



Universidade Estadual Paulista

Campus de São José do Rio Preto

Instituto de Biociências, Letras e Ciências Exatas

**Reticulados Ideais via
Corpos Abelianos**

Grasiele Cristiane Jorge

Orientador: Prof. Dr. Antonio Aparecido de Andrade

Dissertação apresentada ao Departamento de Matemática - IBILCE - UNESP, como parte dos requisitos para a obtenção do título de Mestre em Matemática

São José do Rio Preto

Fevereiro - 2008

Banca Examinadora

Antonio Aparecido de Andrade

Professor Doutor - IBILCE - UNESP

Orientador

Henrique Lazari

Professor Doutor - UNESP - Rio Claro

1º Examinador

Tatiana Bertoldi Carlos

Professora Doutora - IBILCE - UNESP

2º Examinador

AGRADECIMENTOS

Ao concluir este trabalho agradeço:

Primeiramente à Deus.

Ao meu orientador, Prof. Dr. Antonio Aparecido de Andrade, pelos conselhos, pela paciência, pela amizade, por me ajudar no conhecimento obtido sempre me indicando o caminho a ser seguido nos momentos de maior dificuldade e por depositar sua confiança em mim diante desse trabalho.

Aos meus pais Claudio Donizetti Jorge (in memorian) e Maria de Lourdes Faioto Jorge que, em meio a tantas dificuldades, sempre me apoiaram e incentivaram a seguir os estudos. E, ao meu irmão Gustavo.

À banca examinadora.

Ao Gil, por ter dividido comigo todos momentos difíceis e felizes desta caminhada.

Aos meus amigos por estarem ao meu lado em todos os momentos.

À Capes, pelo auxílio financeiro, no período de março a agosto de 2006

À FAPESP, pelo auxílio financeiro, no período de setembro de 2006 a fevereiro de 2008

À todos que direta ou indiretamente contribuíram para a realização deste trabalho.

A Matemática, quando a compreendemos bem, possui não somente a verdade, mas também a suprema beleza.

(Bertrand Russel)

Resumo

O objetivo deste trabalho é o estudo de reticulados ideais. Neste estudo enfatizamos o artigo “Lattices and Number Fields” de Eva Bayer-Fluckiger, que apresenta alguns reticulados ideais com as mesmas propriedades que os reticulados A_{p-1} , p primo, D_4 , E_6 , E_8 , K_{12} e Λ_{24} .

Palavras-Chave: Reticulados ideais, diferente, reticulados rotacionados.

Abstract

The aim of this work is the study of ideal lattices. In this study we stress a Eva Bayer-Fluckiger's article "Lattices and Number Fields" with presents some ideal lattices with same properties that lattices A_{p-1} , p prime number, D_4 , E_6 , E_8 , K_{12} e Λ_{24} .

Keywords: Ideal lattices, different, rotated lattices.

Índice de Símbolos

\mathbb{N} : conjunto dos números naturais

\mathbb{Z} : conjunto dos números inteiros

\mathbb{Q} : conjunto dos números racionais

\mathbb{C} : conjunto dos números complexos

\mathbb{R} : conjunto dos números reais

\prod : produtório

\sum : somatório

\bar{x} : conjugado complexo de x

$\#B$: cardinalidade do conjunto B

$A = (a_{ij})$: matriz

$\det(A)$: determinante da matriz A

\mathcal{A} : anel

I, J, P, Q, \dots : ideais

\mathcal{A}/I : anel quociente

$\mathcal{A}[x]$: anel de polinômios com coeficientes em \mathcal{A}

$\text{grau}(f)$: grau do polinômio f

$\text{Ker}(f)$: núcleo da aplicação f

$\text{Im}(f)$: imagem da aplicação f

f' : derivada de f

$\mathbb{K}, \mathbb{L}, \mathbb{M}, \mathbb{F}, \mathbb{E}$: corpos

$[\mathbb{L} : \mathbb{K}]$: grau da extensão $\mathbb{L}|\mathbb{K}$

$\text{Gal}(\mathbb{L}|\mathbb{K})$: grupo de Galois de \mathbb{L} sobre \mathbb{K}

$N_{\mathbb{L}|\mathbb{K}}(\alpha)$: norma do elemento $\alpha \in \mathbb{L}$

$\text{min}_{\mathbb{K}}(\theta)$: polinômio minimal de θ sobre \mathbb{K}

$T_{\mathbb{L}|\mathbb{K}}(\alpha)$: traço do elemento $\alpha \in \mathbb{L}$

$\mathcal{O}_{\mathbb{L}}$: anel de inteiros de \mathbb{L} sobre \mathcal{A}

$D_{\mathbb{L}|\mathbb{K}}(\alpha_1, \dots, \alpha_n)$: discriminante da n -upla $(\alpha_1, \dots, \alpha_n) \in \mathbb{L}$

$D_{\mathbb{L}|\mathbb{K}}$: discriminante da extensão \mathbb{L} sobre \mathbb{K}

$Disc(\mathbb{L}|\mathbb{K})$: discriminante absoluto da extensão \mathbb{L} sobre \mathbb{K}

$N(I)$: norma do ideal I

$S^{-1}\mathcal{A}$: anel de frações de \mathcal{A} com relação a S

$\varphi(n)$: função de Euler aplicada a n

$\phi_n(x)$: n -ésimo polinômio ciclotômico

$\Delta(\mathbb{L}|\mathbb{K})^{-1}$: codiferente da extensão \mathbb{L} sobre \mathbb{K}

$\Delta(\mathbb{L}|\mathbb{K})$: diferente da extensão \mathbb{L} sobre \mathbb{K}

div : diversidade

$d_{p,min}$: distância produto mínima

Sumário

1	Conceitos Preliminares	14
1.1	Anéis e Corpos	14
1.2	Módulos Noetherianos	19
1.3	Extensões de Corpos	24
1.4	Norma e Traço	25
1.5	Anel de Inteiros	28
1.6	Discriminante	37
1.7	Ideais Fracionários	41
1.8	Anéis de Dedekind	43
1.9	Norma de um Ideal	46
1.10	Anéis de Frações	51
2	Corpos Quadráticos e Ciclotômicos	57
2.1	Corpos Quadráticos	57
2.2	Corpos Ciclotômicos	59
3	Codiferente e Diferente	63
3.1	Codiferente	63
3.2	Diferente	70
3.2.1	Definição e Propriedades	70
3.2.2	Diferente e Discriminante	75
4	Ramificação de Ideais	79
4.1	Teorema de Kummer	79
4.2	Ramificação e Discriminante	93
4.3	Ramificação e Diferente	97
4.4	Ramificação em Corpos Ciclotômicos	101

5	Reticulados no \mathbb{R}^n	108
5.1	Definição	108
5.2	Empacotamento Reticulado	114
6	Reticulados Algébricos	117
6.1	Homomorfismo de Minkowski	117
6.2	Homomorfismo Torcido	121
7	Reticulados Ideais	123
7.1	Definição e Propriedades	123
8	Construção de \mathbb{Z}^n-Reticulados Rotacionados via Reticulados Ideais	133
8.1	Reticulados Rotacionados via o Corpo Ciclotômico $\mathbb{Q}(\zeta_p)$	134
8.2	Reticulados Rotacionados via o Corpo Ciclotômico $\mathbb{Q}(\zeta_{2^r})$	139
9	Identificação de certos reticulados com reticulados ideais	147
9.1	Construção	147
9.2	O reticulado A_{p-1} , p primo	150
9.3	O reticulado D_4	151
9.4	O reticulado E_8	153
9.4.1	E_8 via $\mathbb{Q}(\zeta_{24})$	153
9.4.2	E_8 via $\mathbb{Q}(\zeta_{20})$	154
9.4.3	E_8 via $\mathbb{Q}(\zeta_{15})$	155
9.5	O reticulado E_6	156
9.6	O reticulado Coxeter-Todd K_{12}	158
9.7	O reticulado Λ_{24}	159
9.7.1	Λ_{24} via $\mathbb{Q}(\zeta_{39})$	159
9.7.2	Λ_{24} via $\mathbb{Q}(\zeta_{35})$	160
10	Reticulados Ideais Complexos	162
10.1	Definição	162
10.2	Construção Ciclotômica sobre $\mathbb{Q}(\zeta_{2^r})$	167
10.3	Construções Complexas a partir de Construções Reais	171
	Índice Remissivo	175

Introdução

A Teoria Algébrica dos Números é um ramo da matemática que vem despertando o interesse de grandes pesquisadores no decorrer de muitos séculos. Um dos mais famosos problemas de Teoria Algébrica dos Números e que foi recentemente resolvido é conhecido como Teorema de Fermat e diz que não existe solução inteira para a igualdade $x^n + y^n = z^n$ com $n \geq 3$. Em busca de se resolver alguns problemas ligados a números naturais e inteiros como, por exemplo, o Teorema de Fermat, muito se tem progredido nesta área.

Nos últimos anos, a Teoria Algébrica dos Números tem sido a base do estudo de Códigos Corretores de Erros e Reticulados. A Teoria dos Códigos Corretores de Erros propriamente dita foi fundada pelo matemático Claude A. Shannon, por volta de 1940 e, a partir daí, tem tido um enorme crescimento.

Sempre que transmitimos informações há uma possibilidade da mensagem recebida ser diferente da mensagem enviada. Visando recuperar a mensagem enviada ao receptor e construir códigos com pequena probabilidade de ocorrerem erros, fazemos uso da Teoria de Códigos Corretores de Erros e Reticulados.

Graças ao surgimento de códigos e reticulados muito se progrediu na geração de aparelhos transmissores de informações. Inicialmente, a teoria de códigos e reticulados contribuiu para a geração de aparelhos com fio, como televisão e computadores. Mas, atualmente tem contribuído no surgimento de aparelhos sem fio, como por exemplo, celulares. Nas comunicações sem fio muito se tem usado o canal Rayleigh com desvanecimento.

Com esta nova demanda por aparelhos sem fio, utilizamos alguns parâmetros diferentes específicos para a geração de bons códigos e reticulados. Com isto, muito se tem estudado sobre reticulados ideais e reticulados rotacionados.

Quando utilizamos um canal Rayleigh com desvanecimento dois parâmetros relacionados com a probabilidade de erros são a diversidade e a distância produto mínima. Para termos uma transmissão com pequena probabilidade de erros, devemos utilizar códigos com diversidade alta e distância produto mínima alta. Desta forma, sempre que códigos são construídos para este

canal, deve-se maximizar a diversidade e a distância produto mínima. Neste trabalho, veremos que quando consideramos corpos de números totalmente reais temos diversidade máxima e quanto menor for o discriminante do corpo, maior é a sua distância produto mínima.

Neste trabalho, fizemos o estudo de reticulados ideais e suas principais propriedades. Enfatizamos nosso estudo no artigo [16] de Eva Bayer Fluckiger. Vimos alguns reticulados, famosos na literatura, que podem ser vistos como reticulados ideais. Vimos também a construção de \mathbb{Z}^n -reticulados rotacionados, para certos valores de n .

