(\alpha) = 0$.

3) $m(x)$ é o único polinômio irredutível tal que $m(\alpha) = 0$.

Para o que segue, dadas uma extensão de corpos $E|F$ e $\alpha \in E$, denotamos por $F(\alpha)$ o menor subcorpo de E que contém F e α, e por $F[\alpha]$ o menor subanel de E que contém F e α. É imediato mostrar que

$$F[\alpha] = \{f(\alpha); f \in F[x]\}.$$

Teorema 3.1.3. *Seja $E|F$ uma extensão de corpos e $\alpha \in E$ algébrico sobre F. Se o polinômio minimal $m(x)$ de α sobre F tem grau n, então $F(\alpha) = F[\alpha]$. Mais precisamente, nesse caso:*

(a) $F[\alpha] = \{0\} \cup \{f(\alpha); f \in F[x] \setminus \{0\}$ *tem grau menor que* $n\}$.

(b) $\{1, \alpha, \ldots, \alpha^{n-1}\}$ *forma uma base para o espaço vetorial $F(\alpha)$ sobre o corpo F.*

Consequentemente $[F(\alpha) : F] = n$.

Proposição 3.1.4. *Suponha que $F \leq K \leq E$ são corpos, e sejam $\{\alpha_i; i \in I\}$ e $\{\beta_j; j \in J\}$ bases de E sobre K e de K sobre F, respectivamente. Então, $\{\alpha_i\beta_j; i \in I, j \in J\}$ forma uma base de E sobre F.*

Na proposição anterior, os conjuntos I e J não precisam ser finitos. De qualquer forma, o resultado a seguir é uma consequência imediata dela.

Teorema 3.1.5. *Se $F \leq K \leq E$ são corpos, então $[E : F] = [E : K] \cdot [K : F]$. Em particular, $[E : F]$ é finito se e, somente se, $[E : K]$ e $[K : F]$ são também finitos.*

Se f é um polinômio sobre o corpo F, então, pelo Teorema 3.1.1, podemos encontrar uma extensão E_1 de F contendo uma raiz α_1 de f. Caso E_1 não contenha todos as raízes de f, então podemos encontrar uma outra extensão E_2 de E_1 contendo alguma outra raiz α_2 de f. Se continuarmos esse processo, eventualmente chegaremos a uma extensão de F na qual o polinômio f se fatora completamente.

As considerações acima motivam a próxima definição. Para seu enunciado, se E é uma extensão de F e $\alpha_1, \cdots, \alpha_k \in E$, usaremos a notação $F(\alpha_1, \cdots, \alpha_k)$ para o menor subcorpo de E gerado por F e $\alpha_1, \cdots, \alpha_k$. Prova-se facilmente que $F(\alpha_1, \cdots, \alpha_k)$ é a coleção de todas as funções racionais em α_i, com $i = 1, 2, \cdots, n$ e que $[F(\alpha_1, \cdots, \alpha_k) : F] < \infty$.

Definição 3.1.5. *Se E é uma extensão de F e $f \in F[x]$, dizemos que f se decompõe sobre E se f pode ser escrito como*

$$f(x) = \lambda \cdot (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k),$$

para certos $\alpha_1, \cdots, \alpha_k \in E$ e $\lambda \in F$.

Definição 3.1.6. *Se K é uma extensão de F e $f \in F[x]$, dizemos que K é um corpo de decomposição para f sobre F se f se decompõe sobre K mas não sobre qualquer subcorpo de K contendo F.*

Damos, agora, uma condição equivalente para que uma extensão K de um corpo F seja um corpo de decomposição de um polinômio $f \in F[x]$.

Proposição 3.1.6. *Sejam F um corpo, $f \in F[x]$ e K uma extensão de F. Então, K é um corpo de decomposição para f se f se decompõe sobre K e K é gerado sobre F pelas raízes $\alpha_1, \cdots, \alpha_n$.*

É possível provar o seguinte

Teorema 3.1.7. *Se $f \in F[x]$ e o grau de f é menor do que ou igual a n, então f tem um corpo de decomposição K sobre F com $[K : F] \leq n!$.*

O próximo resultado nos mostra que se α e β são raízes de um mesmo polinômio irredutível $f \in F[x]$, então necessariamente $F(\alpha)$ e $F(\beta)$ são corpos isomorfos.

Teorema 3.1.8. *Se α e β são raízes do polinômio irredutível $f \in F[x]$ em uma extensão E de F, então $F(\alpha)$ é isomorfo a $F(\beta)$ via um isomorfismo que leva α em β e é a identidade em F.*

Nas condições do enunciado do teorema anterior, dizemos que α e β são elementos *conjugados* uma do outro.

Consideremos, agora, um polinômio não constante f de graun n sobre os complexos. É possível que f não tenha qualquer raiz racional ou real. No entanto, o Teorema Fundamental da Álgebra garante que f tem sempre n raízes complexas, repetidas de acordo com suas multiplicidades. Em outras palavras, f pode ser escrito como:

$$f(x) = \lambda \cdot (x - \alpha_1) \cdot (x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n),$$

com $\lambda, \alpha_1, \ldots, \alpha \in \mathbb{C}$.

Esta situação pode ser replicada para qualquer corpo, isto é, dado um corpo F, podemos construir uma extensão algébrica C de F com a seguinte propriedade: qualquer polinômio em $C[x]$ pode ser decomposto sobre C. A próxima proposição dá condições equivalentes para que isto aconteça.

Proposição 3.1.9. *Se C é um corpo, as seguintes condições são equivalentes:*

(a) Cada polinômio $f \in C[x]$ tem pelo menos uma raiz em C.

(b) Cada polinômio não constante $f \in C[x]$ se decompõe em C.

(c) Cada polinômio irredutível $f \in C[x]$ é linear.

(d) C não tem extensões algébricas próprias.

Definição 3.1.7. *Dizemos que um corpo C é algebricamente fechado se C satisfaz uma qualquer das condições equivalentes da proposição anterior.*

Definição 3.1.8. *Uma extensão C de um corpo F é um fecho algébrico de F se C é algébrico sobre F e C é algebricamente fehado.*

Proposição 3.1.10. *Se E é gerado sobre F por elementos $\alpha_1, \ldots, \alpha_n$ algébricos sobre F, isto é, se $E = F(\alpha_1, \ldots, \alpha_n)$), então E é uma extensão finita de F.*

Corolário 3.1.1. *Se E é uma extensão de F e A é o conjunto de todos os elementos em E que são algébricos sobre F, então A é um subcorpo de E.*

Nas notações do enunciado do corolário anterior, dizemos que A é o *fecho algébrico* de F em E. O próximo corolário garante a transitividade de extensões algébricas.

Corolário 3.1.2. *Se E é algébrico sobre K e K é algébrico sobre F, então E é algébrico sobre F.*

Proposição 3.1.11. *Se C é uma extensão algébrica de F, então C é um fecho algébrico de F se, e somente se, cada polinômio não constante em $F[x]$ se decompõe sobre C.*

Investigaremos, agora, a multiplicidade de raízes de polinômios.

Definição 3.1.9. *Um polinômio irredutível $f \in F[x]$ é separável se f não tem raízes repetidas em um corpo de decomposição. Caso contrário, dizemos que f é inseparável. Se f é um polinômio arbitrário não necessariamente irredutível, diremos que f é separável se cada um de seus fatores irredutíveis o for.*

Para o que segue, dados um corpo F e $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$, definimos a *derivada* de f como o polinômio f' dado por:

$$f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}.$$

É imediato verificar que essa definição, apesar de meramente formal, ainda retém todas as propriedades algébricas elementares de derivadas de polinômios, tais como as regras de derivação de somas, produtos e a regra da cadeia.

Proposição 3.1.12. *Sejam F um corpo e $f \in F[X] \setminus \{0\}$. Se g é o maior divisor comum de f e f', então f tem raízes repetidas em um corpo de decomposição se, e somente se, o grau de g for pelo menos* 1.

Corolário 3.1.3.

(a) Sobre um corpo de característica zero, todo polinômio é separável.

(b) Sobre um corpo F de característica p, um polinômio irredutível f é inseparável se, e somente se, f' é o polinômio zero; equivalentemente f é um polinômio em x^p.

Proposição 3.1.13. *Sobre um corpo finito todo polinômio é separável.*

Para a definição a seguir, se E é uma extensão de F e $\alpha \in E$ é algébrico sobre F, denotamos por $\min(\alpha, F)$ o polinômio minimal de α sobre F.

Definição 3.1.10. *Se E é uma extensão de F e $\alpha \in E$, então α é separável sobre F se α é algébrico sobre F e* $\min(\alpha, F)$ *é um polinômio separável.*

Definição 3.1.11. *Seja E uma extensão de F. Se cada elemento de E é separável sobre F, dizemos que E é uma extensão separável de F, que $E|F$ é separável ou, ainda, que E é separável sobre F.*

É possível provar a seguinte

Proposição 3.1.14. *Sejam $F \leq K \leq E$ corpos. Se E é separável sobre F, então E é separável sobre K e K é separável sobre F.*

A recíproca, isto é, a transitividade da noção de separabilidade, também é verdadeira, mas é bem mais difícil de ser demonstrada. Faremos isto a partir de agora.

Lema 3.1.2. *Seja E uma extensão algébrica de um corpo F, de característica prima p, e seja $\alpha \in E$. Se $m(x) = \min(\alpha, F(\alpha^p))$, então $m(x)$ se decompõe sobre E e α é a única raiz de $m(x)$. Consequentemente $m(x)$ é uma potência de $x - \alpha$.*

Demonstração. Temos que α é uma raiz de $x^p - \alpha^p = (x-\alpha)^p$. Assim, pelas propriedades do polinômio minimal dadas logo após a Definição 3.1.4, teremos que $m(x)|(x-\alpha)^p$ e, portanto, $m(x) = (x-\alpha)^r$, para algum $r \in \{1, \ldots, p\}$. Logo, $m(x)$ se decompõe sobre E e α é sua única raiz. □

Lema 3.1.3. *Seja E uma extensão algébrica de um corpo F de característica prima p, seja $\alpha \in E$ e $m(x) = \min(\alpha, F(\alpha^p))$. Se α for separável sobre $F(\alpha^p)$, então $\alpha \in F(\alpha^p)$.*

Demonstração. Sendo α separável sobre $F(\alpha^p)$, segue que $m(x) = (x-\alpha)^r$ não pode ter raízes repetidas em nenhum corpo de decomposição. Logo, devemos ter $r = 1$ e, portanto, $m(x) = x - \alpha$. Consequentemente, $\alpha \in F(\alpha^p)$. □

Definição 3.1.12. *Um corpo F é perfeito se todo polinômio não nulo sobre F for separável. Equivalentemente, F é perfeito se toda extensão algébrica de F for separável.*

Teorema 3.1.15. *Seja F um corpo de característica prima p. Então, F é perfeito se, e somente se, todo elemento de F for uma p-ésima potência de um elemento de F.*

Demonstração. Suponha primeiramente que todo elemento de F é uma p-ésima potência de um elemento de F; mostremos que F é perfeito. Seja $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ um polinômio irredutível com raízes repetidas em algum corpo de decomposição. Pelo Corolário 3.1.3, f tem a forma

$$f(x) = a_0 + a_1 x^p + \cdots + a_n x^{np}.$$

Por hipótese, temos que $a_i = b_i^p$ para $1 \leq i \leq n$, de sorte que

$$f(x) = a_0 + a_1 x^p + \ldots + a_n x^{np} = b_0^p + b_1^p x^p + \ldots + b_n^p x^{np} = (b_0 + b_1 x + \ldots + b_n x^n)^p.$$

Mas isso contradiz a irredutibilidade de f. Logo, F é perfeito.

Agora, suponha que F é perfeito. Seja $b \in F$ e $f(x) = x^p - b$ um polinômio sobre F. Adjuntando uma raiz α de F, temos $\alpha^p = b$ nessa extensão. Consequentemente $F(\alpha^p) = F(b) = F$. Por hipótese, temos que α é separável sobre $F = F(\alpha^p)$, logo, pelo Lema 3.1.3, temos $\alpha \in F$. Desta forma, $b = \alpha^p$, com $\alpha \in F$. □

Observação 3.1.16. *Como consequência do Teorema anterior podemos escrever $F = F^p$.*

Seja E uma extensão de corpos de característica prima p. Para o que segue, denotaremos por $K = F(E^p)$ o subcorpo de E obtido pela adjunção a F das potências p-ésimas de todos os elementos de E.

Lema 3.1.4. *Seja $E|F$ uma extensão finita de corpos, de característica prima p. Então, $F(E^p)$ consiste de todas as combinações lineares finitas de elementos em E^p, com coeficientes em F.*

Demonstração. Como $[E : F] < \infty$, podemos tomar uma base $\{\alpha_1, \cdots, \alpha_n\}$ de E sobre F. Mostremos que $K = F(\alpha_1^p, \ldots, \alpha_n^p)$.

Temos que $F \subset F(E^P)$ e que $\alpha_i^p \in E^p$ para $1 \leq i \leq n$. Logo, $F(\alpha_1^p, \ldots, \alpha_n^p) \subseteq F(E^p)$, já que $F(\alpha_1^p, \ldots, \alpha_n^p)$ é o menor subcorpo de E que contém F e $\{\alpha_1^p, \ldots, \alpha_n^p\}$.

Para mostrarmos que $F(E^p) \subset F(\alpha_1^p, \ldots, \alpha_n^p)$, basta mostrarmos que $E^p \subseteq F(\alpha_1^p, \ldots, \alpha_n^p)$. Para tanto, se $a \in E^p$, temos que $a = b^p$, para algum $b \in E$. Como $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de E sobre F, temos $b = b_1\alpha_1 + \cdots + b_n\alpha_n$, para certos $b_1, \ldots, b_n \in F$. Assim, o fato de os corpos envolvidos terem característica p, juntamente com a fórmula de expansão binomial e as congruências $\binom{p}{k} \equiv 0 \pmod{p}$ (para $1 \leq k < p$) dão

$$b^p = b_1^p \cdot \alpha_1^p + \cdots + b_n^p \cdot \alpha_n^p.$$

Dessa forma, $a \in F(\alpha_1^p, \ldots, \alpha_n^p)$.