Desta forma, organizamos este trabalho da seguinte forma:

- No Capítulo 1, apresentamos alguns conceitos de módulos e módulos noetherianos, extensões de corpos, norma e traço de um elemento, discriminante de uma extensão, ideais fracionários de um anel, anéis de Dedekind, norma de um ideal fracionário e anéis de frações. Se destaca o fato de que todo ideal fracionário num anel de Dedekind se fatora de forma única como um produto de ideais primos do anel com potências inteiras.
- No Capítulo 2, apresentamos algumas propriedades de corpos quadráticos e ciclotômicos, como anel de inteiros, discriminante e grupo de Galois.
- No Capítulo 3, apresentamos os conceitos de codiferente e diferente de uma extensão. Visto que o diferente será muito utilizado no decorrer dos próximos capítulos, apresentamos algumas de suas propriedades que serão utilizadas no decorrer do trabalho. Em especial, temos que a norma do diferente é o módulo do discriminante da extensão.
- No Capítulo 4, apresentamos um estudo de ramificação de ideais. Dados \mathcal{A} um anel de Dedekind, \mathbb{K} seu corpo de frações, \mathbb{L} uma extensão de \mathbb{K} de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de \mathbb{L} sobre \mathcal{A} , temos que um ideal primo P de \mathcal{A} se ramifica em $\mathcal{O}_{\mathbb{L}}$ se, e somente se, P divide o discriminante da extensão e que um ideal primo Q de $\mathcal{O}_{\mathbb{L}}$ se ramifica em $\mathcal{O}_{\mathbb{L}}$ se, e somente se, Q divide o diferente da extensão. Além disso, apresentamos o Teorema de Kummer que permite encontrar a decomposição de um ideal estendido em um produto de ideais primos. Apresentamos também o estudo de ramificação, discriminante e diferente em corpos ciclotômicos, que serão utilizados nos capítulos finais.
- No Capítulo 5, apresentamos um estudo de reticulados no \mathbb{R}^n , descrevendo as suas principais propriedades.
- No Capítulo 6, apresentamos reticulados algébricos e, neste ponto, temos a ligação entre a teoria de códigos e a teoria dos números.

- No Capítulo 7, apresentamos reticulados ideais e suas principais propriedades.
- No Capítulo 8, apresentamos a construção de \mathbb{Z}^n -reticulados rotacionados via o anel de inteiros algébricos dos subcorpos reais maximais dos corpos $\mathbb{Q}(\zeta_p)$, p primo e $\mathbb{Q}(\zeta_{2^r})$, r inteiro positivo.
- No Capítulo 9, apresentamos a identificação de alguns reticulados, famosos na literatura, tais como, A_{p-1} , com p primo, D_4 , E_6 , E_8 , K_{12} e Λ_{24} , via reticulados ideais.
- No Capítulo 10, apresentamos um estudo de reticulados ideais complexos e duas construções de tais reticulados.

As referências utilizadas foram as seguintes:

- Nos Capítulos 1, 2, 3 e 4, utilizamos as referências [1], [2], [3], [4], [5], [6], [7], [8], [9] [10], [11] e [12].
- Nos Capítulos 5 e 6, utilizamos as referências [3], [13].
- Nos Capítulos 7 e 8, utilizamos as referências [13], [15], [16], [17] e [18].
- No Capítulo 9, utilizamos as referências [19], [20], [22] e [21].
- No Capítulo 10, utilizamos as referências [20] e [23].

Além das referências acima, utilizamos o Programa Mathematica em alguns cálculos, o qual nos poupou grande trabalho.

No decorrer do trabalho, seguem alguns resultados sem demonstração. Alguns por se tratarem de resultados clássicos e outros por apresentarem uma demonstração muito longa. No entanto, sempre que omitimos uma demonstração colocamos a referência onde pode ser encontrada.

Capítulo 1

Conceitos Preliminares

Neste capítulo segue uma série de resultados de teoria algébrica dos números e módulos que serão utilizados como ferramentas no decorrer dos demais capítulos. Na Seção 1.1, apresentamos os conceitos de anéis, corpos, ideais, ideais primos e maximais, Teorema do Isomorfismo de anéis e alguns resultados envolvendo estes conceitos. Na Seção 1.2, apresentamos os conceitos de módulos, submódulos, módulos noetherianos e Teorema do Isomorfismo para módulos. Na Seção 1.3, apresentamos os conceitos de extensões de corpos, CM-corpo, corpo composto e alguns resultados importantes envolvendo estes conceitos. Na Seção 1.4, apresentamos os conceitos de norma e traço de um elemento. Na Seção 1.5, apresentamos os conceitos de elemento inteiro, anel de inteiros e anel integralmente fechado. Na Seção 1.6, apresentamos o conceito de discriminante de uma n -upla e de uma extensão e alguns resultados que facilitam seu cálculo. Na Seção 1.7, apresentamos o conceito de ideais fracionários e algumas de suas propriedades. Na Seção 1.8, apresentamos o conceito de anéis de Dedekind e o resultado de que todo ideal fracionário não nulo num anel de Dedekind se fatora de forma única como produto de ideais primos. Na Seção 1.9, apresentamos a norma de um ideal inteiro e fracionário e algumas de suas propriedades. Na Seção 1.10, apresentamos alguns conceitos sobre anéis de frações e algumas de suas propriedades.

1.1 Anéis e Corpos

Nesta seção, apresentamos algumas definições sobre grupos, anéis, corpos, ideais, ideais primos e maximais e alguns resultados envolvendo estes conceitos que serão utilizados nos próximos capítulos. Alguns resultados seguem sem demonstração por se tratarem de resultados clássicos de álgebra abstrata.

Definição 1.1.1 Dizemos que um conjunto não vazio G é um **grupo** com relação a uma operação $*$ se:

- $a * b \in G$, para todo $a, b \in G$;
- $a * (b * c) = (a * b) * c$, para todo $a, b, c \in G$;
- Existe $e \in G$ tal que $a * e = e * a = a$, para todo $a \in G$;
- Para todo $a \in G$, existe $b \in G$ tal que $a * b = b * a = e$.

Se além disso, $a * b = b * a$, para todo $a, b \in G$, dizemos que G é **abeliano**.

Definição 1.1.2 Dizemos que um conjunto não vazio \mathcal{A} é um **anel** se em \mathcal{A} estão definidas duas operações “+” e “.”, tais que \mathcal{A} é um grupo abeliano com relação a operação “+” e a operação “.” satisfaz:

- $a.(b.c) = (a.b).c$, para todo $a, b, c \in \mathcal{A}$;
- $a.(b + c) = a.b + a.c$ e $(b + c).a = b.a + c.a$, para todo $a, b, c \in \mathcal{A}$.

Se, além disso:

- $a.b = b.a$, para todo $a, b \in \mathcal{A}$, dizemos que \mathcal{A} é um **anel comutativo**;
- existe $1 \in \mathcal{A}$ tal que $a.1 = 1.a = a$, para todo $a \in \mathcal{A}$, dizemos que \mathcal{A} é um **anel com unidade**.

Para simplificarmos a notação faremos $a.b = ab$, para todo $a, b \in \mathcal{A}$.

Definição 1.1.3 Um anel comutativo com unidade \mathcal{A} é chamado de **anel de integridade**, ou **domínio**, se para todo $a, b \in \mathcal{A}$, sempre que $ab = 0$, então $a = 0$ ou $b = 0$.

Definição 1.1.4 Dizemos que um anel de integridade \mathbb{K} é um **corpo**, se para todo elemento não nulo $a \in \mathbb{K}$ existe $b \in \mathbb{K}$ tal que $a.b = 1$.

Definição 1.1.5 Dizemos que um subconjunto não vazio I de um anel \mathcal{A} é um **ideal** de \mathcal{A} se:

- Para todo $x, y \in I$ tem-se $x - y \in I$;
- Para todo $x \in I$ e $a \in \mathcal{A}$ tem-se $ax \in I$.

Definição 1.1.6 *Sejam \mathcal{A} um anel e I, J ideais de \mathcal{A} . Definimos a soma e a multiplicação dos ideais I e J , respectivamente, por:*

- $I + J = \{a + b; a \in I, b \in J\};$
- $IJ = \left\{ \sum_{i=1}^n a_i b_i; a_i \in I, b_i \in J, n \in \mathbb{N}^* \right\}.$

Observação 1.1.1 *Notemos que os conjuntos $I + J$ e IJ definidos acima são ideais de \mathcal{A} e que a soma e a multiplicação de ideais pode ser estendida para um número finito de ideais de \mathcal{A} .*

Definição 1.1.7 *Sejam \mathcal{A} e \mathcal{B} anéis. Uma aplicação $f : \mathcal{A} \longrightarrow \mathcal{B}$ é um homomorfismo de \mathcal{A} em \mathcal{B} se satisfaz:*

- $f(x + y) = f(x) + f(y)$, para todo $x, y \in \mathcal{A}$;
- $f(xy) = f(x)f(y)$, para todo $x, y \in \mathcal{A}$.

Se, além disso, a aplicação f for injetora, dizemos que f é um monomorfismo e se f for bijetora, dizemos que f é um isomorfismo e que \mathcal{A} é isomorfo a \mathcal{B} .

Observação 1.1.2 *Notemos que um isomorfismo de \mathcal{A} em \mathcal{B} preserva todas as propriedades estruturais de \mathcal{A} em \mathcal{B} .*

Proposição 1.1.1 ([1], pags. 147, 148 e 157) *Sejam \mathcal{A} e \mathcal{B} anéis e $f : \mathcal{A} \longrightarrow \mathcal{B}$ um homomorfismo. Temos que:*

(1) - *A imagem de f , $Im(f) = \{f(x); x \in \mathcal{A}\}$, é um subanel de \mathcal{B} .*

(2) - *O núcleo de f , $Ker(f) = \{x \in \mathcal{A}; f(x) = 0\}$, é um ideal de \mathcal{A} , e f é injetora se, e somente se, $Ker(f) = \{0\}$. ■*

Teorema 1.1.1 ([1], pag. 166). **(Teorema do Isomorfismo de Anéis)** *Se \mathcal{A} e \mathcal{B} são anéis e $f : \mathcal{A} \longrightarrow \mathcal{B}$ um homomorfismo, então os anéis $\mathcal{A}/Ker(f)$ e $Im(f)$ são isomorfos, isto é, $\mathcal{A}/Ker(f) \simeq Im(f)$. ■*

Lema 1.1.1 *Se I_1, I_2 são ideais de um anel \mathcal{A} com unidade tal que $I_1 + I_2 = \mathcal{A}$, então $I_1 I_2 = I_1 \cap I_2$.*

Demonstração: Como $I_1 I_2 \subset I_1$ e $I_1 I_2 \subset I_2$, segue que $I_1 I_2 \subset I_1 \cap I_2$. Agora, seja $x \in I_1 \cap I_2$. Por hipótese, como $I_1 + I_2 = \mathcal{A}$, segue que existem elementos $a_1 \in I_1, a_2 \in I_2$ tal que $1 = a_1 + a_2$. Desta forma, $x = a_1 x + a_2 x \in I_1 I_2$. Assim, $I_1 \cap I_2 \subset I_1 I_2$. Logo, $I_1 I_2 = I_1 \cap I_2$. ■

Lema 1.1.2 Se \mathcal{A} é um anel com unidade e $\{I_1, \dots, I_n\}$ é um conjunto finito de ideais de \mathcal{A} , tais que $I_i + I_j = \mathcal{A}$, para todo $i \neq j$, então $\mathcal{A} / \prod_{i=1}^n I_i \simeq \prod_{i=1}^n \mathcal{A} / I_i$.

Demonstração: Faremos a prova por indução sobre n . Para o caso $n = 2$, considere a aplicação:

$$\begin{aligned} \varphi : \mathcal{A} &\longrightarrow \mathcal{A}/I_1 \times \mathcal{A}/I_2 \\ a &\longmapsto (a + I_1, a + I_2). \end{aligned}$$

Temos que φ é um homomorfismo de anéis e $\ker(\varphi) = I_1 \cap I_2$. De fato, $\varphi(x) = (\bar{0}, \bar{0})$ se, e somente se, $(x + I_1, x + I_2) = (\bar{0}, \bar{0})$ se, e somente se, $x + I_1 = \bar{0}$ e $x + I_2 = \bar{0}$ se, e somente se $x \in I_1$ e $x \in I_2$, se e somente se, $x \in I_1 \cap I_2$. Além disso, φ é sobrejetora. De fato, dados $y, z \in \mathcal{A}$, devemos encontrar $x \in \mathcal{A}$ tal que $(y + I_1, z + I_2) = (x + I_1, x + I_2) = \varphi(x)$. Como $I_1 + I_2 = \mathcal{A}$, segue que existem elementos $a_1 \in I_1$, $a_2 \in I_2$ tais que $1 = a_1 + a_2$. Seja $x = a_1 z + a_2 y$. Como $a_2 \equiv 1 \pmod{I_1}$ e $a_1 \equiv 1 \pmod{I_2}$, segue que $x \equiv y \pmod{I_1}$ e $x \equiv z \pmod{I_2}$, isto é, $x + I_1 = y + I_1$ e $x + I_2 = z + I_2$, ou seja, φ é sobrejetora. Portanto, pelo Teorema (1.1.1), segue que

$$\mathcal{A}/I_1 \cap I_2 \simeq \mathcal{A}/I_1 \times \mathcal{A}/I_2.$$

Pelo Lema (1.1.1), segue que $I_1 \cap I_2 = I_1 I_2$. Assim,

$$\mathcal{A}/I_1 I_2 \simeq \mathcal{A}/I_1 \times \mathcal{A}/I_2.$$

Agora, suponha que o resultado vale para $k = n - 1$. Fazendo $B = I_2 \dots I_n$, temos que $I_1 + B = \mathcal{A}$. De fato, como $I_1 + I_i = \mathcal{A}$, para $i \geq 2$, segue que, para todo $i = 2, \dots, n$, existem elementos $e_i \in I_1$ e $a_i \in I_i$ tais que $e_i + a_i = 1$. Logo, $1 = \prod_{i=2}^n (e_i + a_i) = e + a_2 \dots a_n$, onde e é a soma dos termos que contém no mínimo um e_i como fator. Temos que $e \in I_1$. Como $a_2 \dots a_n \in B$, segue que $I_1 + B = \mathcal{A}$. Pelo caso $n = 2$, segue que $\mathcal{A}/I_1 B \simeq \mathcal{A}/I_1 \times \mathcal{A}/B$, e por hipótese de indução, temos que

$$\mathcal{A} / \prod_{i=1}^n I_i \simeq \prod_{i=1}^n \mathcal{A} / I_i,$$

o que prova o lema. ■

Definição 1.1.8 Sejam \mathcal{A} um anel comutativo, $P \neq \mathcal{A}$ e $M \neq \mathcal{A}$ ideais de \mathcal{A} . Dizemos que:

- P é um **ideal primo** de \mathcal{A} , se para todo $x, y \in \mathcal{A}$, sempre que $xy \in P$ implica que $x \in P$ ou $y \in P$;

- M é um ideal maximal de \mathcal{A} , se para todo ideal J de \mathcal{A} tal que $M \subseteq J \subseteq \mathcal{A}$ implica que $M = J$ ou $J = \mathcal{A}$.

Proposição 1.1.2 *Sejam \mathcal{A} um anel comutativo com unidade e $I \subsetneq \mathcal{A}$ um ideal. Temos que:*

- (1) - \mathcal{A}/I é um domínio se, e somente se, I é um ideal primo;
- (2) - \mathcal{A}/I é um corpo se, e somente se, I é um ideal maximal.

Demonstração: (1) - Sejam \mathcal{A}/I um domínio e $a, b \in \mathcal{A}$ tal que $ab \in I$. Temos que $(a + I)(b + I) = ab + I = 0 + I$, pois $ab \in I$. Como \mathcal{A}/I é um domínio, segue que $a + I = 0 + I$ ou $b + I = 0 + I$. Logo, $a \in I$ ou $b \in I$. Portanto, I é um ideal primo. Agora, seja I um ideal primo. Suponha que $(a + I)(b + I) = 0 + I$, para $a, b \in \mathcal{A}$. Como $(a + I)(b + I) = ab + I = 0 + I$, segue que $ab \in I$. Como I é um ideal primo, segue que $a \in I$ ou $b \in I$. Logo, $a + I = 0 + I$ ou $b + I = 0 + I$. Portanto, \mathcal{A}/I é um domínio.

(2) - Seja \mathcal{A}/I um corpo. Suponha que existe um ideal $J \subseteq \mathcal{A}$ tal que $I \subset J \subset \mathcal{A}$. Seja $a \in J - I$. Como $a \notin I$, segue que $a + I \neq 0 + I$. Como \mathcal{A}/I é um corpo e $a + I \neq 0 + I$, segue que existe $b \in \mathcal{A} - I$ tal que $(a + I)(b + I) = 1 + I$. Logo, $(a + I)(b + I) = ab + I = 1 + I$. Desta forma, $ab - 1 \in I$. Como $a \in J$, segue que $ab \in J$ e, assim, $1 \in J$. Portanto, $J = \mathcal{A}$, o que implica que I é maximal. Agora, seja I um ideal maximal. Temos que \mathcal{A}/I é um anel de integridade. Falta mostrar que todo elemento não nulo de \mathcal{A}/I é inversível. Seja $a \in \mathcal{A}$ tal $a + I \neq 0 + I$. Como $a + I \neq 0 + I$, segue que $a \notin I$. Assim, $I \subsetneq I + \langle a \rangle = \mathcal{A}$, pois I é um ideal maximal. Logo, $1 = m + ax$, com $m \in I$ e $x \in \mathcal{A} - I$, $x \neq 0$. Desta forma, como $1 - ax = m \in I$, segue que $1 + I = ax + I = (a + I)(x + I)$. Portanto, $a + I$ é inversível e, desta forma, \mathcal{A}/I é um corpo. ■

Lema 1.1.3 *Sejam \mathcal{A} é um anel e Q, P_1, \dots, P_r ideais primos de \mathcal{A} tais que $Q \not\subseteq P_i$, para todo $i = 1, \dots, r$. Temos que existe um elemento $b \in Q$ tal que $b \notin P_i$, para todo $i = 1, \dots, r$.*

Demonstração: Sem perda de generalidade, podemos considerar o caso em que $P_j \not\subseteq P_i, \forall i \neq j$. Tomemos elementos $x_{ij} \in P_j - P_i$, para $i \neq j, 1 \leq i, j \leq r$, e elementos $a_i \in Q - P_i$. Se $b_i = a_i \prod_{j \neq i} x_{ij}$, então $b_i \in Q$, $b_i \in \mathcal{A} - P_i$ e $b_i \in P_j$ para todo $j \neq i$. Tomando $b = b_1 + \dots + b_r$, temos que $b \in Q$ e $b \equiv b_i \pmod{P_i}$, isto é, $b \notin P_i, \forall i$. Assim, $b \in Q - \bigcup_{i=1}^r P_i$ é o elemento procurado. ■

Proposição 1.1.3 *Se $\mathcal{A} \subseteq \mathcal{B}$ são anéis e $P \subset \mathcal{B}$ um ideal primo, então $P \cap \mathcal{A}$ é um ideal primo de \mathcal{A} .*

Demonstração: Considere a aplicação $\varphi : \mathcal{A} \xrightarrow{i} \mathcal{B} \xrightarrow{\pi} \mathcal{B}/P$, onde i é a inclusão e π é a projeção. A função $\varphi = \pi \circ i$ é um homomorfismo, pois π e i são homomorfismos e $\ker(\varphi) = \mathcal{A} \cap P$, pois $\varphi(x) = (\pi \circ i)(x) = \pi(x) = x + P = \bar{0}$ se, e somente se, $x \in P \cap \mathcal{A}$. Portanto, $\mathcal{A}/(P \cap \mathcal{A}) \simeq \text{Im}(\varphi) \subset \mathcal{B}/P$. Como \mathcal{B}/P é um domínio, segue que $\mathcal{A}/(P \cap \mathcal{A})$ é um domínio. Portanto, pelo Teorema (1.1.2), temos que $P \cap \mathcal{A}$ é um ideal primo de \mathcal{A} . ■

Lema 1.1.4 *Sejam \mathcal{A} um anel e P um ideal primo de \mathcal{A} . Se P contém um produto de ideais I_1, \dots, I_n de \mathcal{A} então P contém pelo menos um dos I_i .*

Demonstração: Se $I_j \not\subset P, \forall j = 1, \dots, n$, então existe $\alpha_j \in I_j$ e $\alpha_j \notin P, \forall j$. Como P é primo, segue que $\alpha_1 \cdots \alpha_n \notin P$. Mas $\alpha_1 \cdots \alpha_n \in I_1 \cdots I_n \subset P$, o que é um absurdo. Portanto, P contém I_j para algum $j = 1, \dots, n$. ■

Definição 1.1.9 *Seja \mathcal{A} um anel. Dizemos que um elemento $a \in \mathcal{A}$ é **nilpotente** se $a^n = 0$, para algum $n \geq 0$. Dizemos que \mathcal{A} é um **anel reduzido** se o único elemento nilpotente de \mathcal{A} é o zero.*

1.2 Módulos Noetherianos

Nesta seção, apresentamos os conceitos de módulos, submódulos e módulos noetherianos juntamente com suas principais propriedades. Alguns resultados seguem sem demonstração por se tratarem de resultados elementares de teoria de módulos.

Definição 1.2.1 *Seja \mathcal{A} um anel comutativo com unidade. Um \mathcal{A} -módulo M é um grupo abeliano aditivo M , munido de uma aplicação $\mathcal{A} \times M \longrightarrow M$, definida por $(a, m) \longmapsto am$, tal que para quaisquer $a, b \in \mathcal{A}$ e $x, y \in M$, tem-se:*

- $a(x + y) = ax + ay$;
- $(a + b)x = ax + bx$;
- $(ab)x = a(bx)$;
- $1x = x$.

Definição 1.2.2 *Sejam \mathcal{A} um anel comutativo com unidade e M um \mathcal{A} -módulo. Um subconjunto $N \subset M$ não vazio é um \mathcal{A} -submódulo de M se, com as operações herdadas de M , N também é um \mathcal{A} -módulo.*

No que segue, consideraremos todo anel \mathcal{A} como sendo um anel comutativo com unidade.

Observação 1.2.1 *Todo anel \mathcal{A} pode ser considerado como um \mathcal{A} -módulo. Basta notarmos que se $M = \mathcal{A}$, então valem todas as condições da Definição (1.2.1).*

Definição 1.2.3 *Um \mathcal{A} -módulo M é dito **finitamente gerado** se existem $x_1, \dots, x_r \in M$ tais que $M = \mathcal{A}x_1 + \dots + \mathcal{A}x_r$, e neste caso, dizemos que $\{x_1, \dots, x_r\}$ formam um sistema de geradores de M . Se além disso, $\{x_1, \dots, x_r\}$ forem linearmente independentes sobre \mathcal{A} , dizemos que eles formam uma **base** de M sobre \mathcal{A} . Um \mathcal{A} -módulo que possui uma base é chamado de **\mathcal{A} -módulo livre**. O número de elementos da base de M é chamado de **posto** de M .*

Observação 1.2.2 *Nem todo módulo finitamente gerado possui uma base. Por exemplo, o anel \mathbb{Z}_2 é um \mathbb{Z} -módulo finitamente gerado mas não é livre, pois $\{\bar{1}\}$ é gerador e $\{\bar{1}\}$ não é linearmente independente.*

Observação 1.2.3 *Nem sempre um \mathcal{A} -submódulo N de um \mathcal{A} -módulo livre M , é livre. Basta tomarmos $M = \mathcal{A} = \mathbb{Z}_6$. Temos que \mathbb{Z}_6 é um \mathbb{Z}_6 -módulo livre com base $\{\bar{1}\}$. Já o \mathbb{Z}_6 -submódulo $N = \{\bar{0}, \bar{2}, \bar{4}\}$ não é livre.*

Teorema 1.2.1 ([3], pag. 21) *Se \mathcal{A} é um anel principal, M um \mathcal{A} -módulo livre de posto n e M' um \mathcal{A} -submódulo de M , então:*

(1)- M' é livre de posto q , $0 \leq q \leq n$.