Agora, mostremos que $F(E^p)$ consiste de todas as combinações lineares finitas de elementos em E^p com coeficientes em F. Ora, como α_1 é algébrico sobre F, os elementos de $F(\alpha_1^p)$ podem ser expressos como polinômios em α_1^p com coeficientes em F. Também, sendo α_2^p algébrico sobre F, consequentemente sobre $F(\alpha_1^p)$, vemos que cada elemento de $F(\alpha_1^p, \alpha_2^p)$ pode ser escrito como um polinômio em α_2^p com coeficientes em $F(\alpha_1^p)$. Logo, um elemento de $F(\alpha_1^p, \alpha_2^p)$ tem a forma

$$\sum_s \left(\sum_r b_{rs} \alpha_1^{pr} \right) \alpha_2^{ps},$$

com $b_{rs} \in F$. Prosseguindo indutivamente desta forma, obtemos o resultado desejado.

h □

Observação 3.1.17. *Temos que um produto da forma $\alpha_1^{pr_1} \cdot \alpha_2^{pr_2} \cdot \ldots \cdot \alpha_n^{pr_n}$ pode ser escrito como $c_1\alpha_1^p + \cdots + c_n\alpha_n^p$, com $c_1, \ldots, c_n \in F$. De fato, $\alpha_1^{pr_1} \cdot \alpha_2^{pr_2} \cdot \ldots \cdot \alpha_n^{pr_n} = (\alpha_1^{r_1} \cdot \alpha_2^{r_2} \cdot \ldots \cdot \alpha_n^{r_n})^p$; como $\alpha_1^{r_1}, \ldots, \alpha_n^{r_n} \in E$, segue que $\alpha_1^{r_1} \cdot \alpha_2^{r_2} \cdot \ldots \cdot \alpha_n^{r_n} = d_1\alpha_1 + \ldots + d_n\alpha_n$, para certos $d_1, \ldots, d_n \in F$. Logo,*

$$(\alpha_1^{r_1} \cdot \alpha_2^{r_2} \cdot \ldots \cdot \alpha_n^{r_n})^p = (d_1\alpha_1 + \ldots + d_n\alpha_n)^p = d_1^p\alpha_1^p + \ldots + d_n^p\alpha_n^p.$$

Fazendo $c_i = d_i^p$ para $i = 1, \ldots, n$, temos o resultado desejado.

Lema 3.1.5. *Seja E uma extensão finita do corpo F, de característica prima p. Se os elementos $y_1, \ldots, y_r \in E$ são linearmente independentes sobre F, então $y_1^p, \ldots, y_r^p$ são também linearmente independentes sobre F.*

Demonstração. Estendamos $\{y_1, \ldots, y_r\}$ a uma base $\{y_1, \ldots, y_n\}$ de E sobre F. Pela observação anterior, cada elemento $y \in E$ tem a forma $y = a_1y_1^p + \ldots + a_ny_n^p$, com $a_i \in F$ para $1 \leq i \leq n$. Assim, $\{y_1^p, \ldots, y_n^p\}$ gera E sobre F, logo, $\{y_1^p, \ldots, y_n^p\}$ contém uma base de E sobre F. Mas, uma vez que uma tal base contém exatamente n vetores, concluímos que $\{y_1^p, \ldots, y_n^p\}$ é L.I. Então, $\{y_1^p, \ldots, y_r^p\}$, por ser um subconjunto de um conjunto L.I., também é L.I. □

Teorema 3.1.18. *Seja E uma extensão finita do corpo F, de característica prima p. Então, E é separável sobre F se, e somente se, $E = F(E^p)$.*

Demonstração. Suponha que E é uma extensão separável sobre F e seja $\alpha \in E$. Então, α é separável sobre F, consequentemente sobre $F(\alpha^p)$. Logo, $\alpha \in F(\alpha^p)$, pelo Lema 3.1.3, e, portanto, $\alpha \in F(E^p)$. Consequentemente $E = F(E^p)$.

Reciprocamente, suponha que $E = F(E^p)$ mas que a extensão $E|F$ não seja separável. Então, existe $\alpha \in E$ tal que o polinômio minimal $m(x)$ de α sobre F é inseparável. Desta forma, pelo Corolário 3.1.3, item b, $m(x)$ tem a forma

$$m(x) = b_0 + b_1x^p + \ldots + b_{r-1}x^{(r-1)p} + x^{rp},$$

para certos $r \in \mathbb{N}$ e $b_0, b_1, \ldots, b_{r-1} \in F$. Como $m(\alpha) = 0$, os elementos 1, α^p, ..., α^{rp} formam um conjunto L.D. sobre F. Mas, pela minimalidade do grau de $m(x)$, temos que 1, α, ..., α^{rp-1} também forma um conjunto L.I. sobre F. Consequentemente, 1, α, ..., α^r é um conjunto

L.I. sobre F. Para ver isto, basta notar que $rp-1 \geq 2r-1 \geq r$. Assim, pelo Lema 3.1.5, $\{1, \alpha^p, \ldots, \alpha^{rp}\}$ é L.I. sobre F, o que é um absurdo. Logo, $E|F$ é separável. □

Chegamos finalmente ao resultado desejado.

Teorema 3.1.19. *Sejam $F \leq K \leq E$ corpos, com $[E:F] < \infty$. Se E é separável sobre K e K é separável sobre F, então E é separável sobre F.*

Demonstração. Sobre um corpo de característica zero, qualquer extensão é separável (Corolário 3.1.3). Suponhamos, pois, que F tem característica finita p. Pelo teorema anterior, temos que $E = K(E^p)$ e $K = F(K^p)$; logo, $E = F(K^p, E^p) = F(E^p)$, já que $K \leq E$. Portanto, novamente pelo teorema anterior, $E|F$ é separável. □

Lema 3.1.6. *Seja $E = F(\alpha_1, \ldots, \alpha_n)$, onde cada α_i é algébrico e separável sobre F. Então, E é separável sobre F.*

Demonstração. Fazendo $E_i = F(\alpha_1, \ldots, \alpha_i)$ (equivalentemente, $E_{i+1} = E_i(\alpha_{i+1})$), mostremos primeiramente que

$$E_{i+1} = E_i(E_{i+1}^p), \ \ \forall i = 1, \ldots, n-1.$$

Ora, temos que E_{i+1}^p e E_i estão ambos contidos em E_{i+1}; portanto, $E_i(E_{i+1}^p) \subseteq E_{i+1}$, já que $E_i(E_{i+1}^p)$ é o menor subcorpo de E contém E_i e E_{i+1}^p. Uma vez que $E_{i+1} = E_i(\alpha_{i+1})$, basta mostrar que $\alpha_{i+1} \in E_i(E_{i+1}^p)$ para obtermos $E_{i+1} \subseteq E_i(E_{i+1}^p)$. Por hipótese, α_{i+1} é algébrico sobre F, consequentemente, sobre E_{i+1}^p. Logo, pelo Lema 3.1.3, $\alpha \in E_i(\alpha_{i+1}^p) \subseteq E_i(E_{i+1}^p)$ e, assim, $E_{i+1} = E_i(E_{i+1}^p)$.

Agora, mostremos por indução sobre n que $E = F(\alpha_1, \ldots, \alpha_n)$ é separável sobre F. Para $n = 0$ a afirmação é óbvia, já que $F|F$ é uma extensão separável. Agora, suponhamos que ela seja válida para um certo i e mostremos sua validade também para $i+1$. Pelo Teorema 3.1.18 E_{i+1} é separável sobre E_i. Como, por hipótese, E_i é separável sobre F, segue do Teorema 3.1.19 que E_{i+1} é separável sobre F. Logo, $E|F$ é separável. □

A demonstração do resultado a seguir é trivial.

Lema 3.1.7. *Seja $\sigma : E \to E$ um $F-$homomorfismo. Assuma que os polinômios $f \in F[x]$ se decompõem sobre E. Se α é raiz de f em E, então $\sigma(\alpha)$ também o é. Desta forma, σ permuta as raízes de f.*

No resultado a seguir, tomamos C como um fecho algébrico de um corpo E e contamos o número de $F-$homomorfismos de E em C. Usaremos a notação $g = \sigma(f)$ para signficar que se a_i é um dos coefiente de f, então o coeficiente correspondente de g será dado por $\sigma(a_i)$.

Teorema 3.1.20. *Sejam $E|F$ uma extensão finita de grau n e separável, e σ um mergulho de F em C. Então, σ se estende para exatamente n mergulhos de E em C. Em outras palavras, existem exatamente n mergulhos de γ, de F em C, tais que a restrição $\gamma|_F$ de γ a F coincide com σ. Em particular, tomando σ como a inclusão de F em C, concluímos que existem exatamente n $F-$homomorfismos de E em C que a estendem.*

Demonstração. Usaremos indução sobre n. Para $n = 1$ teremos que $E = F$ e neste caso não há nada o que provar.Logo assumiremos $n > 1$ e suporemos o resultado válido para $n = 2, 3, \cdots, k-1$. Mostraremos assim que o resultado é valido para k. Desta forma escolhamos um elemento α de modo que $\alpha \in E$ mas $\alpha \notin F$. Sendo f o polinômio minimal de α, seja $g = \sigma(f)$.Ora, como qualquer fatoração de g pode ser levado via a inversa de σ em uma fatoração de f então teremos que g é irredutível e separável sobre o corpo $\sigma(F)$. Tomando β como qualquer raiz de g, então pelo Teorema 3.1.8 (Uma vez que F e $\sigma(F)$ são isomorfos) existe um único isomorfismo que entre $F(\alpha)$ e $\sigma(F)(\beta)$ que leva α em β e que coincide com σ em F. Explicitamente tal isomorfismo pode ser dado por

$$b_0 + b_1\alpha + \cdots + b_r\alpha^r \to \sigma(b_0) + \sigma(b_1)\beta + \cdots + \sigma(b_r)\beta^r$$

onde $r = grau(f)$. Agora se $grau(g) = r$ então $[F(\alpha) : F] = grau(f) = grau(g) = r$, e portanto pelo Teorema 3.1.5 $[E : F(\alpha)] = \dfrac{k}{r} < n$. Como g é separável então g têm r raízes distintas em C. Consequentemente existem r possibilidades para escolha de β. Em cada caso, pela hipótese de indução, teremos que cada mergulho de $F(\alpha)$ em C se estende para exatamente $\dfrac{k}{r}$ mergulhos de E em C. Isto produz k mergulhos distintos de E em C. Mas se τ é qualquer mergulho de E em C que estende σ, então τ deve levar α em alguma raiz de g, isto é, a um dos β_s. Consequentemente se houvesse mais do que k possiíveis dos τ_s, então haveria mais do que $\dfrac{k}{r}$ extensões possíveis de pelo menos um dos mergulhos de $F(\alpha)$ em C. Isto, porém, contradiria a hipótese de indução. Portanto temos exatamente k mergulhos de E em C. □

Definição 3.1.13. *Seja $E|F$ uma extensão algébrica. Dizemos que $E|F$ é normal, ou que E é normal sobre F, se todo polinômio sobre F que têm pelo menos uma raiz em E se decompõe sobre E .*

O próximo resultado nos dá condições equivalentes para que $E|F$ seja normal.

Teorema 3.1.21. *A extensão finita $E|F$ é normal se, e somente se, cada $F-$monomorfismo de E em um fecho algébrico C de E é, em verdade, um $F-$automorfismo de E.*

Demonstração. Suponha $E|F$ normal e seja τ um $F-$ monomorfismo de E em C. Pelo Lema 3.1.7, teremos que τ leva cada $x \in E$ em um de seus conjugados . Consequentemente $\tau(E) \subseteq E$. Já que $[E:F] < \infty$ e $\tau(E)$ um subespaço de vetorial com mesma dimensão de E, visto que $\tau(E)$ e E serem isomorfos então segue-se que $\tau(E) = E$. Inversamente seja $\alpha \in E$, e seja β qualquer conjugado de α sobre F. Como na prova do Teorema 3.1.20 existe um $F-$ monorfismo de E em C que leva α em β. Como todo $F-$ monomorfismo é na verdade um $F-$ automorfismo de E então teremos que $\beta \in E$, concluindo assim que E é normal sobre F. □

Observação 3.1.22. *Os resultados dos teoremas 3.1.20 e 3.1.21 continuam válidos se C for substituído por uma extensão normal de F contendo E.*

Teorema 3.1.23. *Uma extensão finita $E|F$ é normal se, e somente se, E é um corpo de decomposição de algum polinômio $f \in F[x]$.*

Demonstração. Suponha primeiramente que E é normal sobre F.Dado que $[E:F]$ é finito, seja $\alpha_1, \cdots, \alpha_n$ uma base de E sobre F e seja f_i o polinômio minimal de α_i sobre F, com $i = 1, \cdots, n$.Como cada f_i têm a raiz α_i em E então segue-se da hipótese que f_i se decompõe sobre E. Consequentemente $f = f_1 \cdots f_n$ também se decompõe sobre E. Se f se decompõe sobre um corpo K com $F \subseteq K \subseteq E$, então cada $\alpha_i \in K$, e portanto K deve coincidir com E. Logo E é um corpo de decomposição para f sobre F. Inversamente seja E um corpo de decomposição para algum polinômio f sobre F, onde as raízes de f são $\alpha_1, \cdots, \alpha_n$. Seja assim τ um $F-$ monomorfismo de E em um fecho algébrico de E. Como $E = F(\alpha_1, \cdots, \alpha_n)$ então cada elemento de E é uma combinação linear finita sobre F de produtos finitos dos elementos $\alpha_1, \cdots, \alpha_n$. Logo $\tau(E) \subseteq E$, pois um monomorfismo leva uma raiz de f em outra raiz de f. Usando o mesmo argumento dado no Teorema 3.1.21 segue-se que $\tau(E) = E$ e pelo mesmo teorema $E|F$ é normal. □

Corolário 3.1.4. *Seja $F \leq K \leq E$, onde E é uma extensão finita de F. Se $E|F$ for normal, então $E|K$ também é normal.*

Definição 3.1.14. *Uma extensão $E|F$ é galoisiana se for normal e separável.*

Teorema 3.1.24. *Se E é um corpo de decomposição de um polinômio separável f sobre F, então $E|F$ é galoisiana.*

Demonstração. Pelo Teorema 3.1.23, $E|F$ é normal; pelo Teorema 3.1.7, $E|F$ é finita. Como E é um corpo de decomposição para f, temos que $E = F(\alpha_1, \ldots, \alpha_n)$, onde $\alpha_1, \ldots, \alpha_n$ são as raízes de f em E. Uma vez que $\min(\alpha_1, F)$ divide o polinômio separável f, temos que cada α_i é separável sobre F. Portanto, pelo lema 3.1.6, E é separável sobre F. □

Definição 3.1.15. *Seja E uma extensão finita de F. Chamamos de fecho normal de E sobre F, à menor extensão normal de F que contém E.*

Teorema 3.1.25 (Lema de Dedekind)**.** *Sejam $\sigma_1, \ldots, \sigma_n$ automomorfismos (ou simplesmente monomorfismos) distintos do corpo K. Então, $\sigma_1, \ldots, \sigma_n$ são L.I. sobre K.*

Demonstração. Por absurdo, suponha que $\sigma_1, \cdots, \sigma_n$ sejam linearmente dependentes. Reenumerando se preciso for, seja

$$a_1\sigma_1 + \cdots + a_r\sigma_r = 0 \tag{3.1}$$

onde os a_i são diferentes de zero e r é o menor possível. Veja que, necessariamente, temos $r \geq 2$ pois, caso contrário, $a_1\sigma_1 = 0$, o que é impossível. Como $\sigma_1, \ldots, \sigma_n$ são todos distintos, existe $t \neq 0$ de modo que $\sigma_1(t) \neq \sigma_2(t)$. Usando a multiplicatividade de $\sigma_1, \ldots, \sigma_n$, temos, para todos $g, h \in K^*$,

$$\sum_{i=1}^{r} a_i\sigma_i(h)\sigma_i(g) = 0. \tag{3.2}$$

Agora, multiplicando (3.1) por $\sigma_1(t)$ e subtraindo (3.2) do resultado, temos, para todos g e h como acima,

$$\sum_{i=1}^{r} a_i(\sigma_1(t) - \sigma_i(h))\sigma_i(g) = 0. \tag{3.3}$$

Mas, observe que

$$\sigma_1(t) - \sigma_i(h) = \begin{cases} 0, \text{ se } h = t \\ \neq 0, \text{ se } h \neq t \end{cases}.$$

Assim, tomando $h = t$ em (3.3), segue que

$$\sum_{i=2}^{r} a_i(\sigma_1(t) - \sigma_i(t))\sigma_i(g) = 0,$$

o que é uma contradição em vista da minimalidade de r. □

3.2 Módulos

Nesta seção, basearemos nossas afirmações em (GARCIA; LEQUAIN, 2006) e (ASH, 2013). Em tudo o que segue, R é um anel comutativo com unidade.

Definição 3.2.1. *Um grupo abeliano $(M,+)$, dotado de uma multiplicação por escalar*

$$\begin{aligned} R\times M &\longrightarrow M \\ (a,m) &\longmapsto a\cdot m \end{aligned}$$

é dito um $R-$módulo se satisfizer os seguintes axiomas, para todos $a_1,a_2\in R$, $m_1,m_2\in M$:

(a) $1\cdot m_1 = m_1$;

(b) $(a_1\cdot a_2)\cdot m_1 = a_1\cdot(a_2\cdot m_1)$;

(c) $(a_1+a_2)\cdot m_1 = a_1\cdot m_1 + a_2\cdot m_1$;

(d) $a_1\cdot(m_1+m_2) = a_1\cdot m_1 + a_1\cdot m_2$.

Se $a\in R$ e $m\in M$, sempre que não houver perigo de confusão escreveremos am para denotar o elemento $a\cdot m$ do R-módulo M.

Definição 3.2.2. *Seja R um anel e M um $R-$módulo. Um subgrupo N de M é um $R-$submódulo de M se a multiplicação por escalar do módulo M preserva N, isto é, se*

$$a\cdot n\in N,\ \ \forall a\in R, n\in N.$$

Definição 3.2.3. *Sejam M um $R-$módulo, $t\in\mathbb{N}$ e $m_1,m_2,\ldots,m_t\in M$. O subconjunto N de M dado por*

$$N=\{a_1m_1+a_2m_2+\ldots+a_tm_t;\, a_i\in R \text{ para } 1\leq i\leq t\}$$

é um $R-$submódulo de M, chamado o submódulo gerado por $m_1,m_2,\ldots,m_t$. Denotamos $N=Rm_1+Rm_2+\ldots+Rm_t$.

Ainda em relação à definição anterior, dizemos que um $R-$módulo M é finitamente gerado quando existem $t\in\mathbb{N}$ e $m_1,m_2,\ldots,m_t\in M$ tais que

$$M=Rm_1+Rm_2+\ldots+Rm_t.$$

Neste caso, dizemos também que $\{m_1,m_2,\ldots,m_t\}$ é um conjunto de geradores para M sobre R. Em particular, um $R-$módulo M é cíclico se é gerado por um único elemento, isto é, $M=R\cdot a$, para algum $a\in M$.

Definição 3.2.4. *Se M e N são $R-$módulos, um homomorfismo de módulos (também chamado de um $R-$homomorfismo) de M para N é uma aplicação $f : M \to N$ tal que*

$$f(rx+sy) = rf(x)+sf(y),\ \forall x,y \in M,\ r,s \in R.$$

Se $f : M \to N$ é um R-homomorfismo, definimos o núcleo e a imagem de f, respectivamente, por

$$\ker(f) = \{x \in M;\ f(x) = 0\} \ \text{ e } \ \mathrm{Im}(f) = \{f(x);\ x \in\ M\}.$$

Não é difícil verificar que $\ker(f)$ é um submódulo de M e $\mathrm{Im}(f)$ é um submódulo de N.

Teorema 3.2.1. *Se $f : M \to M'$ é um homomorfismo de R-módulos com núcleo N, então f induz um isomorfismo*

$$\overline{f} : M/N \to Im(f).$$

A seguir, definimos duas construções úteis de R-módulos.

Definição 3.2.5. *Seja dados um conjunto $I \neq \emptyset$ e, para cada $i \in I$, um $R-$módulo M_i. O produto cartesiano*

$$\prod_{i\in I} M_i := \{(a_i)_{i\in I};\ a_i \in M_i\}$$

é chamado de produto direto (externa) dos M_i quando munido com a estrutura de R-módulo com operações dadas por

$$(a_i)+(b_i) = (a_i+b_i) \ \ e \ \ r(a_i) = (ra_i).$$

Nas notações da definição anterior, o subconjunto de $\bigoplus_{i\ \in\ I} M_i$ de $\prod_{i\in I} M_i$ dado por

$$\bigoplus_{i\ \in\ I} M_i = \left\{(a_i)_{i\ \in\ I} \in \prod_{i\in I} M_i;\ a_i = 0 \text{ para quase todo } j \in I\right\}$$

é um R-submódulo de $\prod_{i\in I} M_i$, denominado a soma direta (externa) dos M_i. Aqui, $a_i = 0$ *para quase todo* $i \in I$ significa que, dado $(a_i)_{i\ \in\ I} \in \bigoplus_{i\ \in\ I} M_i$, existe um subconjunto finito J de I (que depende de $(a_i)_{i\ \in\ I}$) tal que $a_i = 0$ para todo $i \notin J$.

Observe que as definições de produto direto e soma direta coincidem quando o conjunto de índices for finito.

Definição 3.2.6. *Dada uma família $\{M_i; i \in I\}$ de submódulos de um $R-$módulo M, dizemos que M é a soma direta interna dos M_i se cada $x \in M$ puder ser expresso unicamente como $x = x_{i_1} + \ldots + x_{i_n}$, para certos índices dois a dois distintos $i_1, \ldots, i_n \in I$ e certos $x_{i_k} \in M_{i_k}$ para $k = 1, \ldots, n$.*

O resultado a seguir dá condições necessárias e suficientes úteis para que um R-módulo seja uma soma direta interna de uma família de submódulos.

Proposição 3.2.2. *Um $R-$módulo M é a soma direta interna da família de $R-$submódulos $\{M_i; i \in I\}$ se, e somente se, as seguintes condições forem satisfeitas:*

(a) $M = \sum_{i \in I} M_i$, isto é, cada $x \in M$ é uma soma finita da forma $x = x_{i_1} + \ldots + x_{i_n}$, para certos índices $i_1, \ldots, i_n \in I$ e elementos $x_{i_k} \in Mi_k$, para $1 \leq k \leq n$.

(b) $M_i \cap \sum_{j \neq i} M_j = \{0\}$ para cada $i \in I$.

Ademais, sendo esse o caso, temos

$$M \simeq \bigoplus_{i \in I} M_i.$$

Precisamos de mais algumas definições.

Definição 3.2.7. *Um subconjunto S do $R-$módulo M é linearmente independente (abreviamos LI) sobre R se uma igualdade da forma $a_1x_1 + \ldots + a_nx_n = 0$, com $a_1, \ldots, a_n \in R$ e $x_1, \ldots, x_n \in S$ necessariamente implicar $a_i = 0$ para $i = 1, 2, \ldots, n$. Uma base para um R-módulo M é um subconjunto S de M que é simultaneamente LI e um conjunto de geradores para M.*

Definição 3.2.8. *Um $R-$módulo livre é um R-módulo isomorfo a uma soma direta (externa) de cópias isomórficas de R.*

É imediato que todo R-módulo livre possui uma base. Reciprocamente, se S é uma base para o R-módulo M, não é difícil verificar que M é um R-módulo livre, isomorfo à soma direta de uma família, indexada por S, de $R-$módulos isomorfos a R.

O resultado a seguir garante que para R-módulos livres, não precisamos nos preocupar em qual base escolher.

Teorema 3.2.3. *Duas bases quaisquer de um R-módulo livre M têm a mesma cardinalidade.*

Se $n \in \mathbb{N}$ e um R-módulo M possuir uma base com n elementos, diremos que M é um $R-$módulo livre de posto n. Nesse caso, o seguinte teorema é válido. Uma vez que sua prova é bastante longa, a omitiremos aqui, referindo o leitor interessado a (GARCIA; LEQUAIN, 2006).

Teorema 3.2.4. *Sejam R um domínio de ideais principais e M um $R-$módulo livre de posto $n \in \mathbb{N}$. Se $K \neq \{0\}$ é um submódulo de M, então K é livre de posto $r \leq n$. Mais precisamente, existem uma base $\{y_1, \ldots, y_n\}$ para M, um natural $r \leq n$ e elementos $a_1, \ldots, a_r \in R \setminus \{0\}$ tais que a_i divide a_{i+1} para $1 \leq i < r$ e $\{a_1 y_1, \ldots, a_r y_r\}$ é uma base para K.*

4 EXCERTOS DE TEORIA ALGÉBRICA DOS NÚMEROS

4.1 Extensões Inteiras

A partir de agora, todos os anéis serão assumidos comutativos e com unidade.

Definição 4.1.1. *Seja A um subanel do anel R, e seja $x \in R$. Dizemos que x é inteiro sobre A se x é a raíz de um polinômio mônico f com coeficientes em A. Neste caso, $f(x) = 0$ é chamada uma equação de dependência inteira.*

Definição 4.1.2. ***(Inteiro Algébrico):*** *Se x é um número real ou complexo que é inteiro sobre $\mathbb{Z}$ então x é denominado inteiro algébrico.*

Note que se considerarmso $A[x]$ como sendo o conjunto dos polinômios em x com coeficientes em A, onde $x \in R$ e A um subanel de R, então teremos que $A[x]$ é um $A-$módulo. De fato, basta notar que se somarmos dois polinômios em $A[x]$ e multiplicarmos um polinômio também em $A[x]$ por um elemento de A, então obteremos elementos em $A[x]$.

A próxima proposição nos dá condições equivalentes para que um elemento x seja inteiro sobre um subanel A de uma anel R.A relação entre x ser inteiro sobre A e o anel $A[x]$ ser um $A-$módulo finitamente gerado será usado para mostrar que os elementos inteiros de um anel R sobre um subanel A formam um subanel de R.

Proposição 4.1.1. *Seja A um subanel de R, com $x \in R$. Então as seguintes condições são equivalentes:*

(i) x é um inteiro sobre A;

(ii) O $A-$módulo $A[x]$ é finitamente gerado;

(iii) x pertence a um subanel B de R tal que $A \subseteq B$ e B é um finitamente gerado $A-$módulo.

Demonstração. $(i) \Rightarrow (ii)$ Como x é inteiro sobre A, então existe um polinômio mônico $p(y) = y^n + a_{n-1}y^{n-1} + \ldots + a_0$,tal que $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$. Mostremos que qualquer x^m será uma combinação linear dos elementos $1, x, x^2, \ldots, x^{n-1}$ com coeficientes em A. Faremos isto por indução sobre m. Para $m = 0$, o resultado é obvio. Suponhamos que seja verdadeiro para k, e mostremos para $k+1$. Bom, como o resultado é verdadeiro para k, então:

$$x^k = b_0 + b_1x + \ldots + b_{n-1}x^{n-1} \tag{4.1}$$

Logo, multiplicando a equação (4.1) por x, obteremos:

$$x^{k+1} = b_0x + b_1x^2 + \ldots + b_{n-1}x^n \tag{4.2}$$

Como $x^n \in A[x]$ e $x^n = -a_{n-1}x^{n-1} - \ldots - a_0$ por hipótese. Então substituindo o valor de x^n em (4.2), teremos

$$x^{k+1} = b_0x + b_1x^2 + \ldots + b_{n-1}(-a_0 - a_1x - \ldots - a_{n-1}x^{n-1})$$

e logo,

$$x^{k+1} = -b_{n-1}a_0 + (-b_{n-1}a_1 + b_0)x + \ldots + (-b_{n-1}a_{n-1})x^{n-1}.$$

Isto é, uma combinação dos elementos $1, x, \ldots, x^{n-1}$. Concluímos assim que $A[x]$ é um $A-$módulo finitamente gerado.

$(ii) \Rightarrow (iii)$

Basta tomar $B = A[x]$.

$(iii) \Rightarrow (i)$

Devemos mostrar que x é inteiro sobre A. Como B é um finitamente gerado $A-$módulo, seja $\beta_1, \ldots, \beta_n$ os geradores de B sobre A. Então, $x \cdot \beta_i$ com $i = 1, \ldots, n$, será uma combinação linear dos β_j, isto é

$$x \cdot \beta_i = \sum_{j=1}^{n} c_{ij} \cdot \beta_j.$$

Assim, se B_c for o vetor coluna cujas coordenadas são os elementos β_i, I for a matriz identidade de ordem n e $C = [c_{ij}]$, então podemos escrever

$$(x \cdot I - C) \cdot B_c = 0. \tag{4.3}$$

Multiplicando (4.3) pela matriz adjunta da matriz $x \cdot I - C$, obteremos:

$$det(x \cdot I - C) \cdot I \cdot B_c = 0. \tag{4.4}$$

Desta forma, seja $b \in B$ então $b = a_1\beta_1 + \ldots + a_n\beta_n$. Então, $det(x \cdot I - C) \cdot b = det(x \cdot I - C) \cdot (a_1\beta_1 + \ldots + a_n\beta_n) = det(x \cdot I - C) \cdot (a_1\beta_1) + \ldots + det(x \cdot I - C) \cdot (a_n\beta_n) = a_1 \cdot (det(x \cdot I - C))\,\beta_1 + \ldots + a_n \cdot (det(x \cdot I - C) \cdot B_n) = a_1 \cdot 0 + \ldots + a_n \cdot 0 = 0$.