(2)- Se $M' \neq 0$, então existe uma base $\{e_1, \dots, e_n\}$ de M e elementos não nulos $a_1, \dots, a_q \in \mathcal{A}$ tal que $\{a_1e_1, \dots, a_qe_q\}$ é uma base de M' e a_i divide a_{i+1} , para $i = 1, 2, \dots, q - 1$. ■

Definição 1.2.4 *Sejam \mathcal{A} um anel e N_1, N_2 \mathcal{A} -submódulos de um \mathcal{A} -módulo M . Definimos a **soma** dos módulos N_1 e N_2 como o módulo $N_1 + N_2 = \{a + b \text{ tal que } a \in N_1, b \in N_2\}$.*

Definição 1.2.5 *Sejam \mathcal{A} um anel, M um \mathcal{A} -módulo e N um \mathcal{A} -submódulo de M . Definimos o **módulo quociente** M/N como o \mathcal{A} -módulo $M/N = \{m + N \text{ tal que } m \in M\}$, cujas leis de composição interna “+” e “ \times ” são definidas por $(m_1 + N) + (m_2 + N) = (m_1 + m_2) + N$, para todo $m_1, m_2 \in M$ e $a \times (m + N) = am + N$, para todo $a \in \mathcal{A}$ e $m \in M$, respectivamente.*

Definição 1.2.6 *Sejam \mathcal{A} um anel e M, N dois \mathcal{A} -módulos. Uma aplicação $f : M \rightarrow N$ é dita um **homomorfismo** de \mathcal{A} -módulos se ela satisfaz:*

- $f(x + y) = f(x) + f(y)$, $\forall x, y \in M$;

- $f(ay) = af(y), \forall y \in M, a \in \mathcal{A}$.

Se, além disso, a aplicação f for injetora, dizemos que f é um **monomorfismo** e se f for bijetora, dizemos que f é um **isomorfismo** e que \mathcal{A} é isomorfo a \mathcal{B} .

Proposição 1.2.1 ([2], pag. 29) *Sejam \mathcal{A} um anel, M, N dois \mathcal{A} -módulos e $f : M \longrightarrow N$ um homomorfismo. Temos que:*

(1) - *A imagem de f , $Im(f) = \{f(x); x \in M\}$, é um submódulo de N .*

(2) - *O núcleo de f , $Ker(f) = \{x \in M; f(x) = 0\}$, é um submódulo de M , e f é injetora se, e somente se, $Ker(f) = \{0\}$.* ■

Teorema 1.2.2 ([2], pag. 32) (**Teorema do Isomorfismo de Módulos**) *Se \mathcal{A} é um anel, M, N dois \mathcal{A} -módulos e $f : M \longrightarrow N$ um homomorfismo, então os módulos $M/Ker(f)$ e $Im(f)$ são isomorfos, isto é, $M/Ker(f) \simeq Im(f)$.* ■

Definição 1.2.7 *Sejam \mathcal{A} um anel e M um \mathcal{A} -módulo. Dizemos que M é um **\mathcal{A} -módulo noetheriano** se M satisfaz uma das seguintes condições equivalentes:*

- *Toda família não vazia de \mathcal{A} -submódulos de M tem um elemento maximal;*
- *Toda sequência crescente de \mathcal{A} -submódulos de M é estacionária;*
- *Todo \mathcal{A} -submódulo de M é finitamente gerado.*

*Dizemos que \mathcal{A} é um **anel noetheriano** se \mathcal{A} considerado como um \mathcal{A} -módulo for noetheriano.*

Proposição 1.2.2 *Todo anel principal \mathcal{A} é noetheriano.*

Demonstração: Temos que os \mathcal{A} -submódulos de \mathcal{A} são exatamente os ideais de \mathcal{A} . Como \mathcal{A} é um anel principal, segue que os ideais de \mathcal{A} são principais. Logo, finitamente gerados. Portanto, \mathcal{A} é noetheriano. ■

Proposição 1.2.3 *Sejam \mathcal{A} um anel, M um \mathcal{A} -módulo e N um \mathcal{A} -submódulo de M . Temos que M é noetheriano se, e somente se, $\frac{M}{N}$ e N são noetherianos.*

Demonstração: Suponha que M é noetheriano. Se $(M_n)_{n \geq 0}$ é uma sequência crescente de \mathcal{A} -submódulos de N , então $(M_n)_{n \geq 0}$ também é uma sequência crescente de \mathcal{A} -submódulos de M . Como M é noetheriano, segue que $(M_n)_{n \geq 0}$ é estacionária. Portanto, N é noetheriano. Para mostrar que $\frac{M}{N}$ é noetheriano, sejam $S = \{ \text{submódulos de } M \text{ que contém } N \}$ e $T =$

$\{ \text{submódulos de } \frac{M}{N} \}$. A aplicação $\varphi : S \longrightarrow T$ definida por $\varphi(L) = \frac{L}{N}$, para $L \in S$, é uma bijeção de S em T . Assim, se $(M_n)_{n \geq 0}$ é uma seqüência crescente de \mathcal{A} -submódulos de $\frac{M}{N}$, então $(\varphi^{-1}(M_n))_{n \geq 0}$ também é uma seqüência crescente de \mathcal{A} -submódulos de M . Como M é noetheriano, segue que $(\varphi^{-1}(M_n))_{n \geq 0}$ é estacionária, e portanto $(M_n)_{n \geq 0}$ é estacionária. Assim, $\frac{M}{N}$ é noetheriano. Reciprocamente, suponhamos que $\frac{M}{N}$ e N são noetherianos. Seja $(M_n)_{n \geq 0}$ uma seqüência crescente de \mathcal{A} -submódulos de M . Assim, $(N \cap M_n)_{n \geq 0}$ é uma seqüência crescente de \mathcal{A} -submódulos N . Como N é noetheriano, segue que $(M_n \cap N)_{n \geq 0}$ é estacionária, ou seja, existe $n_1 \in \mathbb{N}$ tal que $M_n \cap N = M_{n+1} \cap N, \forall n \geq n_1$. Agora, $\left(\frac{M_n + N}{N} \right)_{n \geq 0}$ é uma seqüência crescente de \mathcal{A} -submódulos de $\frac{M}{N}$. Logo, existe $n_2 \in \mathbb{N}$ tal que $\frac{M_n + N}{N} = \frac{M_{n+1} + N}{N}, \forall n \geq n_2$. Tomando $n_0 = \max\{n_1, n_2\}$, temos que

$$M_n \cap N = M_{n+1} \cap N \quad \text{e} \quad \frac{M_n + N}{N} = \frac{M_{n+1} + N}{N}, \quad \forall n \geq n_0.$$

Como $M_n \subseteq M_{n+1}, \forall n$, resta mostrar que existe $k \in \mathbb{N}$ tal que $M_{n+1} \subseteq M_n, \forall n \geq k$. Seja $x \in M_{n+1}$, para algum $n \geq n_0$. Como $\frac{M_n + N}{N} = \frac{M_{n+1} + N}{N}, \forall n \geq n_0$, existe $y \in M_n$ e $w \in N$ tal que $x + N = (y + w) + N$, o que implica que $x - y - w \in N$. Assim, existe $a \in N$ tal que $x - y - w = a$ e assim $x - y = a + w \in N$. Como $x - y \in M_{n+1}$, então $x - y \in N \cap M_{n+1} = N \cap M_n$. Desta forma, $x - y \in M_n$ e, assim, $x \in M_n$. Portanto, $M_n = M_{n+1}, \forall n \geq n_0$. Tomando $k = n_0$, temos que $M_n = M_{n+1}$, para todo $n \geq k$. Logo, N é noetheriano. ■

Corolário 1.2.1 *Se M_1, \dots, M_n são \mathcal{A} -módulos noetherianos então o produto $M_1 \times \dots \times M_n$ é um \mathcal{A} -módulo noetheriano.*

Demonstração: Faremos a prova por indução sobre n . Para $n = 2$, identificamos $M_1 \simeq M_1 \times \{0\} \subseteq M_1 \times M_2$ e definimos a função $\varphi : M_1 \times M_2 \longrightarrow M_2$ tal que $\varphi(x, y) = y$. Como φ é um homomorfismo sobrejetor, segue que $\frac{M_1 \times M_2}{\text{Ker}(\varphi)} \simeq M_2$, onde $\text{Ker}(\varphi) = M_1 \times \{0\}$. Como M_2 é noetheriano, segue que $\frac{M_1 \times M_2}{M_1 \times \{0\}} \simeq M_2$ é noetheriano e como $M_1 \times \{0\}$ é noetheriano, segue da Proposição (1.2.3), que $M_1 \times M_2$ é noetheriano. Suponhamos agora, por hipótese de indução, que $M = M_1 \times \dots \times M_{n-1}$ é noetheriano. Como M_n é noetheriano, segue do caso $n = 2$, que $M = M_1 \times \dots \times M_n$ é um \mathcal{A} -módulo noetheriano. ■

Corolário 1.2.2 *Se \mathcal{A} é um anel noetheriano e M é um \mathcal{A} -módulo finitamente gerado, então M é um \mathcal{A} -módulo noetheriano.*

Demonstração: Seja $\{e_1, \dots, e_n\}$ um conjunto de geradores do \mathcal{A} -módulo M . Temos que a aplicação

$$\varphi : \mathcal{A}^n \longrightarrow M$$

$$(a_1, \dots, a_n) \longmapsto a_1e_1 + \dots + a_ne_n,$$

é um homomorfismo sobrejetor. Assim, pelo Teorema (1.1.1), temos que $\frac{\mathcal{A}^n}{\text{Ker}(\varphi)} \simeq M$. Como

\mathcal{A} é noetheriano, pelo Corolário (1.2.1), segue que \mathcal{A}^n é noetheriano. Pela Proposição (1.2.3), temos que $\frac{\mathcal{A}^n}{\text{Ker}(\varphi)}$ é noetheriano. Portanto, segue que M é um \mathcal{A} -módulo noetheriano. ■

Proposição 1.2.4 *Em um anel noetheriano \mathcal{A} todo ideal contém um produto de ideais primos.*

Demonstração: Sejam \mathcal{A} um anel noetheriano e F o conjunto dos ideais de \mathcal{A} que não contém um produto de ideais primos. Suponhamos $F \neq \emptyset$. Como \mathcal{A} é noetheriano, segue que F tem um elemento maximal M . Temos que M não é um ideal primo, senão $M \notin F$. Assim, existem $x, y \in \mathcal{A} - M$ tal que $xy \in M$. Notemos que $M \subsetneq \langle x \rangle + M$ e $M \subsetneq \langle y \rangle + M$. Logo, $\langle x \rangle + M$ e $\langle y \rangle + M$ não pertencem a F . Assim, existem $P_1, \dots, P_n, Q_1, \dots, Q_s$ ideais primos de \mathcal{A} tais que

$$P_1P_2 \dots P_n \subseteq \langle x \rangle + M \quad \text{e} \quad Q_1Q_2 \dots Q_s \subseteq \langle y \rangle + M.$$

Desta forma,

$$(P_1P_2 \dots P_n)(Q_1Q_2 \dots Q_s) \subseteq (\langle x \rangle + M)(\langle y \rangle + M) \subseteq M,$$

o que é um absurdo. Portanto, $F = \emptyset$. ■

Corolário 1.2.3 *Em um anel noetheriano todo ideal não nulo contém um produto de ideais primos não nulos.*

Demonstração: Análoga a Proposição (1.2.4). ■

Corolário 1.2.4 *Se \mathcal{A} é um anel noetheriano reduzido, então o ideal nulo de \mathcal{A} é uma intersecção finita de ideais primos não nulos distintos de \mathcal{A} .*

Demonstração: Pela Proposição (1.2.4), temos que o ideal nulo de um anel noetheriano contém um produto de ideais primos. Portanto, $\langle 0 \rangle = \prod_{i=1}^g P_i^{e_i}$, $e_i \geq 1$. Vamos mostrar que

$\langle 0 \rangle = \bigcap_{i=1}^g P_i$. Temos que $\langle 0 \rangle \subseteq P_1 \cap \dots \cap P_g$. Por outro lado, se $x \in P_1 \cap \dots \cap P_g$, então

$x^{e_1+e_2+\dots+e_g} \in P_1^{e_1} \dots P_g^{e_g} = \langle 0 \rangle$. Como \mathcal{A} é reduzido, segue que $x = 0$. Portanto, $\langle 0 \rangle = \bigcap_{i=1}^g P_i$. ■

1.3 Extensões de Corpos

Nesta seção, apresentamos os conceitos de extensões de corpos, CM-corpos, corpos compostos e alguns resultados importantes como a multiplicidade dos graus e o Teorema do Elemento Primitivo. Omitimos a demonstração de todos os resultados por se tratarem de fatos conhecidos de teoria de Galois.

Definição 1.3.1 *Sejam \mathbb{K}, \mathbb{L} corpos. Dizemos que \mathbb{L} é uma **extensão** de \mathbb{K} se $\mathbb{K} \subset \mathbb{L}$.*

Observação 1.3.1 *Seja $\mathbb{K} \subset \mathbb{L}$ uma extensão de corpos. É fácil verificar que \mathbb{L} é um \mathbb{K} -espaço vetorial. Assim, existe uma base de \mathbb{L} sobre \mathbb{K} .*

Definição 1.3.2 *Seja $\mathbb{K} \subset \mathbb{L}$ uma extensão de corpos. A dimensão do \mathbb{K} -espaço vetorial \mathbb{L} é chamada de **grau da extensão** e denotada por $[\mathbb{L} : \mathbb{K}]$.*

Teorema 1.3.1 ([3], pag. 31) *Se $\mathbb{F} \subset \mathbb{K} \subset \mathbb{L}$ são corpos, então $[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}]$. ■*

Definição 1.3.3 *Sejam $\mathbb{K} \subset \mathbb{L}$ corpos. Um elemento $\alpha \in \mathbb{L}$ é chamado de **algébrico** sobre \mathbb{K} se existe $f(x) \in \mathbb{K}[x] - \{0\}$ tal que $f(\alpha) = 0$. O polinômio mônico de menor grau $f(x)$ tal que $f(\alpha) = 0$ é chamado de **polinômio minimal** de α sobre \mathbb{K} e é denotado por $\min_{\mathbb{K}}\alpha$.*

Definição 1.3.4 *Um **corpo de números** \mathbb{K} é uma extensão finita de \mathbb{Q} .*

Teorema 1.3.2 ([4], pag. 40) *Se \mathbb{K} é um corpo de números, então existe $\theta \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$. O elemento θ é chamado **elemento primitivo**. ■*

Proposição 1.3.1 ([4], pag. 23) *Se \mathbb{K} é um corpo de números tal que $\mathbb{K} = \mathbb{Q}(\theta)$, então $[\mathbb{K} : \mathbb{Q}] = \text{grau}(\min_{\mathbb{Q}}\theta)$. ■*

Teorema 1.3.3 ([4], pag. 41) *Se $\mathbb{K} = \mathbb{Q}(\theta)$ é uma extensão de \mathbb{Q} de grau n , então existem exatamente n homomorfismos $\{\sigma_1, \dots, \sigma_n\}$ de \mathbb{K} em \mathbb{C} . Tais homomorfismos são dados por $\sigma_i(\theta) = \theta_i$, onde $\{\theta_1, \dots, \theta_n\}$ são as raízes de $\min_{\mathbb{Q}}\theta$ em \mathbb{C} . ■*

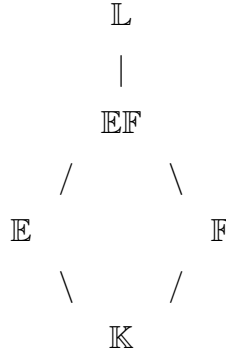
Definição 1.3.5 *Seja \mathbb{K} um corpo de números de grau n e $\{\sigma_1, \dots, \sigma_n\}$ os n \mathbb{Q} -homomorfismos distintos de \mathbb{K} em \mathbb{C} . Dizemos que o homomorfismo σ_i é **real** se $\sigma_i(\mathbb{K}) \subset \mathbb{R}$, caso contrário, dizemos que σ_i é **imaginário**. Além disso, se todos os σ_i 's, para $i = 1, \dots, n$, forem reais, dizemos que o corpo \mathbb{K} é **totalmente real** e, se todos os σ_i 's, para $i = 1, \dots, n$, forem imaginários, dizemos que \mathbb{K} é **totalmente imaginário**.*

Definição 1.3.6 Um corpo de números \mathbb{K} é chamado de **CM-corpo** se existe um corpo de números totalmente real \mathbb{F} tal que \mathbb{K} é uma extensão quadrática totalmente imaginária de \mathbb{F}

Observação 1.3.2 ([20], pag. 14) Se \mathbb{K} é um CM-corpo, então a conjugação complexa comuta com todos os \mathbb{Q} -homomorfismos $\{\sigma_1, \dots, \sigma_n\}$ de \mathbb{K} em \mathbb{C} . ■

Definição 1.3.7 Sejam $\mathbb{K} \subset \mathbb{L}$ corpos. Dizemos que $\mathbb{L}|\mathbb{K}$ é uma **extensão de Galois** se existe $f(x) \in \mathbb{K}[x]$ tal que $\mathbb{L} = \mathbb{K}(R_f)$, onde R_f denota as raízes de f .

Definição 1.3.8 Sejam \mathbb{E}, \mathbb{F} extensões de um corpo \mathbb{K} . Se \mathbb{E} e \mathbb{F} estão contidas em algum corpo \mathbb{L} , então denotamos por \mathbb{EF} o menor subcorpo de \mathbb{L} contendo \mathbb{E} e \mathbb{F} . Chamamos o corpo \mathbb{EF} de **composto** de \mathbb{E} e \mathbb{F} em \mathbb{L} .



Teorema 1.3.4 ([9], pag. 196) Se \mathbb{E} é uma extensão de Galois finita de \mathbb{K} e \mathbb{F} é uma extensão de \mathbb{K} tal que \mathbb{E}, \mathbb{F} são subcorpos de um corpo \mathbb{L} , então \mathbb{EF} é uma extensão de Galois de \mathbb{F} e \mathbb{E} é uma extensão de Galois de $\mathbb{E} \cap \mathbb{F}$. Além disso, $\phi : Gal(\mathbb{EF}|\mathbb{F}) \longrightarrow Gal(\mathbb{E}|\mathbb{E} \cap \mathbb{F})$, onde $\phi(\sigma) = \sigma|_{\mathbb{E}}$ é um isomorfismo. ■

1.4 Norma e Traço

Nesta seção, apresentamos os conceitos de norma e traço de um elemento. Iremos trabalhar com anéis \mathcal{A} e \mathcal{B} tais que $\mathcal{A} \subset \mathcal{B}$ e \mathcal{B} é um \mathcal{A} -módulo livre de posto n . Em particular, podemos tomar \mathcal{A}, \mathcal{B} corpos tal que \mathcal{B} é uma extensão de grau n de \mathcal{A} .

Sejam $\mathcal{A} \subseteq \mathcal{B}$ anéis tal que \mathcal{B} é um \mathcal{A} -módulo livre de posto finito n e $\{e_1, \dots, e_n\}$ uma base de \mathcal{B} sobre \mathcal{A} .

Considere o endomorfismo $\sigma_\alpha : \mathcal{B} \longrightarrow \mathcal{B}$, definido por $\sigma_\alpha(x) = \alpha x$, onde $\alpha \in \mathcal{B}$. Temos que

$$\begin{aligned}\sigma_\alpha(e_1) &= a_{11}e_1 + a_{21}e_2 + \cdots + a_{n1}e_n \\ \sigma_\alpha(e_2) &= a_{12}e_1 + a_{22}e_2 + \cdots + a_{n2}e_n \\ &\vdots \\ \sigma_\alpha(e_n) &= a_{1n}e_1 + a_{2n}e_2 + \cdots + a_{nn}e_n,\end{aligned}$$

com $a_{ij} \in \mathcal{A}$, onde $1 \leq i, j \leq n$.

Definição 1.4.1 Definimos o **traço** de $\alpha \in \mathcal{B}$ por $Tr_{\mathcal{B}|\mathcal{A}}(\alpha) = \sum_{i=1}^n a_{ii}$, a **norma** de α por $N_{\mathcal{B}|\mathcal{A}}(\alpha) = \det(a_{ij})$ e o **polinômio característico** de α por $m_{\mathcal{B}|\mathcal{A}}(x) = \det(xI - (a_{ij}))$.

Vale ressaltar que quando não houver dúvidas a respeito dos anéis com os quais estamos trabalhando, denotaremos $Tr_{\mathcal{B}|\mathcal{A}}$, $N_{\mathcal{B}|\mathcal{A}}$ e $m_{\mathcal{B}|\mathcal{A}}(x)$ simplesmente por Tr , N e $m(x)$.

Sejam $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L}$ corpos, onde $\mathbb{K} \subseteq \mathbb{L}$ é uma extensão finita. Se $\alpha, \alpha' \in \mathbb{L}$ e $a \in \mathbb{K}$, então valem as seguintes propriedades:

- (1)- $Tr_{\mathbb{L}|\mathbb{K}}(\alpha + \alpha') = Tr_{\mathbb{L}|\mathbb{K}}(\alpha) + Tr_{\mathbb{L}|\mathbb{K}}(\alpha')$;
- (2)- $Tr_{\mathbb{L}|\mathbb{K}}(a\alpha) = aTr_{\mathbb{L}|\mathbb{K}}(\alpha)$;
- (3)- $Tr_{\mathbb{L}|\mathbb{K}}(a) = [\mathbb{L} : \mathbb{K}]a$;
- (4)- $N_{\mathbb{L}|\mathbb{K}}(a) = a^{[\mathbb{L}:\mathbb{K}]}$;
- (5)- $N_{\mathbb{L}|\mathbb{K}}(a\alpha) = a^{[\mathbb{L}:\mathbb{K}]}N_{\mathbb{L}|\mathbb{K}}(\alpha)$;
- (6)- $N_{\mathbb{L}|\mathbb{K}}(\alpha\alpha') = N_{\mathbb{L}|\mathbb{K}}(\alpha)N_{\mathbb{L}|\mathbb{K}}(\alpha')$.