Assim, fazendo $b = 1$, concluímos que x é raíz do polinômio mônico $det(xI - C)$ em $A[x]$.

□

Usaremos o Lema a seguir para mostrarmos a transitividade da propriedade de um elemento ser inteiro sobre um anel.

Lema 4.1.1. *Seja A um subanel de R , com $x_1, \ldots, x_n \in R$. Se x_1 é inteiro sobre A, x_2 inteiro sobre $A[x_1], \ldots, x_n$ inteiro sobre $A[x_1, \ldots, x_{n-1}]$, então $A[x_1, \ldots, x_n]$ é um $A-$módulo finitamente gerado.*

Demonstração. A prova será feia por indução sobre n. O caso $n = 1$ segue-se inteiramente da proposição 4.1.1. Suponhamos agora que seja válido para k e mostremos que é válido para $k+1$. Como x_{k+1} é inteiro sobre $A[x_1, \ldots, x_k]$, então $A[x_1, \ldots, x_k][x_{k+1}]$ = A[$x_1, \ldots, x_k, x_{k+1}$] é um $A[x_1, x_2, \ldots, x_k]-$ módulo finitamente gerado. Seja assim

$$C = \sum_{j=1}^{r} b_j \cdot y_j \in A[x_1, \ldots, x_k, x_{k+1}], b_j \in A[x_1, \ldots, x_k]$$

para cada $j = 1, \ldots, r$, onde $\{y_1, \ldots, y_r\}$ é um conjunto de geradores de $A[x_1, \ldots, x_k, x_{k+1}]$ sobre $A[x_1, \ldots, x_k]$. Como por hipótese de indução $A[x_1, \ldots, x_k]$ é um $A-$módulo finitamente gerado, então cada b_j pode ser escrito como

$$b_j = \sum_{k=1}^{s} d_{k_j} \cdot e_k$$

onde cada $d_k \in A$ e $\{e_1, \ldots, e_s\}$ um conjunto de geradores de $A[x_1, \ldots, x_k]$ sobre A. Consequentemente,

$$C = \sum_{j=1}^{r} b_j \cdot y_j = \sum_{j=1}^{r} \sum_{k=1}^{s} d_{k_j} \cdot e_j \cdot y_j.$$

Logo, $A[x_1, \ldots, x_k, x_{k+1}]$ é um $A-$módulo finitamente gerado. Assim, $A[x_1, \ldots, x_n]$ é um $A-$módulo finitamente gerado para cada n.

□

Agora, mostraremos a propriedade de Transitividade de Extensões Inteiras.

Definição 4.1.3. *Sejam A, B subanéis de um anel R. Diremos que B é inteiro sobre A, se cada elemento de B é inteiro sobre A.*

Proposição 4.1.2. *Sejam A, B e C subanéis de R. Se C é inteiro sobre B e B é inteiro sobre A, então C é inteiro sobre A.*

Demonstração. Seja $x \in C$. Como C é inteiro sobre B, então existe um polinômio mônico p de grau n, com coeficientes em B, tal que $p(x) = 0$. Isto é, temos que

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

Como $b_0, \ldots, b_{n-1} \in B$. Como consequência imediata então x também é inteiro sobre $A[b_0, \ldots, b_{n-1}]$. Já que cada b_i é inteiro sobre A, então também o é sobre $A[b_0, \ldots, b_{i-1}]$. Logo, $A[b_0, \ldots, b_{n-1}, x]$ é um $A-$módulo finitamente gerado pelo Lema anterior, e assim pela proposição 4.1.1, parte $(III \Rightarrow I)$, x é inteiro sobre A. Logo, C é inteiro sobre A.

□

Enunciamos e demonstramos a seguir dois importantes lemas os quais serão essenciais para demonstração de nosso Teorema Principal.

Lema 4.1.2. *Seja A um subanel do domínio integral B, com B inteiro sobre A. Então A é um corpo se, e somente se, B é um corpo.*

Demonstração. Assumimos primeiramente que B é um corpo e tomamos $a \in A$. Para mostrarmos que A e um corpo, basta mostrarmos que $a^{-1} \in A$. Ora, como B é inteiro sobre A, então existe uma equação da forma

$$(a^{-1})^n + c_{n-1}(a^{-1})^{n-1} + \ldots + c_1 a^{-1} + c_0 = 0 \tag{4.5}$$

com $c_i \in A$, para cada $i = 1, \ldots, n-1$.

Multiplicando (4.5) por a^{n-1} , então teremos:

$$(a^{-1}) + c_{n-1} + \ldots + c_1 a^{n-2} + c_0 \cdot a^{n-1} = 0.$$

Logo,

$$(a^{-1}) = -(c_{n-1} + \ldots + c_1 a^{n-2} + c_0 \cdot a^{n-1}) \in A.$$

Concluímos assim que A é um corpo. Agora suponha que A é um é um corpo e seja $b \in B$. Pelo Teorema 3.1.3, $A[b]$ é um espaço vetorial de dimensão finita sobre A. Seja f uma transformação $A-$linear neste espaço vetorial dado pela multiplicação por $''b''$, em outras palavras $f(z) = b \cdot z$ com $z \in A[b]$. Mostremos que f é injetiva. Pelo Teorema 2.5.2, parte 2, basta mostrarmos que $N(f) = \{0\}$. Seja então $z \in A[b]$ tal que $f(z) = b \cdot z = 0$. Ora, como $b \neq 0$ e $A[b]$ sendo um corpo , em particular um domínio, então necessariamente $z = 0$. Assim, pelo Teorema do Núcleo e da Imagem, teremos que fé sobrejetiva. Logo, para cada $b \in B$, existe $z \in B$, tal que $b \cdot z = 1$. Consequentemente B é um corpo. □

Proposição 4.1.3. *Seja A um subanel de um anel B, B inteiro sobre A , Q um ideal primo de B e* $P = Q \cap A$, *então:*

i) P é um ideal primo e A/P *pode ser considerado como um subanel de* B/Q;

ii) B/Q *é um inteiro sobre* A/P;

iii) P é um ideal maximal de A se, e somente se, Q é um ideal maximal de B.

Demonstração. i) Seja i a função identidade de A em B. Já que i é um homomorfismo e Q é um ideal primo de B, então pela Proposição 2.5.3, $i^{-1}(Q)$ é um ideal primo de A. Mas, $i^{-1}(Q) = \{x \in A;\ i(x) \in Q\} = Q \cap A$. Logo $Q \cap A$ é um ideal primo. Para mostrar que A/P pode ser considerado como um subanel de B/Q seja j a função que leva $x+P$ em $x+Q$, para cada $x \in A$. Mostremos que j está bem definida e é injetiva. De fato, seja $x_1 + P = x_2 + P$, então $x_1 = x_2 + a$, com $a \in P$. Logo, $x_1 + Q = (x_2 + a) + Q = x_2 + Q$, já que $a \in Q$. Logo, $f(x_1 + P) = f(x_2 + P)$. Portanto, J está bem definida. Agora vejamos a questão da injetividade. Suponha que tenhamos $f(x_1 + P) = f(x_2 + P)$, isto é, $x_1 + Q = x_2 + Q$. Então $x_1 + a = x_2 + b$, como $a, b \in Q$. Então $x_1 - x_2 = b - a$. Ora, com $x_1 - x_2 \in A$ e $b - a \in Q$ então $x_1 - x_2 \in P = Q \cap A$. Logo, $x_1 + P = x_2 + P$. Como consequencia A/P pode ser visto como sua imagem isomorfa $j(A/P)$.

ii) Seja $b + Q \in B/Q$. Então, já que B é inteiro sobre A então b satisfaz uma equação da forma

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0, a_i \in A, i = 0, \ldots, n-1.$$

Mostremos que se a_i for substituído por $a_i + P$, então $b + Q$ satisfaz a equação acima.

De fato

$$(b+Q)^n + (a_{n-1}+P)\cdot(b+Q)^{n-1} + \ldots + (a_1+P)\cdot(b+Q) + (a_0+P)\cdot(1+Q) =$$

$$(b^n+Q) + (a_{n-1}+P)\cdot(b^{n-1}+Q) + \ldots + (a_1+P)\cdot(b+Q) + (a_0+P)\cdot(1+Q) =$$

$$(b^n + a_{n-1}\cdot b^{n-1} + \ldots + a_1 P + a_0) + Q = Q.$$

Logo, B/Q é inteiro sobre A/P. □

Observação: Veja que a penúltima igualdade só é possível devido a identificação dada em *i*.

iii) Já que A/P pode ser considerado como um subanel de B/Q por *i*, B/Q é inteiro sobre A/P por *ii*), então pelo Lema 4.1.2, A/P será um corpo se, e somente se, B/Q é um corpo. Pelo Teorema 2.4.1 segue-se o resultado.

Definição 4.1.4. *Seja A um subanel de R. Chamamos de fecho inteiro de A em R ao conjunto A_c dos elementos de R que são inteiros sobre A.*

Definição 4.1.5. *Seja A um subanel de R. Dizemos que A é integralmente fechado em R se $A_c = A$.*

Sempre que dissermos que A é integralmente fechado sem referência a R, assumimos que A é um domínio integral com corpo quociente K, e A é integralmente fechado em K.

Proposição 4.1.4. *O fecho inteiro de A em R é um subanel de R contendo A.*

Demonstração. Note que sempre temos $A \subseteq A_c$, pois cada $a \in A$ é raiz de $x - a$. Seja agora $x, y \in A_c$, então pelo Lema 4.1.1, $A[x,y]$ é um $A-$módulo finitamente gerado. Já que $x+y, x-y$ e $x\cdot y$ pertencem a este módulo, segue-se pela Proposição 4.1.1 que estes são inteiros sobre A. Logo, pertencem a A_c. □

Proposição 4.1.5. *O fecho inteiro A_c de A em R é integralmente fechado em R. Em outras palavras $(A_c)_c = A_c$.*

Demonstração. Temos sempre que $A_c \subseteq (A_c)_c$. Seja assim $b \in (A_c)_c$. Então, b é inteiro sobre A_c e existe um polinômio da forma

$$b^n + a_{n-1}\cdot b^{n-1} + \ldots + a_1 \cdot b + a_0 = 0$$

com $a_{n-1},\ldots,a_0 \in A_c$. Em particular, temos que b é inteiro sobre $A[a_{n-1},\ldots,a_0]$. Assim, usando o mesmo argumento da Proposição 4.1.2 , teremos que $A[a_{n-1},\ldots,a_0,\ b]$ é um $A-$módulo finitamente gerado e, portanto, b é inteiro sobre A. Logo, $b \in A_c$. □

Através da próxima proposição poderemos identificar uma larga classe de anéis integralmente fechados.

Proposição 4.1.6. *Seja A um domínio de Fatoração Única, então A é integralmente fechado.*

Demonstração. Precisamos mostrar que $A = A_c$. Já temos que $A \subseteq A_c$, então basta mostrar que $A_c \subseteq A$. Seja $x \in A_c$ e suponhamos que x pertença ao corpo de frações de A. Então, podemos escrever $x = \frac{a}{b}$, onde $MDC\{a,b\} = 1$. (Observe que pela Proposição 2.6.1, em qualquer Domínio de Fatoração Única existe a noção de MDC). Como $x \in A_c$ existe um polinômio da forma:

$$\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + a_1\left(\frac{a}{b}\right) + a_0 = 0 \tag{4.6}$$

com $a_i \in A$, para todo $i = 0,1,\ldots,n-1$. Multiplicando (4.6) por b^n, teremos:

$$b^n\left(\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + a_1\left(\frac{a}{b}\right) + a_0\right) = b^n 0$$

isto é,

$$a^n + a_{n-1}ba^{n-1} + \ldots + b^n a_0 = 0. \tag{4.7}$$

Ora, pondo b em evidência, podemos escrever (4.7) como

$$a^n + b\cdot\left(a_{n-1}\cdot a^{n-1} + \ldots + b^{n-1}\cdot a_0\right) = 0. \tag{4.8}$$

Logo, fazendo $c = a_{n-1}\cdot a^{n-1} + \ldots + b^{n-1}\cdot a_0$ então 4.8 torna-se

$$a^n + b\cdot c = 0,$$

ou seja, $a^n = -b\cdot c$. Como $MDC\{a,b\} = 1$, então $MDC\{a^n,b\} = 1$ Desta forma, como $b|a^n$ então b é necessariamente invertível e, portanto, $x \in A$. Logo, $A_c \subseteq A$ e temos $A = A_c$. □

Chamaremos de Corpo Numérico a qualquer subcorpo L dos numéros complexos ($\mathbb{C}$) de modo que L seja uma extensão finita de de $\mathbb{Q}$. Teremos assim que os elementos de L serão números algébricos. Chamaremos o fecho inteiro de $\mathbb{Z}$ em L de Anel de inteiros Algébricos de L e denotaremos por I_L.

4.2 Normas e Traços.

Seja E/F uma extensão de corpos de grau n, e seja x qualquer elemento de E. Consideremos a transformação linear $m(x)$ dada pela multiplicação por x, isto é, $m(x)\cdot y = x\cdot y$ para cada $y \in E$. Definimos a norma e o traço de x, relativamente a extensão E/F, como :

$$N[E/F](x) = det\ m(x),\ T[E/F](x) = \text{traço}\ m(x).$$

Escreveremos simplesmente $N(x)$ e $T(x)$ se E/F for conhecida. Se a matriz $A(x) = [a_{ij}(x)]$ represente $m(x)$ com respeito a alguma base de E sobre F. Então, a norma de x é o determinante de $A(x)$ e o traço de x é o traço de $A(x)$, isto é, a soma dos elementos da diagonal principal. Definimos também a característica polinomial de x como sendo a característica polinomial da matriz $A(x)$, isto é

$$char[E/F](x) = det[x\cdot I - A(x)].$$

Como acima, se E/F for conhecida, então escreveremos simplesmente $char(x)$ para denotar a característica polinomial de x.

Como exemplo seja então $E = \mathbb{C}$ e $F = \mathbb{R}$. Uma base para $\mathbb{C}$ sobre $\mathbb{R}$ é $\{1, i\}$, e , com $x = a + bi$, temos:

$$(a+bi)(1) = a\cdot(1) + b\cdot(i)\ \text{e}(a+bi)(i) = -b\cdot(1) + a\cdot(i).$$

Então,

$$A(a+bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

Então a norma, traço e característica polinomial de $a+bi$, são:

$$N(a+bi) = a^2 + b^2,$$

$$T(a+bi) = 2a,$$

$$char\ (a+bi) = x^2 - 2ax + a^2 + b^2.$$

Note que no exemplo acima, a norma e o traço de x são, respectivamente, o termo constante de *char x* e o inverso aditivo do coeficiente de x em *char x*. No caso geral isto também acontece, ou seja, podemos escrever $char(x)$ como :

$$char(x) = x^n - T(x) \cdot x^{n-1} + \ldots + (-1)^n \cdot N(x).$$

Para ver isto, basta usar a Definição de Determinante. Pois, sendo:

$$char(x) = det(x \cdot I - A(x)) = \sum \sigma(p) \cdot a_{1j_1} \cdot a_{1j_1} \cdot \ldots \cdot a_{nj_n},$$

então teremos que $char(x)$ será um polinômio de grau n, e o único produto elementar que produzirá o coeficiente de x^{n-1} será

$$(x - a_{11}) \cdot (x - a_{22}) \cdot \ldots \cdot (x - a_{nn}).$$

Neste caso, o coeficiente de x^{n-1} será exatamente $-(a_{11} + a_{22} + \ldots + a_{nn})$ ou seja, $-T(x)$. E fazendo $x = 0$ teremos que o termo constante de $char(x)$ será $(-1)^n \cdot detA(x)$.

Lema 4.2.1. *Se E é uma extensão de F e $x \in E$ então $N(x)$, $T(x)$ e os coeficientes de $char(x)$ pertencem a F. Se $a \in F$, então $N(a) = a^n$; $T(a) = n \cdot a$ e $char(a) = (x-a)^n$.*

Demonstração. A primeira parte segue-se somente observando que os coeficientes da matriz $A(x)$ pertencem a F, pois sendo $N(x)$, $T(x)$ e os coeficientes de $char(x)$ somas e produtos de elementos de F,então pertencem a F. Para a segunda parte seja $\{b_1, \ldots, b_n\}$ uma base de E sobre F e seja $m(a)$ a transformação linear dada pela multiplicação por a. Então, sendo

$$m(a) \cdot b_1 = ab_1 = ab_1 + 0b_2 + \ldots + 0b_n.$$

Logo, a primeira coluna da matriz $A(a)$ será $(a, 0, \ldots, 0)$. Da mesma forma,

$$m(a) \cdot b_i = 0b_1 + 0b_2 + \ldots + 0b_i + \ldots + 0b_n,$$

para cada $i = 2, \ldots n$. Desta forma, a matriz $A(a)$ da transformação linear $m(a)$ será da forma

$$\begin{bmatrix} a & 0 & \dots & 0 \\ 0 & a & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & \dots & a \end{bmatrix}.$$

Assim ,

$$char(a) = det\left(\begin{bmatrix} a & 0 & \dots & 0 \\ 0 & a & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & \dots & a \end{bmatrix}\right) = (x-a)^n,\ N(a) = a^n \text{ e } T(a) = n \cdot a.$$

□

A próxima proposição nos dá uma conexão entre a característica polinomial de x e o polinômio minimal de x sobre F.

Proposição 4.2.1. *Seja E/F uma extensão finita. Então, $char[E/F](x) = [min(x,F)]^r$, onde $r = [E : F(x)]$.*

Demonstração. Primeiramente assumimos que $r = 1$, logo $E = F(x)$. Pelo Teorema de Cayley Hamilton, a Transformação Linear $m(x)$(que é na verdade um operador linear) satisfaz $char(x)$. Já que $m(x)$ é a multiplicação por x, então segue-se que x é uma raíz de $char(x)$. Logo, $min(x,F)$ divide $char(x)$, pela propriedade 1, dada logo após a Definição 3.1.4 . Ora, como ambos $min(x,F)$ e $char(x)$ são mônicos e possuem o mesmo grau, então segue-se que são iguais. Portanto

$$char[E|F](x) = min(x,F).$$

No caso geral, seja $y_1,\dots,y_s$ uma base para $F(x)$ sobre F e seja $z_1,\dots,z_r$ uma base de E sobre $F(x)$. Seja $A(x) = A$ a matriz representando a multiplicação por x na extensão $F(x)|F$. Então, suas colunas serão formadas pelos elementos a_{k_i} de modo que

$$x \cdot y_i = \sum_{k=1}^{s} a_{k_i} \cdot y_k.$$

Como os elementos $y_1 \cdot z_1, y_2 \cdot z_1, \ldots, y_s \cdot z_1;\ y_1 \cdot z_2, \ldots, y_s \cdot z_2, \ldots, y_1 \cdot z_r, y_2 \cdot z_r, \ldots, y_s \cdot z_r$ formam uma base de E sobre F, então a matriz $B = B(x)$ que representa a multiplicação por x nesta extensão terá a forma

$$B = \begin{bmatrix} A & & & 0 \\ & \ddots & & \\ & & A & \\ & & & \ddots \\ 0 & & & A \end{bmatrix}.$$

Já que $x \cdot (y_i \cdot z_j) = \sum_{k=1}^{s} a_{k_i} \cdot (y_k \cdot z_j))$.

Logo,

$$char[E|F](x) = \ det(x \cdot I - B) = [\ det(x \cdot I - A)]^r = [\ min(x,F)]^r.$$

Observe que a última igualdade é válida pelo caso $r = 1$ feito anteriormente.

□

Corolário 4.2.1. *Seja $[E : F] = n$ e $[F(x) : F] = d$. Sejam $x_1, \ldots, x_d$ as raízes de $min(x,F)$ em um corpo de decomposição (contando com a multiplicidade). Então:*

$$N(x) = \left(\prod_{i=1}^{d} x_i \right)^{\frac{n}{d}},\ T(x) = \frac{n}{d} \cdot \sum_{i=1}^{d} x_i$$

e

$$char(x) = \left(\prod_{i=1}^{d} (x - x_i) \right)^{\frac{n}{d}}.$$

Demonstração. Pelo Teorema 3.1.5 temos que $[E : F] = [E : F(x)] \cdot [F(x) : F]$. Consequentemente, $[E : F(x)] = \frac{n}{d}$. Logo, pelo Teorema anterior, teremos que $char(x) = [min(x,F)]^r = [min(x,F)]^{\frac{n}{d}}$.

Sendo K o corpo de decomposição de $min(x,F)$, então podemos escrever neste corpo

$$char(x) = \left(\prod_{i=1}^{d} (x - x_i) \right)^{\frac{n}{d}}.$$

Sendo $min(x,F) = x^d + a_{d-1} \cdot x^{d-1} + \ldots + a_1 x + a_0$ então o coeficiente de x^{n-1} em $(min(x,f))^{\frac{n}{d}}$ será

$$\frac{n}{d} \cdot a_{n-1} = -\frac{n}{d} \cdot \sum_{i=1}^{d} x_i$$

onde $a_{d-1} = -\sum_{i=1}^{d} x_i$.

Isto é facilmente notado já que o termo x^{n-1} só irá aparecer quando tivermos um produto da forma

$$x^d \cdot x^d \cdot \ldots \cdot x^d \cdot a_{d-1} \cdot x^{d-1} \tag{4.9}$$

Em que o termo x^d aparece $\frac{n}{d} - 1$ vezes e o termo $a_{d-1} \cdot x^{d-1}$ apenas uma vez. Como (4.9) aparece $\frac{n}{d}$ vezes em $(min(x,F))^{\frac{n}{d}}$, então segue-se o resultado. Fazendo $x = 0$ em $char(x)$, temos

$$char(x) = \left(\prod_{i=1}^{d}(0 - x_i)\right)^{\frac{n}{d}} = \left((-1)^d\right)^{\frac{n}{d}} \cdot \left(\prod_{i=1}^{d} x_i\right) = (-1)^n \cdot \left(\prod_{i=1}^{d} x_i\right).$$

Logo,

$$N(x) = (-1)^n \cdot (-1)^n \left(\prod_{i=1}^{d} x_i\right) = \prod_{i=1}^{d} x_i.$$

Se E é uma extensão separável de F, então existe uma expressão alternativa para o traço e a norma.

□

Proposição 4.2.2. *Seja E/F uma extensão separável de grau n, e seja $\sigma_1, \ldots, \sigma_n$, os distintos $F-$monomorfismos de E em um fecho algébrico de E, ou, igualmente, uma extensão normal de L em F contendo E. Então*

$$T[E|F](x) = \sum_{i=1}^{n} \sigma_1(x) \text{ e } N[E|F](x) = \prod_{i}^{n} \sigma_i(x).$$

Consequentemente, $T(ax+by) = a \cdot T(x) + b \cdot T(y)$ e $N(x \cdot y) = N(x) \cdot N(y)$, para todo $x,\ y \in E$, $a,\ b \in F$.

Demonstração. Seja $x \in E$ e suponhamos que $[F(x) : F] = d$. Pelo Teorema 2.8.4 teremos que $[E : F(x)] = \frac{n}{d}$. Agora, pelo Teorema 3.1.20 existem distintos $F-$mergulhos de $F(x)$ em L os quais chamaremos de $\tau_1, \ldots, \tau_d$ que levam x em um único conjugado x_i de x e que se estendem estendem para exatamente $\frac{n}{d}$ $F-$mergulos se E em L, que chamaremos de $\omega_{i_1}, \ldots, \omega_{i_{n/d}}$ e que tambéd levam x em x_i, onde $i = 1, \ldots, d$. Então

$$\sum_{j=1}^{n} \omega_j = \sum_{i=1}^{n} \sigma_i = \frac{n}{d} \cdot \tau_1(x) + \ldots + \frac{n}{d} \cdot \tau_d(x) = \frac{n}{d} \cdot \sum_{i=1}^{d} \tau_i(x) = T(x).$$

E analogamente,

$$\prod_{j=1}^{n} \omega_j = \prod_{i=1}^{n} \sigma_i(x) = \tau_1(x)^{\frac{n}{d}} \cdot \ldots \cdot \tau_d(x)^{\frac{n}{d}} = (\tau_1(x) \cdot \ldots \cdot \tau_d(x))^{\frac{n}{d}} = \left(\prod_{i=1}^{d} \tau_i(x) \right)^{\frac{n}{d}} = N(x).$$

A linearidade de T e a multiplicidade de N não precisa da suposição de separabilidade bastando observar que

$$m(ax + by) = a \cdot m(x) + b \cdot m(y) \text{ e } m(xy) = m(x) \circ m(y).$$

□

Corolário 4.2.2. ***(Transitividade do Traço e da Norma.)*** *Se $F \leq K \leq E$, onde $E|F$ é finita e separável, então $T[E|F] = T[K|F] \circ T[E|K]$ e $N[E|F] = N[K|F] \circ N[E|K]$.*

Demonstração. Como a extensão $E|F$ é finita e separável então as extensões $K|F$ e $E|K$ são finitas e separáveis pelo Teorema 3.1.5 e pela Proposição 3.1.14, respectivamente. Desta forma, sejam $\sigma_1, \ldots, \sigma_n$ os distintos $F-$mergulhos de K em L e $\tau_1, \ldots, \tau_m$ os distintos $K-$mergulhos de E em L, onde L é o fecho normal de E. Mostremos que $L|F$ é uma extensão Galoisiano. Como $[E : F]$ é finito, então existem $\alpha_1, \ldots, \alpha_n$ tal que $E = F(\alpha_1, \ldots, \alpha_n)$. Como L é o fecho normal de E sobre F, então L é o corpo de decomposição do polinômio $g = f_1 \cdot f_2 \cdot \ldots \cdot f_n$, onde f_i é o polinômio minimal de α_i sobre F. Então, pelo Teorema 3.1.24, $L|F$ é Galoisiana. Consequentemente, pelos Teoremas 3.1.20, 3.1.21 e pela observação logo após o teorema 2.8.19, cada σ_i e cada τ_j se estende para um automorfismo de L. Portanto, podemos considerar as composições

$$T[K \circ F] \circ T[E|K](x) \text{ e } N[K|F] \circ N[E|K].$$

Assim, mostremos que vale

$$T[E|F](x) = (T[K|F] \circ T[E|K])(x)$$

e

$$N[E|F] = N[K|F] \circ N[E|K](x)$$

para cada $x \in E$.

Temos que pela Proposição 4.2.2

$$T[K|F](T[E|K](x)) = \sum_{i=1}^{n} \sigma_i \left(\sum_{j=1}^{m} \tau_j(x) \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} \sigma_i \tau_j(x).$$

Observe que cada $\sigma_i \tau_j$ é um $F-$mergulho de E em L, e o número destas aplicações é $m \cdot n = [E : K] \cdot [K : F] = [E : F]$. Veja ainda que cada $\sigma_i \cdot \tau_j$ são todos distintos quanto restritos a E, pois se

$$\sigma_i \cdot \tau_j = \sigma_k \cdot \tau_l$$

em E, então vale, necessariamente, em K, já que $K < E$. Logo, $\sigma_i = \sigma_k$, pois τ_j e τ_l são identidades em K. Portanto, $i = k$, por injetividade. Como consequencia, $l = j$. □

Corolário 4.2.3. *Se $E|F$ é uma extensão separável finita, então $T[E|F](x)$ não pode ser 0 para todo $x \in E$.*

Demonstração. Suponhamos por absurdo que $T(x) = 0$ para todo $x \in E$. Por 4.2.2, então $\sum \sigma_i(x) = 0$ para todo $x \in E$. Mas isto contraria o Lema de Dedekind dado no Teorema 3.1.25. □

Seja A um domínio integral corpo quociente K e L uma extensão separável finita de K. Seja B o conjunto de elemetos de L que são inteiros sobre A, isto é, B é o fecho inteiro de A em L. O diagrama abaixo sumariza todas as informações

$$\begin{array}{ccc} B & \text{——} & L \\ | & & | \\ A & \text{——} & K \end{array}$$

Chamaremos o conjunto $\{A,K,L,B\}$ de configuração básica para a Teoria dos Números Algébricos e denotaremos por $AKLB$.No caso especial em que $A=\mathbb{Z}$ e $K=\mathbb{Q}$, L será um corpo numérico e $B=I_L$ o anel de Inteiros Algébricos

Proposição 4.2.3. *Seja AKBL uma configuração básica e seja $x \in B$. Então os coeficientes de $char[L|K](x)$ e $min(x,K)$ são inteiros sobre A. Em particular $T[L|K](x)$ e $N[L|K](x)$ são inteiros sobre A. Se A é integralmente fechado, então os coeficientes de $char(x)$ pertencem a A.*

Demonstração. Pelo Teorema 4.2.1 e pela observação logo após a definição 4.1.5 basta mostrarmos que cada raíz x_i do polinômio minimal $min(x,F)$ é inteiro sobre A. Já que todos os coeficientes de $char(x)$ são somas e produtos dos elementos x_i. Como cada x_i é um conjugado de x sobre K, então pelo Teorema 2.8.8 existe um $K-$isomorfismo $\tau_1 : K(x) \to K(x_1)$ tal que $\tau_i(x) = x_i$. Ora, como x é inteiro sobre A, então existe um polinômio em x sobre A da forma

$$x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_1 \cdot x + a_0 = 0 \tag{4.10}$$

Logo, aplicando τ_i em ambos os lados de (4.10), teremos

$$x_i^n + a_{n-1} \cdot x_i^{n-1} + \ldots + a_i \cdot x + a_0 = 0.$$

já que $\tau_i(x) = x_i,\ \tau_i(a_i) = a_i$, para $i = 1,\ldots,n-1$. Consequentemente cada x_i é inteiro sobre A. Já que $T[L|K](x)$ e $N[L|K](x)$ são coeficientes de $char(x)$, o resultado segue-se. A última afirmação é trivial. □

4.3 O Discriminante.

Para o que se segue nós consideraremos a configuração básica $AKLB$, definida anteriormente, com $n = [L|K]$.