Proposição 1.4.1 ([6], pag. 23) Sejam $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ corpos. Temos que:

- (1)- $N_{\mathbb{L}|\mathbb{K}}(\alpha) = N_{\mathbb{M}|\mathbb{K}}(N_{\mathbb{L}|\mathbb{M}}(\alpha))$;
- (2)- $T_{\mathbb{L}|\mathbb{K}}(\alpha) = T_{\mathbb{M}|\mathbb{K}}(T_{\mathbb{L}|\mathbb{M}}(\alpha))$. ■

Proposição 1.4.2 Se \mathbb{K} é um corpo de números, \mathbb{L} uma extensão de \mathbb{K} de grau n , α um elemento de \mathbb{L} e $\alpha_1, \dots, \alpha_n$ as raízes do polinômio minimal de α sobre \mathbb{K} , então $Tr(\alpha) = \alpha_1 + \cdots + \alpha_n$, $N(\alpha) = \alpha_1 \dots \alpha_n$ e $m(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$.

Demonstração: Primeiro faremos a demonstração para o caso em que α é um elemento primitivo de \mathbb{L} sobre \mathbb{K} , ou seja, $\mathbb{L} = \mathbb{K}[\alpha]$. Se $f(x) = x^n + \cdots + a_1x + a_0$ é o polinômio minimal de α sobre \mathbb{K} , então $\{1, \alpha, \dots, \alpha^{n-1}\}$ é uma base de \mathbb{L} sobre \mathbb{K} . Temos que

a matriz do endomorfismo σ_α com respeito a esta base é dada por

$$M = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}.$$

Assim, $\det(xI - M)$ é o determinante da matriz

$$xI_n - M = \begin{bmatrix} x & 0 & \cdots & 0 & a_0 \\ -1 & x & \cdots & 0 & a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & x + a_{n-1} \end{bmatrix}. \quad (1.1)$$

Calculando o determinante da matriz (1.1), obtemos o polinômio característico em α , que é igual a $f(x)$, o polinômio minimal de α . Sabemos que,

$$m(x) = \det(xI_n - M) = x^n - (\text{Tr}(\alpha))x^{n-1} + \cdots + (-1)^n \det(M).$$

Como α é primitivo, segue que

$$m(x) = f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) = x^n - \left(\sum_{i=1}^n \alpha_i \right) x^{n-1} + \cdots + (-1)^n \left(\prod_{i=1}^n \alpha_i \right).$$

Logo, $\text{Tr}(\alpha) = \sum_{i=1}^n \alpha_i$ e $N(\alpha) = \prod_{i=1}^n \alpha_i$. Para o caso geral, seja $r = [\mathbb{L} : \mathbb{K}[\alpha]]$. É suficiente mostrar que o polinômio característico $m(x)$ de α , com relação a \mathbb{L} sobre \mathbb{K} , é igual a r -ésima potência do polinômio minimal de α sobre \mathbb{K} . Seja $\{y_1, \dots, y_q\}$ uma base de $\mathbb{K}[\alpha]$ sobre \mathbb{K} e seja $\{z_1, \dots, z_r\}$ uma base de \mathbb{L} sobre $\mathbb{K}[\alpha]$ com $n = qr$. Seja $M = (a_{ih})$ a matriz do endomorfismo de $\mathbb{K}[\alpha]$ sobre \mathbb{K} com relação a base $\{y_1, \dots, y_q\}$. Assim, $\alpha y_i = \sum_{h=1}^q (a_{ih}) y_h$ e

Definição 1.5.1 *Sejam $\mathcal{A} \subset \mathcal{B}$ anéis. Dizemos que um elemento $\alpha \in \mathcal{B}$ é **inteiro** sobre \mathcal{A} , se α é raiz de um polinômio mônico com coeficientes em \mathcal{A} , ou seja, existem $a_0, \dots, a_{n-1} \in \mathcal{A}$, não todos nulos, tal que*

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

*Essa equação é chamada de **equação de dependência integral** de α .*

Teorema 1.5.1 *Sejam $\mathcal{A} \subseteq \mathcal{B}$ anéis e $\alpha \in \mathcal{B}$. São equivalentes as seguintes afirmações:*

- (1)- α é inteiro sobre \mathcal{A} ;
- (2)- O anel $\mathcal{A}[\alpha]$ é um \mathcal{A} -módulo finitamente gerado;
- (3)- Existe um subanel R do anel \mathcal{B} tal que R é um \mathcal{A} -módulo finitamente gerado que contém \mathcal{A} e α .

Demonstração: (1) \Rightarrow (2) Temos que $\mathcal{A}[\alpha] = \{\sum_i a_i \alpha^i; a_i \in \mathcal{A}\}$. Por hipótese, temos que α é inteiro sobre \mathcal{A} , assim existem $a_0, \dots, a_{n-1} \in \mathcal{A}$, não todos nulos, tal que

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

Seja $M = \langle 1, \alpha, \dots, \alpha^{n-1} \rangle$ um \mathcal{A} -módulo finitamente gerado. Vamos mostrar que $\mathcal{A}[\alpha] = M$. Temos que $\alpha^n = -(a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0)$, ou seja, $\alpha^n \in \langle 1, \alpha, \dots, \alpha^{n-1} \rangle$. Vamos provar por indução que $\alpha^j \in M$, para $j \in \mathbb{N}$. Temos que $\alpha^j \in M, \forall j \leq n$. Suponhamos por hipótese de indução que $\alpha^j \in \langle 1, \alpha, \dots, \alpha^{n-1} \rangle$ e mostremos que $\alpha^{j+1} \in \langle 1, \alpha, \dots, \alpha^{n-1} \rangle$. Por hipótese de indução existem $b_0, \dots, b_{n-1} \in \mathcal{A}$ tal que $\alpha^j = b_{n-1}\alpha^{n-1} + \dots + b_1\alpha + b_0$. Assim,

$$\begin{aligned} \alpha^{j+1} &= \alpha^j \alpha \\ &= (b_{n-1}\alpha^{n-1} + \dots + b_1\alpha + b_0)\alpha \\ &= b_{n-1}\alpha^n + \dots + b_1\alpha^2 + b_0\alpha \\ &= b_{n-1}(-a_{n-1}\alpha^{n-1} - \dots - a_1\alpha - a_0) + \dots + b_1\alpha^2 + b_0\alpha \\ &= -a_0b_{n-1} + (-b_{n-1}a_1 + b_0)\alpha + \dots + (b_{n-2} - b_{n-1}a_{n-1})\alpha^{n-1}, \end{aligned}$$

ou seja, $\alpha^j \in M$, para $j \in \mathbb{N}$. Por outro lado, $\langle 1, \alpha, \dots, \alpha^{n-1} \rangle \subset \mathcal{A}[\alpha]$. Assim, $\langle 1, \alpha, \dots, \alpha^{n-1} \rangle = \mathcal{A}[\alpha]$. Portanto, $\mathcal{A}[\alpha]$ é um \mathcal{A} -módulo gerado por $1, \alpha, \dots, \alpha^{n-1}$.

(2) \Rightarrow (3) Como $\alpha \in \mathcal{A}[\alpha]$ e $\mathcal{A} \subset \mathcal{A}[\alpha]$, é suficiente tomar $R = \mathcal{A}[\alpha]$.

(3) \Rightarrow (1) Seja $R = \langle y_1, \dots, y_n \rangle$ um \mathcal{A} -módulo finitamente gerado tal que $\mathcal{A} \subset R \subset \mathcal{B}$ e $\alpha \in R$, ou seja, $R = \mathcal{A}y_1 + \dots + \mathcal{A}y_n$. Como $\alpha \in R$ segue que $\alpha y_i \in R$, para $i = 1, \dots, n$. Assim,

existem $a_{ij} \in \mathcal{A}$, com $1 \leq i, j \leq n$, de modo que

$$\begin{cases} \alpha y_1 = a_{11}y_1 + \cdots + a_{1n}y_n \\ \alpha y_2 = a_{21}y_1 + \cdots + a_{2n}y_n \\ \vdots \\ \alpha y_n = a_{n1}y_1 + \cdots + a_{nn}y_n. \end{cases}$$

Logo,

$$\begin{cases} (\alpha - a_{11})y_1 - a_{12}y_2 - \cdots - a_{1n}y_n = 0 \\ -a_{12}y_1 + (\alpha - a_{22})y_2 - \cdots - a_{2n}y_n = 0 \\ \vdots \\ -a_{n1}y_1 - a_{n2}y_2 - \cdots + (\alpha - a_{nn})y_n = 0. \end{cases}$$

Na forma matricial, temos

$$\begin{bmatrix} (\alpha - a_{11}) & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & (\alpha - a_{22}) & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & \cdots & \cdots & (\alpha - a_{nn}) \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}. \quad (1.2)$$

Seja D o determinante da matriz dos coeficientes do sistema linear (1.2). Pela regra de Cramer, temos que $Dy_j = 0$, para $j = 1, \dots, n$. Como $1 \in R$, segue que $1 = \sum_{j=1}^n e_j y_j$, com

$e_j \in \mathcal{A}$, e assim, $D = D1 = D \sum_{j=1}^n e_j y_j = \sum_{j=1}^n e_j Dy_j = 0$. Observemos que D é uma equação de dependência integral de α uma vez que $D = \alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_0 = 0$, onde cada $b_i \in \mathcal{A}$. Portanto, α é inteiro sobre \mathcal{A} . ■

Corolário 1.5.1 *Sejam $\mathcal{A} \subseteq \mathcal{B}$ anéis e $\alpha_1, \dots, \alpha_n \in \mathcal{B}$. Se α_1 é inteiro sobre \mathcal{A} , α_2 é inteiro sobre $\mathcal{A}[\alpha_1]$, ..., e α_n é inteiro sobre $\mathcal{A}[\alpha_1, \dots, \alpha_{n-1}]$, então $\mathcal{A}[\alpha_1, \dots, \alpha_n]$ é um \mathcal{A} -módulo finitamente gerado.*

Demonstração: Vamos provar por indução sobre n . Se α_1 é inteiro sobre \mathcal{A} , então pelo Teorema (1.5.1), temos que $\mathcal{A}[\alpha_1]$ é um \mathcal{A} -módulo finitamente gerado. Agora, suponhamos que $R = \mathcal{A}[\alpha_1, \dots, \alpha_{n-1}]$ seja um \mathcal{A} -módulo finitamente gerado por $\{v_1, v_2, \dots, v_t\}$ e que α_n seja inteiro sobre $R = \mathcal{A}[\alpha_1, \dots, \alpha_{n-1}]$. Como R é um anel e $R \subset \mathcal{B}$, pelo Teorema (1.5.1), temos

que $R[\alpha_n]$ é um R -módulo finitamente gerado. Assim existe $\{w_1, \dots, w_s\} \subset R[\alpha_n]$ tal que

$$\mathcal{A}[\alpha_1, \dots, \alpha_n] = R[\alpha_n] = \sum_{i=1}^s R w_i.$$

Como $R = \sum_{j=1}^t \mathcal{A} v_j$, segue que

$$\mathcal{A}[\alpha_1, \dots, \alpha_n] = R[\alpha_n] = \sum_{i=1}^s \left(\sum_{j=1}^t \mathcal{A} v_j \right) w_i = \sum_{j,i} \mathcal{A} v_j w_i.$$

Logo, $\{v_j w_i \text{ para } i = 1, \dots, s \text{ e } j = 1, \dots, t\}$ gera $R[\alpha_n]$ como um \mathcal{A} -módulo. Portanto, $\mathcal{A}[\alpha_1, \dots, \alpha_n]$ é um \mathcal{A} -módulo finitamente gerado. ■

Corolário 1.5.2 *Sejam $\mathcal{A} \subseteq \mathcal{B}$ anéis. Se $\alpha, \beta \in \mathcal{B}$ são inteiros sobre \mathcal{A} , então $\alpha \pm \beta$ e $\alpha\beta$ são inteiros sobre \mathcal{A} .*

Demonstração: Temos que $\alpha \pm \beta, \alpha\beta \in \mathcal{A}[\alpha, \beta]$. Pelo Corolário (1.5.1), como α é inteiro sobre \mathcal{A} , segue que $\mathcal{A}[\alpha]$ é um \mathcal{A} -módulo finitamente gerado e como β é inteiro sobre $\mathcal{A}[\alpha]$, segue que $\mathcal{A}[\alpha, \beta]$ é um \mathcal{A} -módulo finitamente gerado. Seja o anel $R = \mathcal{A}[\alpha, \beta]$. Temos que R é um \mathcal{A} -módulo finitamente gerado, que $\mathcal{A} \subset R$ e que $\alpha \pm \beta, \alpha\beta \in R$. Assim, pelo item (iii) do Teorema (1.5.1), temos que $\alpha \pm \beta, \alpha\beta$ são inteiros sobre \mathcal{A} . ■

Corolário 1.5.3 *Se $\mathcal{A} \subset \mathcal{B}$ são anéis e $\mathcal{O}_{\mathcal{B}} = \{\alpha \in \mathcal{B}; \alpha \text{ é inteiro sobre } \mathcal{A}\}$, então $\mathcal{O}_{\mathcal{B}}$ é um subanel de \mathcal{B} e que $\mathcal{A} \subset \mathcal{O}_{\mathcal{B}} \subset \mathcal{B}$.*

Demonstração: Pelo Corolário (1.5.2), temos que $\mathcal{O}_{\mathcal{B}}$ é um anel. Agora, se $\alpha \in \mathcal{A}$, então α é raiz do polinômio $p(x) = x - \alpha$, que tem coeficientes em \mathcal{A} . Assim, $\alpha \in \mathcal{O}_{\mathcal{B}}$. Portanto, $\mathcal{A} \subseteq \mathcal{O}_{\mathcal{B}} \subseteq \mathcal{B}$. ■

Definição 1.5.2 *Sejam $\mathcal{A} \subseteq \mathcal{B}$ anéis. O anel $\mathcal{O}_{\mathcal{B}} = \{\alpha \in \mathcal{B} : \alpha \text{ é inteiro sobre } \mathcal{A}\}$ é chamado de **anel dos inteiros de \mathcal{B} sobre \mathcal{A}** .*

Definição 1.5.3 *Sejam $\mathcal{A} = \mathbb{Z}$ e \mathcal{B} um anel tal que $\mathcal{A} \subset \mathcal{B}$. Chamamos de **inteiro algébrico** um elemento de \mathcal{B} que é raiz de um polinômio mônico com coeficientes em \mathbb{Z} .*

Teorema 1.5.2 *Seja \mathcal{B} um anel tal que $\mathbb{Z} \subset \mathcal{B}$. Se α é uma raiz de um polinômio mônico, onde os coeficientes são inteiros algébricos, então α é um inteiro algébrico.*

Demonstração: Seja α raiz de $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$, onde a_i é inteiro algébrico para $i = 0, 1, \dots, n-1$. Temos que α é inteiro sobre $\mathbb{Z}[a_0, \dots, a_{n-1}]$. Mas, pelo Corolário (1.5.1) temos que $\mathbb{Z}[a_0, \dots, a_{n-1}]$ é um \mathbb{Z} -módulo finitamente gerado. Desta forma, novamente pelo Corolário (1.5.1) temos que $\mathbb{Z}[a_0, \dots, a_{n-1}, \alpha]$ é um \mathbb{Z} -módulo finitamente gerado. Pelo Teorema (1.5.1), segue que α é inteiro algébrico. ■

Definição 1.5.4 *Sejam $\mathcal{A} \subseteq \mathcal{B}$ anéis. Dizemos que \mathcal{B} é inteiro sobre \mathcal{A} se todo elemento de \mathcal{B} é inteiro sobre \mathcal{A} .*

Proposição 1.5.1 *Sejam $\mathcal{A} \subseteq \mathcal{B} \subseteq \mathcal{R}$ anéis. Temos que, \mathcal{R} é inteiro sobre \mathcal{A} se, e somente se, \mathcal{R} é inteiro sobre \mathcal{B} e \mathcal{B} é inteiro sobre \mathcal{A} .*

Demonstração: Suponhamos que \mathcal{R} é inteiro sobre \mathcal{A} . Se $\alpha \in \mathcal{R}$, então existem $a_0, \dots, a_{n-1} \in \mathcal{A}$, não todos nulos, tal que

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

Como $\mathcal{A} \subseteq \mathcal{B}$, segue que $a_i \in \mathcal{B}$, para $i = 0, 1, \dots, n-1$, ou seja, α é inteiro sobre \mathcal{B} . Portanto, \mathcal{R} é inteiro sobre \mathcal{B} . Agora, seja $\alpha \in \mathcal{B}$. Como $\mathcal{B} \subseteq \mathcal{R}$, segue que $\alpha \in \mathcal{R}$ e então por hipótese α é inteiro sobre \mathcal{A} . Portanto, \mathcal{B} é inteiro sobre \mathcal{A} . Reciprocamente, seja $\alpha \in \mathcal{R}$. Como \mathcal{R} é inteiro sobre \mathcal{B} , segue que existem $b_0, \dots, b_{n-1} \in \mathcal{B}$, não todos nulos, tal que

$$\alpha^n + b_{n-1}\alpha^{n-1} + \dots + b_0 = 0.$$

Seja $C = \mathcal{A}[b_0, \dots, b_{n-1}]$. Logo, α é inteiro sobre C . Como \mathcal{B} é inteiro sobre \mathcal{A} , segue que os b_i 's são inteiros sobre \mathcal{A} . Pelo Corolário (1.5.1), segue que $C[\alpha] = \mathcal{A}[b_0, \dots, b_{n-1}, \alpha]$ é um \mathcal{A} -módulo finitamente gerado. Pelo Teorema (1.5.1), temos que α é inteiro sobre \mathcal{A} . Portanto, \mathcal{R} é inteiro sobre \mathcal{A} . ■

Proposição 1.5.2 *Sejam $\mathcal{A} \subseteq \mathcal{B}$ anéis com \mathcal{B} um domínio e inteiro sobre \mathcal{A} . Temos que \mathcal{A} é um corpo se, e somente se, \mathcal{B} é um corpo.*

Demonstração: Suponha que \mathcal{A} seja um corpo. Seja $\alpha \in \mathcal{B}$, $\alpha \neq 0$. Como \mathcal{B} é inteiro sobre \mathcal{A} , segue que α é inteiro sobre \mathcal{A} e, portanto, pelo Teorema (1.5.1), segue que $\mathcal{A}[\alpha]$ é um espaço vetorial finitamente gerado sobre \mathcal{A} , pois \mathcal{A} é um corpo. Seja

$$\varphi : \mathcal{A}[\alpha] \longrightarrow \mathcal{A}[\alpha]$$

$$b \longmapsto b\alpha.$$

Temos que φ é \mathcal{A} -linear e $\text{Ker}(\varphi) = \{b \in \mathcal{A}[\alpha] : \varphi(b) = 0\} = \{0\}$, pois $\varphi(b) = 0$ se, e somente se, $b\alpha = 0$ e como \mathcal{B} é um domínio e $\alpha \neq 0$ segue que $b=0$. Deste modo, φ é injetora e como estamos considerando espaços de mesma dimensão finita, segue que φ é sobrejetora. Portanto φ é bijetora. Assim, como $1 \in \mathcal{A}[\alpha]$, segue que existe $b' \in \mathcal{A}[\alpha]$ tal que $b'\alpha = 1$, ou seja, α é inversível em \mathcal{B} . Portanto, \mathcal{B} é um corpo. Por outro lado, seja $\alpha \in \mathcal{A}$, $\alpha \neq 0$. Como $\mathcal{A} \subset \mathcal{B}$ segue que $\alpha \in \mathcal{B}$ e como \mathcal{B} é um corpo segue que $\alpha^{-1} \in \mathcal{B}$. Como \mathcal{B} é inteiro sobre \mathcal{A} e $\alpha^{-1} \in \mathcal{B}$ segue que α^{-1} é inteiro sobre \mathcal{A} . Assim, existem $a_i \in \mathcal{A}$ não todos nulos tal que

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

Multiplicando por α^{n-1} , obtemos

$$\alpha^{-1} + a_{n-1} + \cdots + a_1\alpha^{n-2} + a_0\alpha^{n-1} = 0$$

e, assim,

$$\alpha^{-1} = -(a_{n-1} + \cdots + a_1\alpha^{n-2} + a_0\alpha^{n-1}) \in \mathcal{A}.$$

Portanto, \mathcal{A} é um corpo. ■

Definição 1.5.5 *Sejam \mathcal{A} um domínio e $\mathcal{B} = \mathbb{K} = \left\{ \frac{a}{s}; a, s \in \mathcal{A}, s \neq 0 \right\}$, o corpo das frações de \mathcal{A} . Dizemos que \mathcal{A} é **integralmente fechado** se $\mathcal{O}_{\mathbb{K}} = \mathcal{A}$, onde $\mathcal{O}_{\mathbb{K}}$ é o anel dos inteiros de \mathbb{K} sobre \mathcal{A} .*

Proposição 1.5.3 *Se \mathcal{A} é um domínio principal, então \mathcal{A} é um anel integralmente fechado.*

Demonstração: Seja \mathbb{K} o corpo de frações de \mathcal{A} . Como $\mathcal{A} \subset \mathcal{O}_{\mathbb{K}}$, resta mostrar que $\mathcal{O}_{\mathbb{K}} \subset \mathcal{A}$. Seja $\alpha \in \mathcal{O}_{\mathbb{K}}$. Temos que $\alpha = \frac{a}{b}$, com $a, b \in \mathcal{A}$ e $\text{mdc}(a, b) = 1$. Assim, existem $a_i \in \mathcal{A}$, $i = 0, 1, \dots, n-1$, não todos nulos, tal que

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

Substituindo α por $\frac{a}{b}$, temos que

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

Multiplicando por b^n , obtemos

$$a^n = b(-a_{n-1}a^{n-1} - \cdots - a_0b^{n-1}).$$

Logo b divide a^n , o que implica que $b|a$. Como $\text{mdc}(a, b) = 1$ e $b|a$, segue que b é inversível em \mathcal{A} . Logo, $\alpha = ab^{-1} \in \mathcal{A}$. Assim, $\mathcal{O}_{\mathbb{K}} = \mathcal{A}$, o que implica que \mathcal{A} é integralmente fechado. ■

Exemplo 1.5.1 *O anel \mathbb{Z} dos números inteiros é integralmente fechado, pois é principal. Todo domínio fatorial é integralmente fechado.*

Proposição 1.5.4 *Sejam \mathcal{A} um domínio, \mathbb{K} seu corpo de frações e \mathbb{L} uma extensão finita de \mathbb{K} de grau n . Sejam $\{\alpha_1, \dots, \alpha_n\}$ uma base de \mathbb{L} sobre \mathbb{K} , onde $\det(\text{Tr}_{\mathbb{L}|\mathbb{K}}(\alpha_i \alpha_j)) \neq 0$ e $\alpha \in \mathbb{L}$. Se $\text{Tr}_{\mathbb{L}|\mathbb{K}}(\alpha \beta) = 0$ para todo $\beta \in \mathbb{L}$, então $\alpha = 0$.*