Definição 4.3.1. *Para quaisquer $x_1,\ldots,x_n \in L$, definimos o discriminante da $n-$upla $(x_1,\ldots,x_n)$ como*

$$D(x) = det\ \left(T[L|K](x_i \cdot x_j)\right).$$

Então, para calcularmos $D(x)$, formamos a matriz onde o elemento a_{ij} é o traço de $x_i \cdot x_j$, e tomamos o determinante desta matriz. Pelo Lema 4.2.1, $D(x)$ pertence a K. Se os x_i estão em B, então pela Proposição 4.2.3 $D(x)$ é inteiro sobre A.

Lema 4.3.1. *Se $y = C \cdot x$, onde C é uma matriz quadrada de ordem n sobre K, e x e y são n−uplas escritas como vetores colunas, então $D(y) = (det\ C)^2 D(x)$.*

Demonstração. Sendo $y = (y_1, \ldots, y_n)$, $x = (x_1, \ldots, x_n)$ e $C = [c_{ij}]$, então

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} c_{11} & \ldots & c_{1n} \\ c_{21} & \ldots & c_{2n} \\ \vdots & & \vdots \\ c_{n1} & \ldots & c_{nn} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} c_{11} \cdot x_1 + \ldots + c_{1n} \cdot x_n \\ c_{21} \cdot x_1 + \ldots + c_{2n} \cdot x_n \\ \vdots \\ c_{n1} \cdot x_1 + \ldots + c_{nn} \cdot x_n \end{bmatrix}.$$

Assim,

$$y_r \cdot y_s = \sum_{i=1}^{n} c_{ri} \cdot x_i \cdot \sum_{i=1}^{n} c_{si} \cdot x_i = \sum_{i,j=1}^{n} c_{ri} \cdot c_{sj} \cdot x_i \cdot x_j.$$

Logo, o traço de $y_r \cdot y_s$ é

$$T\left(\sum_{i,j=1}^{n} c_{ri} \cdot c_{sj} \cdot x_i \cdot x_j \right) = \sum_{i,j=1}^{n} c_{ri} \cdot T(x_i \cdot x_j) \cdot c_{sj}.$$

Consequentemente a matriz

$$(T(y_r y_s)) = C \cdot T(x_i x_j) \cdot C'$$

onde C' é matriz transposta de C. Logo,

$$det\ (T(y_r y_s)) = det\ [C \cdot T(x_i x_j) \cdot C'] = det\ C \cdot det\ (T(x_i x_j)) \cdot det\ (C').$$

Como $det\ C = det\ C'$, então segue-se o resultado. □

Lema 4.3.2. *Seja $\sigma_1, \ldots, \sigma_n$ os K−mergulhos de L em um fecho algébrico de L. Então, $D(x) = [det\ (\sigma_i(x_j))]^2$(Ou seja, formamos a matriz onde o elemento de coordenada ij é o elemento $\sigma_i(x_j)$, tomamos o determinante e elevamos o resultado ao quadrado).*

Demonstração. Pela Proposição 4.2.2

$$T(x_i x_j) = \sum_{k=1}^{n} \sigma_k(x_i x_j) = \sum_{k=1}^{n} \sigma_k(x_i) \cdot \sigma_k(x_j).$$

Logo, se C é a matriz cujas entradas ij são os elementos $\sigma_i(x_j)$, então

$$\big(T(x_i x_j)\big) = C' \cdot C \tag{4.11}$$

onde C' é a matriz transposta de C. Assim, tomando o determinante de ambos os lados de (4.11), teremos:

$$det\ \big(T(x_i x_j)\big) = det\ (C' \cdot C) = det\ C' \cdot detC.$$

O resultado segue-se já que $det\ C = det\ C'$. □

Proposição 4.3.1. *Seja $x = (x_1, \ldots, x_n)$, então os x_i formam uma base para L sobre K se, e somente se, $D(x) \neq 0$*

Demonstração. Suponhamos que $D \neq 0$ e que os $x_1, \ldots, x_n$ sejam linearmente dependentes. Então existem $c_1, \ldots, c_n$ não todos iguais a zero, tal que

$$\sum_{j=1}^{n} c_j \cdot x_j = 0 \tag{4.12}$$

Então, aplicando δ_i, para $i = 1, \ldots, n$ em ambos os lados da equação 4.12, teremos

$$\delta_i \left(\sum_{j=1}^{n} c_j \cdot x_j \right) = \sum_{j=1}^{n} c_j \cdot \delta_i \cdot (x_j) = 0.$$

Consequentemente, as colunas da matriz $B = (\delta_i(x_j))$ são linearmente dependentes e, portanto, $D(x) = 0$, uma contradição. Agora suponhamos que os n x_j sejam linearmente independentes e consequentemente uma base para L sober K, já que $n = [L : K]$. Se $D(x) = 0$, então as linhas da matriz $B = [\delta_i(x_j)]$ são linearmente dependentes. Logo, existem $c_1, c_2, \ldots, c_n$ não todos nulos, tais que

$$c_1 \cdot (\delta_1(x_1), \ldots, \delta_1(x_n)) + \ldots + c_n \cdot (\delta_n(x_1), \ldots, \delta_n(x_n)) = (0, \ldots, 0)$$

Assim,

$$(c_1 \cdot \delta_1(x_1) + \ldots + c_n \cdot \delta_n(x_1), \ldots, c_1 \cdot \delta_1(x_n) + \ldots + c_n \cdot \delta_n(x_n)) = (0, \ldots, 0)$$

Logo, teremos que para $c_1, \ldots, c_n$ não todos nulos vale que

$$\sum_{i=1}^{n} c_i \cdot \delta_i \cdot (x_j) = 0, \ \forall \ j. \qquad (4.13)$$

Então, se mostrarmos que os δ_i são linearmente dependentes, então chegaremos a uma contradição, em vista do Teorema de Dedekind. Seja então $u \in L$, mostremos que

$$\sum_{i=1}^{n} c_i \cdot \delta_i(u) = 0$$

De fato, como $u \in L$ e $x_1, \ldots, x_n$ é uma base de L sobre K por hipótese, então existem $b_1, \ldots, b_n$ tal que

$$u = b_1 \cdot x_1 + \ldots + b_n \cdot x_n.$$

Logo,

$$\sum_{i=1}^{n} c_i \cdot \delta_i(u) = \sum_{i=1}^{n} c_i \cdot \delta_i \left(\sum_{k=1}^{n} b_k \cdot x_k \right) = \sum_{i=1}^{n} \sum_{k=1}^{n} b_k \cdot c_i \cdot \delta_i(x_k) \ Por \underset{=}{4.13}$$

$$= \sum_{k=1}^{n} b_k \cdot \sum_{i=1}^{n} c_i \cdot \delta_i(x_k) = \sum_{k=1}^{n} b_k \cdot 0 = 0.$$

Consequentemente, $\delta_1, \ldots, \delta_n$ são L.D e segue-se o resultado. □

Lema 4.3.3. *Existe uma base para L/K consistindo inteiramente de elementos de B.*

Demonstração. Sejam $x_1, \ldots, x_n$ uma base de L sobre K. Como cada x_i é algébrico sobre K, então satisfaz uma equação da forma

$$a_m {x_i}^m + \ldots + a_1 x_i + a_0 = 0. \qquad (4.14)$$

com $a_m \neq 0$ e $a_i \in A$.(Inicialmente, temos $a_i \in K$,mas sendo K o corpo de frações de A, então cada a_i é da forma $a_i = \dfrac{b_i}{c_i}$. Tomando $d = mmc(c_0, \ldots, c_m)$, onde *mmc* denota o mínimo múltiplo comum, e multiplicando por (4.14), então obtemos uma equação em que os coeficientes pertencem a A.) Agora, multiplicando a equação (4.14) por a_m^{m-1}, teremos

$$a_m^m \cdot x_i^m + \ldots + a_m^{m-1} \cdot a_0 = 0 \qquad (4.15)$$

Logo, fazendo $y_i = a_m \cdot x_i$, obteremos

$$y_i^m + a_{m-1}^{m-2} \cdot y_i^{m-1} + \ldots + a_m^{m-1} \cdot y_0 = 0.$$

Concluímos assim que y_i é inteiro sobre A, para cada $i = 1, \ldots, n$. É claro que $y_1, \ldots, y_n$ formam uma base já que os $x_1, \ldots, x_n$ são uma base. □

Para o que segue, sejam $x_1, \ldots, x_n$ uma base para o espaço vetorial V sobre K e B uma aplicação bilinear sobre V. Dizemos que $y_1, \ldots, y_n$ é uma base dual referida para V se

$$B(x_i, y_j) = \delta_{ij} = \begin{cases} 1, \ se \ i = j \\ 0, \ se \ i \neq j \end{cases}$$

Teorema 4.3.2. *Se A é integralmente fechado, então B é um A− módulo livre de posto n.*

Demonstração. Observe primeiramente que o Traço pode ser considerado uma aplicação T_r de duas variáveis fazendo $T_r(x,y) = T(xy)$ para todo $x, y \in E$. Mostremos então que T_r é uma forma bilinear, simétrica e não degenerada.

1) Bilinearidade:

$$T_r(cx_1 + cx_2, b) = T((cx_1 + cx_2) \cdot b) = T(cx_1 b + cx_2 b) = T(cx_1 b) + T(cx_2 b) =$$

$$c \cdot T(x_1 b) + c \cdot T(x_2 b) = c \cdot T_r(x_1, b) + c \cdot T_r(x_2, b).$$

Analogamente, prova-se que:

$$T_r(a, cb_1 + cb_2) = c \cdot T_r(a, b_1) + c \cdot T_r(a, b_2).$$

2) Simetria:

Ora, temos que

$$T_r(x,y) = T(x \cdot y) = T(y \cdot x) = T_r(y,x).$$

3) T é não degenerada:

Tomemos $y \neq 0$ e suponhamos que $T_r(x,y) = 0$ para todo $x \in E$. Então, como x pode ser escrito na forma $x = \frac{z}{y}$, teremos que $T_r(x,y) = T_r(\frac{z}{y}, y) = T_(\frac{z}{y} \cdot y) = T(z) = 0, \forall \ z \in E$. Absurdo, pois contraria o Coralário 4.2.3.

Como A é integralmente fechado por hipótese então pela Proposição 4.2.3, o traço de qualquer elemento de B pertence a A. Assim, seja $x_1, \ldots, x_n$ uma base para L sobre K, consistindo de

inteiros, isto é, de elementos de B (Isto é possível pelo Lema 4.3.3) e seja $y_1, \ldots, y_n$ a base dual referida para L. Então, se $z \in B$, podemos escrever

$$z = \sum_{j=1}^{n} a_j \cdot y_j,\ a_j\ \in K.$$

Já sabemos que o Traço de $x_i \cdot z$ pertence a A, consequentemente

$$T_r(x_i, z) = T(x_i \cdot z) = T\left(\sum_{j=1}^{n} a_j \cdot x_i \cdot y_j\right) = \sum_{j=1}^{n} a_j \cdot T(x_i y_i) = \sum_{j=1}^{n} a_j \cdot \delta_{ij} = a_i.$$

Assim, $a_i \in A$ e, portanto, B é um $A-$submódulo do $A-$módulo livre $\bigoplus_{j=1}^{n} A y_j$. Pelo Teorema 3.2.4, B é um $A-$módulo livre de *posto* no máximo n. Pelo Lema 4.3.3 , B contém uma base para L sobre K, e se desejarmos podemos assumir que esta base é $x_1, \ldots, x_n$. Então, B contém o $A-$módulo livre

$$\bigoplus_{j=1}^{n} A x_j$$

.Logo teremos que o *posto* de B é pelo menos n e, portanto, exatamente n. □

Desta forma fazendo $A = \mathbb{Z}$ no teorema anterior provamos que o conjunto $B = I_L$ de inteiros algébricos em qualquer corpo numérico L é um $\mathbb{Z}-$módulo livre de rank $n = [L : \mathbb{Q}]$.

4.4 Módulos Noetherianos.

Em tudo o que segue, salvo menção em contrário, M denota um R-módulo.

Definição 4.4.1. *Uma sequência (*crescente*) $M_1 \subseteq M_2 \subseteq M_3 \subseteq \ldots$ de submódulos de M é estacionária se, para algum $t \geq 1$, tivermos $M_t = M_{t+1} = \ldots$.*

Dizemos então que o módulo M satisfaz a Condição de Cadeia Ascendente (C.C.A) se toda sequência crescente de submódulos for estacionária. A próxima proposição no fornece a definição de $R-$módulo Noetheriano.

Proposição 4.4.1. *As seguintes condições em um $R-$módulo M são equivalentes:*

(1) M satisfaz o C.C.A;

(2) Cada coleção não vazia de submódulos de M têm um elemento maximal (com respeito à inclusão).

Demonstração. Assuma (1) e seja S uma coleção não vazia de submódulos de M. Escolhamos $M_1 \in S$. Se M_1 é maximal, terminamos. Caso contrário, existe $M_2 \in S$ tal que $M_1 < M_2$. Se M_2 é maximal, terminamos. Caso contrário existe M_3 talque $M_1 < M_2 < M_3$. Continuando desta forma, então o processo deve terminar, pois, caso contrário, encontraríamos uma sequência de submódulos que não estabilizaria.

Agora, assumimos (2) e seja $M_1 \leq M_2 \cdots$ uma sequência crescente de submódulos.Consequentemente $M_1 \leq M_2 \cdots$ é estacionária ,pois, caso contrário, a coleção não vazia de submódulos $\{M_1, M_2, \cdots\}$ não teria elemento maximal. □

Definição 4.4.2. *Se um $R-$módulo M satisfaz uma das condições equivalentes acima, dizemos que M é (um R-módulo) noetheriano.Em particular, um anel R é noetheriano se for um R-módulo noetheriano.*

Proposição 4.4.2. *M é Noetheriano se, e somemente se, cada submódulo de M é finitamente gerado.*

Demonstração. Suponha que cada submúdulo de M seja finitamente gerado e que M não seja Noetheriano. Então, existe uma sequência crescente $M_1 \leq M_2 \leq \cdots$ que não é estacionária. Seja assim $N = \bigcup_{i=1}^{\infty} M_i$. Segue-se então que N é um submódulo de M e não pode ser finitamente gerado, pois se $x_1, \ldots, x_t$ gerassem N, então para t suficientemente grande cada x_i pertenceria a M_t. Mas, então

$$N \subseteq M_t \subseteq M_{t+1} \ldots \subseteq N.$$

Logo, $M_t = M_{t+1} = \cdots$ e a sequência $M_1 \leq M_2 \leq \cdots$ seria estacionária.

Agora suponha que seja válido a C.C.A e seja $N \leq M$ Se $N \neq \emptyset$, escolhamos $x_1 \in N$. Se $Rx_1 = N$, então N é finitamente gerado. Caso contrário, existe $x_2 \notin Rx_1$. Se x_1 e x_2 geram N, terminamos. Caso contrário, existe $x_3 \notin Rx_1 + Rx_2$. Como

$$Rx_1 \leq Rx_1 + Rx_2 \leq \cdots$$

então, pelo C.C.A, é estacionária. Consequentemente, teremos que $x_1, \ldots, x_t$ geram N. □

Observação: Veja que se $N \leq M$, então um submódulo L de M que contém N, sempre pode ser escrito na forma $K + N$ para algum submódulo K ($K = L$ é uma possibilidade). Pelo Teorema de correspondência

$$\frac{K_1+N}{N} = \frac{K_2+N}{N} \Rightarrow K_1+N = K_2+N$$

e

$$\frac{K_1+N}{N} \leq \frac{K_2+N}{N} \Rightarrow K_1+N \leq K_2+N.$$

Proposição 4.4.3. *Seja N um submódulo de M. Então M é Noetheriano se, e somente se, N e M/N são Noetherianos.*

Demonstração. Assumimos primeiro que M é Noetheriano e mostremos que N e M/N são Noetheriano. Seja $N_1 \leq N_2 \leq \ldots$ uma sequência crescente de submódulo de N. Como qualquer submódulo de N é também um submódulode M, então segue-se que $N_1 \leq N_2 \leq \ldots$ é estacionária e portanto N é Noetheriano.Pela observação acima uma sequência crescente de submódulos de M/N, tem a forma

$$\frac{M_1+N}{N} \leq \frac{M_2+N}{N} \leq \cdots.$$

Mas então, pelo Teorema da Correspondência para módulos, os M_i+N formam uma sequência crescente de submódulos de M, o qual é estacionária. Consequentemente, $\frac{M_i+N}{N}$, $i = 1,2,\ldots$ também é estacionária. Agora assuma que N e M/N são Noetherianos e seja

$$M_1 \leq M_2 \leq \ldots$$

uma sequência crescente de módulos de M. Tome i suficientemente grande para que ambas as sequências $\{M_i \cap N\}$ e $\{M_i+N\}$ sejam estacionárias. Assim, seja $x \in M_{i+1}$, então $x+N \in M_{i+1}+N = M_i+N$. Logo, $x+a = y+b$, onde $y \in M_i$ e $a,\ b\ \in N$. Assim

$$x = y+(b-a), \text{ com } y \in M_i \text{ e } b-a \in N.$$

Então $x-y \in M_{i+1} \cap N = M_i \cap N$ e, já que $y \in M_i$, então $x \in M_i$. Portanto, $M_i = M_{i+1} = \cdots$. □

Corolário 4.4.1. *Se $M_1,\ldots,M_n$ são R-módulos noethenianos, então a soma direta $M_1 \oplus M_2 \oplus \ldots \oplus M_n$ também é um R-módulo noetheriano.*

Demonstração. Faremos isto por indução sobre n. Para $n = 2$, façamos $N = M_1$. Então, $N := M_1$ será um submódulo de $M := M_1 \oplus M_2$. Seja assim a função projeção de M sobre N dada por

$$P_{r_1} : \underset{x_1+x_2}{M_1 \oplus M_2} \underset{\longmapsto}{\to} \underset{x_2}{M_2}$$

Assim, temos que P_r é um homomorfismo sobrejetor e

$$N(P_{r_1}) = \{x \in M \; ; \; P_{r_1}(x) = 0\} = \{a_1 + a_2 \in M; P_r(a_1 + a_2) = 0\} =$$

$$\{a_1 + a_2 \in M_1 \oplus M_2; a_2 = 0\} = N.$$

Logo, pelo Teorema 3.2.1 $M_2 \cong M/N$. Como M/N e N são Noetherianos, então M é Noetheriano. Agora, suponha o resultado válido para k e tome assim como no caso $n = 2$ uma projeção P_{r_2} de $M_1 \oplus \ldots \oplus M_{k+1}$ sobre $M_2 \oplus \ldots \oplus M_{k+1}$ que pega $x = x_1 + x_2 + \ldots + x_{k+1}$ e leva em $x_2 + x_3 + \ldots + x_{k+1}$. Então, teremos que P_{r_2} é um homomorfismo sobrejetor e $N(P_{r_2}) = N = M_1$. Logo, pelo Primeiro Teorema do Isomorfismo para Módulos, teremos que

$$\frac{M_1 \oplus \ldots \oplus M_{k+1}}{M_1} \cong M_2 \oplus \ldots \oplus M_{k+1}.$$

e, portanto, M_2/N é Noetheriano já $M_2 \oplus \ldots \oplus M_{k+1}$ é Noetheriano por hipótese de indução. Logo, $M_1 \oplus M_2 \oplus \ldots \oplus M_{k+1}$ é Noetheriano para cada n. □

Proposição 4.4.4. *Na configuração básica AKLB, assuma que A é integralmente fechado. Se A é um anel Noetheriano, então B também é.*

Demonstração. Como $[L : K]$ é finito,pelo Lema 4.3.3, existe uma base $x_1, \ldots, x_n$ de L sobre K, consistindo de elementos B. Pela prova de 4.3.2 , B é um submódulo do $A-$módulo livre

$$M = Ax_1 \oplus Ax_2 \oplus \ldots \oplus Ax_n$$

de *rank* finito n. Pelo Corolário 4.4.1, M é Noetheriano por ser finitamente gerado e pela proposição 4.4.3 B é um $A-$módulo Noetheriano. Seja então I um ideal de B, e mostremos que I é finitamente gerado. Um ideal de B é, em particular, um $A-$submódulo de B. Consequentemente finitamente gerado sobre A e, portanto, sobre B. Então B é um anel Noetheriano. □

5 O TEOREMA PRINCIPAL E UM EXEMPLO INTERESSANTE

Neste capítulo, juntamos os conteúdos desenvolvidos até agora para mostrar o resultado principal da dissertação, o qual nomeia a próxima seção. Apresentamos, ainda, dois exemplos interessante, o qual mostra que, na prática, a tarefa de identificar o anel dos inteiros de um corpo de números pode ser bastante não trivial.

5.1 O anel de inteiros de um corpo de números é um dominio de Dedekind

O resultado principal da dissertação tem relação com a definição a seguir.

Definição 5.1.1. *Dizemos que R é um domínio de Dedekind se satisfaz as seguintes condições:*
(I) R é Noetheriano;
(II) R é Integralmente Fechado;
(III) Cada ideal primo diferente de zero é maximal.

O exemplo mais simples possível é $\mathbb{Z}$, e as condições da definição acima são postas exatamente para tentar estender propriedades de $\mathbb{Z}$ a domínios mais gerais.

A seguir, enunciamos e provamos o resultado principal da dissertação.

Teorema 5.1.1. *Na configuração básica AKLB, se A é um Domínio de Dedekind, então B também é. Em particular, o anel de inteiros algébricos em um corpo numérico é um Domínio de Dedekind. Além disso, B é um $A-$módulo finitamente gerado e o corpo quociente de B é L*

Demonstração. Para mostrarmos que B é um Domínio de Dedekin, devemos mostrar que:
a) B é integralmente fechado;
b) B é Noetheriano, e
c) Cada ideal primo de B é maximal.

a) Como B é o fecho inteiro de A em L, a Proposição 4.1.5 garante que B é integralmente fechado em L. Basta, pois, mostrar que L é o corpo de quocientes de B (o que também estabelece a última parte do teorema).Se $x \in L$, então, como x é algébrico sobre K e K é o corpo de quocientes de A, existem $a_0, \ldots, a_m \in A$ tais que $a_m \neq 0$ e

$$a_m x^m + \ldots + a_1 x + a_0 = 0.$$

Multiplicando a igualdade acima por a_m^{m-1} e fazendo $y = a_m x$, concluímos que y é inteiro sobre A, logo, $y \in B$.Como $a_m \in A \subseteq B$ e $x = \frac{y}{a_m}$, concluímos que x pertence ao corpo de quocientes de B, o resultado como queremos.

b) Como A é um domínio de Dedekind, é integralmente fechado. Portanto, pela Proposição 4.4.4., B é um anel noetheriano. Aproveitaremos para mostrar que B é um A-módulo finitamente gerado.Pelo Teorema 4.3.2, B é um submódulo de um A-módulo livre M da forma

$$M = Ax_1 \oplus Ax_2 \oplus \ldots \oplus Ax_n.$$

Pelo Corolário 4.4.1, M é um A-módulo noetheriano. Logo, B também é um $A-$módulo noetheriano.

c) Seja Q um ideal primo não nulo de B e tome $x \in Q \setminus \{0\}$. Como B é inteiro sobre A, x satisfaz uma equação polinomial da forma

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0,$$

com $a_i \in A$ para $0 \leq i < n$.Tomando o menor n possível, temos claramente $a_0 \neq 0$.Assim,

$$a_0 \in Bx \cap A \subseteq Q \cap A.$$

Fazendo $P = Q \cap A$, segue que $a_0 \in P$, logo, $P \neq \{0\}$.Pela Proposição 4.1.3, item (a), P é um ideal primo não nulo de A. Mas, como A é domínio de Dedekind, P é maximal e, daí, A/P é um corpo. Novamente pela Proposição 4.1.3, itens (a) e (b), A/P pode ser considerado como subanel de B/Q, com B/Q inteiro sobre A/P.Mas, como A/P é um corpo, o Lema 4.1.2 garante que B/Q também é um corpo. Finalmente, mais uma vez pela Proposição 4.1.3, item (c), Q é maximal.

□

Como corolário imediato teremos que:

Corolário 5.1.1. *Seja L um corpo de números algébricos. Então I_L é um Domínio de Dedekind.*

5.2 Caraterização de Extensões Quadráticas dos Racionais.

Extensões Quadráticas dos Racionais.

Neste exemplo caracterizaremos e determinaremos o conjunto de inteiros algébricos de $L = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados. Veja que a restrição em d não envolve perda de generalidade, por exemplo $\mathbb{Q}(\sqrt{12}) = \mathbb{Q}(\sqrt{3})$.

Para o Lema abaixo consideraremos σ como o automorfismo de L que leva $a+b\sqrt{d}$ em $a-b\sqrt{d}$. Na verdade prova-se facilmente que o conjunto de todos os automorfismos de L é formado por σ e pela função identidade.

Lema 5.2.1. *Sejam $a,b \in \mathbb{Q}$. Então $a+b\sqrt{d}$ é um inteiro algébrico se e somente se $2a$ e a^2-db^2 pertencem a $\mathbb{Z}$.Neste caso $2b$ também é um inteiro algébrico.*

Demonstração. Seja $x = a+b\sqrt{d}$ um inteiro algébrico. Então x é a raiz de um polinômio mônico $f \in \mathbb{Z}[X]$. Ora, como $f(\sigma(x)) = \sigma(f(x))$ e já que σ é um automoorfismo, então segue-se que $\sigma(x)$ é também um raiz de f, e consequentemente um inteiro algébrico. Segue que pela Proposição 4.1.4 que $x+\sigma(x) = 2a$ e $x\cdot\sigma(x) = a^2-db^2$ são inteiros algébricos. Pela Proposição 4.1.6 $\mathbb{Z}$ é integralmente fechado, logo $2a$ e a^2-db^2 são números inteiros. Agora suponha que $2a$ e a^2-db^2 são números inteiros. Veja que $a+b\sqrt{d}$ é raiz de $(x-a)^2 = db^2$, isto é, raiz de $f(x) := x^2-2ax+a^2-db^2$. Como os coeficientes de $f(x)$ são inteiros segue-se o resultado.

Agora se $2a$ e a^2-db^2 são números inteiros então $(2a)^2-d(2b)^2 = 4(a^2-db^2) \in \mathbb{Z}$. Logo $d(2b)^2 \in \mathbb{Z}$. Se $2b \notin \mathbb{Z}$ então o denominado de b deve incluir algum fator primo p na fatoração de seu denominado que não aparece na fatoração de seu numerador ou que aparece em quantidade maior. Neste caso, esse fator p aparecerá como p^2 em $(2b)^2$. Multiplicando $(2b)^2$ por d teremos um número inteiro, logo p^2 deve aparecer na fatoração de d, que é um absurdo, pois d é livre de quadrados. Isto encerra nossa prova. □

Damos abaixo uma caracterização dos inteiros algébricos B de $\mathbb{Q}(\sqrt{d})$.

Teorema 5.2.1. *O conjunto B de inteiros algébricos de $\mathbb{Q}(\sqrt{d})$ com d livre de quadrados, pode ser descrito como se segue:*

(i) se $d \not\equiv 1 \mod 4$, então B consiste de todos $a+b\sqrt{d}$, onde $a,b \in \mathbb{Z}$.

(ii) se $d \equiv 1 \mod 4$ então B consiste de todos $\frac{u}{2}+\frac{v}{2}\sqrt{d}$, onde $u,v \in \mathbb{Z}$ têm a mesma paridade (Isto é, ambos são pares ou ambos são ímpares).

Demonstração. Pelo Lema anterior, os inteiros algébricos de $\mathbb{Q}(\sqrt{d})$ são da forma $\frac{u}{2}+\frac{v}{2}\sqrt{d}$, onde $u,v \in \mathbb{Z}$ e $\frac{u^2}{4}-d\frac{v^2}{4} \in \mathbb{Z}$, isto é $u^2-dv^2 \equiv 0 \mod 4$. Então se $d \not\equiv 1 \mod 4$ segue que $d \equiv 2 \mod 4$ ou $d \equiv 3 \mod 4$, logo usando calculos simples concluímos que ambos u,v devem ser pares que prova (i). O caso (ii) segue-se de maneira inteiramente análoga. □

5.3 Caracterização dos Inteiros Algébricos da p-ésima Extensão Ciclotômica

Terminamos esta dissertação explicitando o anel dos inteiros da p-ésima extensão ciclotômica $\mathbb{Q}(\zeta)$, onde $\zeta = e^{2\pi i/p}$, com p primo.Usaremos como referência (TALL, 2015). No entanto, faremos antes algumas considerações. Observe primeiramente que para $p = 2$, $\zeta = e^{2\pi i/2} = -1$ logo $\mathbb{Q}(\zeta) = \mathbb{Q}$. Consequentemente ignoramos este caso e assumiremos p ímpar.

É possivel provar facilmente que o polinômio minimal de $\zeta = e^{2\pi i/p}$ sobre $\mathbb{Q}$ é

$$f(t) := t^{p-1} + t^{p-2} + \cdots + t + 1 \tag{5.1}$$

Logo $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$. Veja também que as potências $\zeta, \zeta^2, \cdots, \zeta^{p-1}$ são também pth raízes da unidade,não iguais a 1, com o mesmo polinômio minimal de ζ, isto é, $f(t)$.

Por um argumento simples vemos que $f(t)$ pode ser fatorado sobre $\mathbb{C}$ na forma

$$f(t) = (t - \zeta)(t - \zeta^2)\cdots(t - \zeta^{p-1}) \tag{5.2}$$

e logo $\zeta, \zeta^2, \cdots, \zeta^{p-1}$ serão conjugadas de ζ. Consequentemente pelo Teorema 3.1.20 e pelo Teorema 3.1.8 os $p - 1$ mergulhos (monomorfismos) possíveis serão dados por

$$\sigma_i(\zeta) = \zeta^i, i = 1, 2, \cdots, p - 1 \tag{5.3}$$

Já que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$ então $\{ 1, \zeta^2, \cdots, \zeta^{p-2}\}$ será uma base de $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$. Desta forma um elemento α qualquer de $\mathbb{Q}(\zeta)$ poderá ser escrito como:

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$$

com $a_i \in \mathbb{Q}$, $i = 1, \cdots, p - 2$. Obteremos assim que para cada σ_i dado em 5.3

$$\sigma_i(\alpha) = \sigma_i(a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}) = a_0 + \zeta^i + \cdots + a_{p-1}\zeta^{i(p-2)} \tag{5.4}$$

Usando 5.4, calculemos agora a norma e o traço de cada ζ^i. Pela proposição 4.2.2 , teremos que para cada $\alpha \in \mathbb{Q}(\zeta)$

$$T(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \; e \; N(\alpha) = \prod_{i}^{n} \sigma_i(\alpha).$$

Em particular

$$N(\zeta) = \zeta \cdot \zeta^2 \cdots \zeta^{p-1} \; e \; T(\zeta) = \zeta + \zeta^2 + \cdots + \zeta^{p-1} \tag{5.5}$$

Agora como ζ e ζ^i são conjugadas uma da outra então possuem a mesma norma e o mesmo traço já que os σ_{is} varrem todas as raízes do polinômio minimal de ζ.Assim

$$N(\zeta) = N(\zeta^i) = (-1)^{p-1} \tag{5.6}$$

o qual pode ser calculado usando 5.5 ou fazendo $t = 0$ em 5.2. Como p é ímpar então,

$$N(\zeta) = N(\zeta^i) = 1. \tag{5.7}$$

Já que

$$f(\zeta) = 1 + \zeta + \cdots + \zeta^{p-1}$$

então

$$T(\zeta^i) = -1 \tag{5.8}$$

onde $i = 1, \cdots, p-1$ .Ora, como $\zeta^p = 1$ nós podemos usar as fórmulas em (5.7) e (5.8) para calcular $N(\zeta^s)$ e $T(\zeta^s)$ para todo $s \in \mathbb{Z}$.Este é o resultado do Lema seguinte:

Lema 5.3.1. *Seja $s \in \mathbb{Z}$ então $N(\zeta^s) = 1$ e $T(\zeta^s) = \begin{cases} -1, \text{ se } s \equiv 0 \\ 0, \text{ se } s \not\equiv 0 \end{cases}$.*

Demonstração. Seja $s \in \mathbb{Z}$. Usando divisão eu eclidiana então podemos escrever $s = pq + r$ com $0 \leq |r| < p$. Logo

$$\zeta^s = \zeta^{pq} \cdot \zeta^r = \zeta^r$$

Veja que se $r < 0$ então $\zeta^r = \dfrac{1}{\zeta^{-r}}$. Logo, multiplicando o numerado e o denominador de $\dfrac{1}{\zeta^{-r}}$ por ζ^t onde $t + (-r) = p$ então

$$\zeta^r = \frac{1}{\zeta^{-r}} = \zeta^t$$

Consequentemente

$$N(\zeta^s) = N(\zeta^r) = 1 \tag{5.9}$$

já que ζ e ζ^r são conjugadas uma da outra.Para o traço devemos considerar dois casos:

Caso 01) Vale $s \equiv 0 (mod\, p)$

Temos assim que $s = kp$ onde $k \in \mathbb{Z}$ logo, pelo Lema 4.2.1

$$T(\zeta^s) = T(1) = p - 1$$

Caso 02) Vale que $s \not\equiv 0(mod\, p)$

Neste caso teremos que $s = kp + r$, com $0 < |r| < p$. Logo, assumindo sem perda de generalidade que $r > 0$ então

$$T(\zeta^s) = T(\zeta^r) = -1$$

o que conclui o desejado.

□

Usando o Lema anterior podemos calcular o traço de um elemento qualquer de $\mathbb{Q}(\zeta)$ facilmente. De fato,para $\alpha \in \mathbb{Q}(\zeta)$ temos

$$T\left(\sum_{i=0}^{p-2} a_i\zeta^i\right) = \sum_{i=0}^{p-2} T(a_i\zeta^i) = T(a_0) + \sum_{i=1}^{p-2} T(a_i\zeta^i) = (p-1)a_0 + \sum_{i=1}^{p-2} a_i T(\zeta^i) = (p-1)a_0 - \sum_{i=1}^{p-2} a_i$$

A norma é mais complicada em geral, mas um caso nos será útil

$$N(1-\zeta) = \prod_{i=1}^{p-1}(1-\zeta^i)$$

o qual pode ser calculado fazendo t=1 em (5.2), obtendo assim

$$\prod_{i=1}^{p-1}(1-\zeta^i) = p. \tag{5.10}$$

e portanto

$$N(1-\zeta) = p. \tag{5.11}$$

Agora, voltamos a nossa primeira afirmação. Mostraremos então que

Teorema 5.3.1. *O anel B de inteiros algébricos de* $\mathbb{Q}(\zeta)$ *é* $\mathbb{Z}(\zeta)$.

Demonstração. É claro que todo elemento de $\mathbb{Z}(\zeta)$ é um inteiro algébrico de $\mathbb{Q}(\zeta)$.Reciprocamente, seja $\alpha \in \mathbb{Q}(\zeta)$ um inteiro algébrico. Já vimos que cada $\alpha \in \mathbb{Q}(\zeta)$ pode ser escriro como

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2},$$

para certos racionais $a_0, \ldots, a_{p-2}$. Devemos mostrar que os números racionais a_i são inteiros. Afirmamos primeiramente que, para $0 \leq k \leq p-2$, o número

$$\alpha\zeta^{-k} - \alpha\zeta$$

é um inteiro algébrico.De fato, basta obervar que α, ζ e ζ^{-k} são inteiros algébricos, de sorte que os produtos e somas entre esses elementos também são inteiros algébricos.Agora, como $\mathrm{Tr}(\alpha\zeta^{-k}-\alpha\zeta)$ é um racional que é inteiro sobre $\mathbb{Z}$ e $\mathbb{Z}$ integralmente fechado, temos que $\mathrm{Tr}(\alpha\zeta^{-k}-\alpha\zeta)$ é inteiro. Mas,

$$T(\alpha\zeta^{-k}-\alpha\zeta)=T(a_0\zeta^{-k}+\cdots+a_k+\cdots+a_{p-2}\zeta^{p-k-2}-a_0\zeta-\cdots-a_{p-2}\zeta^{p-1})=$$

$$=pa_k-(a_0+\cdots+a_{p-2}-(a_0-\cdots-a_{p-2})=pa_k$$

Consequentemente $b_k:=pa_k$ é um número inteiro.

Fazendo $\lambda=1-\zeta$, temos $\zeta=1-\lambda$ e, daí,

$$p\alpha=b_0+b_1\zeta+\cdots+b_{p-2}\zeta^{p-2}= \tag{5.12}$$

$$=c_0+c_1\lambda+\cdots+c_{p-2}\lambda^{p-2} \tag{5.13}$$

com

$$c_i=\sum_{j=1}^{p-2}(-1)^i\binom{j}{i}b_j\in\mathbb{Z}$$

Como $\lambda=1-\zeta$, temos, simetricamente,

$$b_i=\sum_{j=1}^{p-2}(-1)^i\binom{j}{i}c_j\in\mathbb{Z}$$

Como $b_k=pa_k$, basta mostrarmos que todos os c_i são divisíveis por p. Para $i=0$ temos:

$$c_0=b_0+\cdots+b_{p-2}=pa_0+\cdots+pa_{p-2}=$$

$$=p(a_0+\cdots+a_{p-2})=p(-T(\alpha)+b_0).$$

Logo $p|c_0$.

Suponha que $p\mid c_i$ para todo $i\leq k-1$, onde $1\leq k\leq p-2$. Por (5.10) , temos que

$$p=\prod_{i=1}^{p-1}(1-\zeta^i)=(1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{p-1})=$$

$$=(1-\zeta)^{p-1}\prod_{i=1}^{p-1}(1+\zeta+\cdots+\zeta^{i-1})=\lambda^{p-1}\cdot k$$

ou seja

$$p = \lambda^{p-1} \cdot k \tag{5.14}$$

com $k \in \mathbb{Z}[\zeta] \subseteq B$.Como $k+1 \leq p-1$, a igualdade $p = \lambda^{p-1}\tau$ garante que

$$p \equiv 0 \,(\mathrm{mod}\,(\lambda^{k+1})), \tag{5.15}$$

onde (λ^{k+1}) denota o ideal de B gerado por λ^{k+1}.Projetemos em $B/(\lambda^{k+1})$ a igualdade (cf.5.12)

$$p\alpha = c_0 + c_1\lambda + \cdots + c_{p-2}\lambda^{p-2}.$$

O lado esquerdo desaparece, por (5.15); os termos até $c_{k-1}\lambda^{k-1}$ do lado direito desaparecem (pela hipótese de indução); os termos a partir de $c_{k+1}\lambda^{k+1}$ também desaparecem, pois são múltiplos de λ^{k+1}. Ficamos com

$$c_k\lambda^k \equiv 0 \,(\mathrm{mod}\,(\lambda^{k+1})),$$

de forma que $c_k\lambda^k = \mu\lambda^{k+1}$, para algum $\mu \in B$. Portanto,

$$c_k = \mu\lambda.$$

Calculando normas em ambos os lados da igualdade acima, segue da multiplicatividade da norma e de $N(1-\zeta) = p$ que

$$c_k^{p-1} = N(c_k) = N(\mu) \cdot N(\lambda) = p \cdot N(\mu).$$

Como $\mu \in B$, que é o anel dos inteiros algébricos de $\mathbb{Q}(\zeta]$, temos que $N(\mu) \in \mathbb{Z}$. Então $p|c_k^{p-1}$ em $\mathbb{Z}$ e, como p é primo, segue que $p \mid c_k$.

□

6 CONCLUSÃO

Ao longo do desenvolvimento deste trabalho nos foi possivel provar que o anel I_L dos inteiros algébricos de um corpo de números L é um domínio de Dedekind. Com isso, ganhamos três propriedades importantes para I_L: ele é noetheriano, integralmente fechado e seus ideais primos diferentes de zero são maximais.

Resultados posteriores mostram que, dado um domínio de Dedekind A, cada ideal fracionário do corpo de frações de A pode ser fatorado unicamente como produto de ideiais. Além disso, o conjunto deste ideais forma um grupo em relação ao produto de ideais.

Outro resultado relevante e interessante que ressaltamos aqui é que, sendo L um corpo de números algébricos, teremos que I_L será um DIP se, e somente se, for um DFU.

Observamos que esta dissertação pode se tornar uma fonte de grande auxílio aos alunos que precisem do resultado principal em si, ou apenas que queiram ter acesso a uma introdução autocontida e elementar dos métodos e resultados da Teorial Algébrica dos Números, os quais não são comumente encontrados em livros textos introdutórios de Álgebra.

Para nós, a confecção dessa dissertação também serviu de porta de entrada a essa bela teoria, assim como incentivo para a consecução de estudos posteriores, mais aprofundados.

REFERÊNCIAS

ASH, R. **Basic Abstract Algebra**. New York: Dover, 2013.

ENDLER, O. **Teoria dos Corpos**. Rio de Janeiro: IMPA, 1972.

GARCIA, A.; LEQUAIN, Y. **Elementos de Álgebra**. Rio de Janeiro: IMPA, 2006.

GONÇALVES, A. **Introdução à Álgebra**. Rio de Janeiro: IMPA, 1979.

TALL, I. S. e D. **Algebraic Number Theory and Fermat's Last Theorem**. New York: Chapman & Hall, 2015.