Demonstração: Como $\{\alpha_1, \dots, \alpha_n\}$ é uma base de \mathbb{L} sobre \mathbb{K} , segue que $\alpha = a_1 \alpha_1 + a_2 \alpha_2 + \dots + a_n \alpha_n$, onde $a_i \in \mathbb{K}$, para $i = 1, \dots, n$. Por hipótese, $\text{Tr}_{\mathbb{L}|\mathbb{K}}(\alpha \alpha_j) = 0$, para $j = 1, \dots, n$. Assim, para $j = 1, \dots, n$, temos que

$$0 = \text{Tr}_{\mathbb{L}|\mathbb{K}}(\alpha \alpha_j) = a_1 \text{Tr}_{\mathbb{L}|\mathbb{K}}(\alpha_1 \alpha_j) + a_2 \text{Tr}_{\mathbb{L}|\mathbb{K}}(\alpha_2 \alpha_j) + \dots + a_n \text{Tr}_{\mathbb{L}|\mathbb{K}}(\alpha_n \alpha_j).$$

Na forma matricial, temos que

$$\begin{bmatrix} \text{Tr}(\alpha_1 \alpha_1) & \text{Tr}(\alpha_2 \alpha_1) & \cdots & \text{Tr}(\alpha_n \alpha_1) \\ \text{Tr}(\alpha_1 \alpha_2) & \text{Tr}(\alpha_2 \alpha_2) & \cdots & \text{Tr}(\alpha_n \alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \text{Tr}(\alpha_1 \alpha_n) & \text{Tr}(\alpha_2 \alpha_n) & \cdots & \text{Tr}(\alpha_n \alpha_n) \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Como $\det(\text{Tr}_{\mathbb{L}|\mathbb{K}}(\alpha_i \alpha_j)) \neq 0$ segue que $a_1 = a_2 = \dots = a_n = 0$. Portanto, $\alpha = 0$. ■

Corolário 1.5.4 *Com as mesmas hipóteses da Proposição (1.5.4), temos que a aplicação*

$$\rho : \mathbb{L} \longrightarrow \text{Hom}_{\mathbb{K}}(\mathbb{L}, \mathbb{K})$$

$$\alpha \longmapsto S_\alpha, \text{ onde } S_\alpha(\beta) = \text{Tr}_{\mathbb{L}|\mathbb{K}}(\alpha \beta),$$

é um isomorfismo.

Demonstração: Temos que ρ é homomorfismo de espaços vetoriais, uma vez que se $\alpha_1, \alpha_2 \in \mathbb{L}$, então

$$\begin{aligned} \rho(\alpha_1 + \alpha_2)(\beta) &= S_{\alpha_1 + \alpha_2}(\beta) = \text{Tr}_{\mathbb{L}|\mathbb{K}}((\alpha_1 + \alpha_2)\beta) \\ &= \text{Tr}_{\mathbb{L}|\mathbb{K}}(\alpha_1 \beta) + \text{Tr}_{\mathbb{L}|\mathbb{K}}(\alpha_2 \beta) = S_{\alpha_1}(\beta) + S_{\alpha_2}(\beta) \end{aligned}$$

$$= \rho(\alpha_1)(\beta) + \rho(\alpha_2)(\beta) \quad e$$

$$\begin{aligned} \rho(a\alpha)(\beta) &= S_{a\alpha}(\beta) = Tr_{\mathbb{L}|\mathbb{K}}(a\alpha\beta) = aTr_{\mathbb{L}|\mathbb{K}}(\alpha\beta) \\ &= aS_{\alpha}(\beta) = a\rho(\alpha)(\beta), \end{aligned}$$

para todo $\beta \in \mathbb{L}, \alpha \in \mathbb{K}$. Agora, seja $\alpha \in \mathbb{L}$ tal que $\rho(\alpha) = 0$. Temos que, $\rho(\alpha)(\beta) = S_{\alpha}(\beta) = Tr(\alpha\beta) = 0, \forall \beta \in \mathbb{L}$. Pela Proposição (1.5.4), temos que $\alpha = 0$, provando assim que ρ é injetora. Finalmente, ρ é sobrejetora, pois $dim_{\mathbb{K}}\mathbb{L} = dim_{\mathbb{K}}(Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{K}))$. Portanto, ρ é um isomorfismo. ■

Proposição 1.5.5 *Se \mathcal{A} é um domínio, \mathbb{K} seu corpo de frações, $\mathbb{K} \subseteq \mathbb{L}$ uma extensão finita e $\alpha \in \mathbb{L}$ um elemento inteiro sobre \mathcal{A} , então os coeficientes do polinômio característico de α são inteiros sobre \mathcal{A} . Em particular, $Tr_{\mathbb{L}|\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}|\mathbb{K}}(\alpha)$ são inteiros sobre \mathcal{A} .*

Demonstração: Pela Proposição (1.4.2), temos que $m(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$. Como os coeficientes de $m(x)$ são somas e produtos dos α_i , é suficiente mostrar que os α_i são inteiros sobre \mathcal{A} . Pela Teoria de Galois, existe um \mathbb{K} -homomorfismo $\sigma_i : \mathbb{K}[\alpha] \rightarrow \mathbb{K}[\alpha_i]$, definido por $\sigma_i(\alpha) = \alpha_i$, para $i = 1, \dots, n$. Como α é inteiro sobre \mathcal{A} , segue que

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

com $a_i \in \mathcal{A}$, não todos nulos, para $i = 1, \dots, n$. Aplicando σ_i , obtemos

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

ou seja, α_i é inteiro sobre \mathcal{A} , para $i = 1, \dots, n$. ■

Corolário 1.5.5 *Se \mathcal{A} é um anel integralmente fechado e $\alpha \in \mathbb{L}$ é inteiro sobre \mathcal{A} , então os coeficientes do polinômio característico de α , $Tr_{\mathbb{L}|\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}|\mathbb{K}}(\alpha)$ são elementos de \mathcal{A} .*

Demonstração: Seja $m(x)$ o polinômio característico de α . Os coeficientes de $m(x)$ são elementos de \mathbb{K} e são inteiros sobre \mathcal{A} . Como \mathcal{A} é integralmente fechado, segue que os coeficientes estão em \mathcal{A} . Portanto, $Tr_{\mathbb{L}|\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}|\mathbb{K}}(\alpha)$ são elementos de \mathcal{A} . ■

Teorema 1.5.3 *Se \mathcal{A} é um anel integralmente fechado, \mathbb{K} seu corpo de frações, $\mathbb{K} \subseteq \mathbb{L}$ uma extensão finita de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros de \mathbb{L} sobre \mathcal{A} , então $\mathcal{O}_{\mathbb{L}}$ é um \mathcal{A} -submódulo de um \mathcal{A} -módulo livre de posto n .*

Demonstração: Seja $\{\alpha_1, \dots, \alpha_n\}$ uma base de \mathbb{L} sobre \mathbb{K} . Como toda extensão finita é algébrica, segue que todos os α_i 's são algébricos sobre \mathbb{K} , ou seja, existem $a_{ij} \in \mathcal{A}$, para $i = 1, \dots, n; j = 0, 1, \dots, n$, não todos nulos, tal que

$$a_{in}\alpha_i^n + a_{i(n-1)}\alpha_i^{n-1} + \dots + a_{i0} = 0.$$

Fixado i , supondo que $a_{in} \neq 0$ e multiplicando esta equação por a_{in}^{n-1} , temos que $a_{in}\alpha_i$ é inteiro sobre \mathcal{A} , uma vez que

$$a_{in}^{n-1}(a_{in}\alpha_i^n + \dots + a_{i0}) = (a_{in}\alpha_i)^n + a_{i(n-1)}(a_{in}\alpha_i)^{n-1} + \dots + a_{in}^{n-1}a_{i0} = 0.$$

Seja $a_{in}\alpha_i = z_i \in \mathcal{O}_{\mathbb{L}}$, para $i = 1, \dots, n$. Vamos mostrar que $\{z_1, \dots, z_n\}$ é uma base de \mathbb{L} sobre \mathbb{K} . Suponhamos que $b_1z_1 + b_2z_2 + \dots + b_nz_n = 0$, onde $b_i \in \mathcal{A}$, para $i = 1, \dots, n$. Assim,

$$b_1a_{1n}\alpha_1 + b_2a_{2n}\alpha_2 + \dots + b_na_{nn}\alpha_n = 0.$$

Como $\{\alpha_1, \dots, \alpha_n\}$ é uma base de \mathbb{L} sobre \mathbb{K} , segue que $b_ia_{in} = 0$ e, assim, $b_i = 0$, para $i = 1, \dots, n$. Portanto, $\{z_1, \dots, z_n\}$ é linearmente independente e como possui n elementos segue que é uma base de \mathbb{L} sobre \mathbb{K} . Pelo Corolário (1.5.4), existe uma base dual $\{y_1, \dots, y_n\}$ tal que

$$\rho(z_i)(y_j) = S_{z_i}(y_j) = Tr_{\mathbb{L}|\mathbb{K}}(z_iz_j) = \delta_{ij}, \text{ para } i, j = 1, \dots, n.$$

Agora, se $\alpha \in \mathcal{O}_{\mathbb{L}}$, então $\alpha z_i \in \mathcal{O}_{\mathbb{L}}$, para $i = 1, \dots, n$. Pelo Corolário (1.5.5), temos que $Tr_{\mathbb{L}|\mathbb{K}}(\alpha z_i) \in \mathcal{A}$, para $i = 1, \dots, n$. Como $\{y_1, \dots, y_n\}$ é uma base de \mathbb{L} sobre \mathbb{K} , segue que $\alpha = c_1y_1 + \dots + c_ny_n$, com $c_i \in \mathbb{K}$, para $i = 1, \dots, n$. Assim, $Tr_{\mathbb{L}|\mathbb{K}}(\alpha z_i) = c_i \in \mathcal{A}$, para $i = 1, \dots, n$. Desta forma, temos que $\alpha \in \sum_{i=1}^n \mathcal{A}y_i$. Portanto, $\mathcal{O}_{\mathbb{L}}$ é um \mathcal{A} -submódulo do

\mathcal{A} -módulo livre $\sum_{i=1}^n \mathcal{A}y_i$ de posto n . ■

Corolário 1.5.6 *Com as mesmas hipóteses do Teorema (1.5.3), se \mathcal{A} é um domínio principal, então $\mathcal{O}_{\mathbb{L}}$ é um \mathcal{A} -módulo livre de posto n .*

Demonstração: Pelo Teorema (1.2.1), temos que todo \mathcal{A} -submódulo de um \mathcal{A} -módulo livre é livre de posto menor ou igual a n . Pela demonstração do Teorema (1.5.3), temos que $\mathcal{O}_{\mathbb{L}}$ contém uma base de n elementos de \mathbb{L} sobre \mathbb{K} . Logo, $\mathcal{O}_{\mathbb{L}}$ tem posto n . ■

Corolário 1.5.7 *Com as mesmas hipóteses do Teorema (1.5.3), se \mathcal{A} é um domínio principal e se $I \subseteq \mathcal{O}_{\mathbb{L}}$ é um ideal não nulo, então I é um \mathcal{A} -módulo livre de posto n .*

Demonstração: Sejam $\{e_1, \dots, e_n\}$ uma base de $\mathcal{O}_{\mathbb{L}}$ sobre \mathcal{A} e $\alpha \in I$, $\alpha \neq 0$. Assim, $\alpha e_1, \dots, \alpha e_n \in I$ e são linearmente independentes sobre \mathcal{A} , uma vez que se $\alpha_1 \alpha e_1 + \dots + \alpha_n \alpha e_n = 0$, com $\alpha_i \in \mathcal{A}$, para $i = 1, \dots, n$, então $\alpha_i \alpha = 0$ para $i = 1, \dots, n$. Como \mathcal{A} é um domínio, segue que $\alpha_i = 0$, para $i = 1, \dots, n$. Logo, I é um \mathcal{A} -módulo livre de posto n . ■

Proposição 1.5.6 *Se \mathcal{A} é um anel noetheriano e integralmente fechado, \mathbb{K} o corpo de frações de \mathcal{A} , $\mathbb{K} \subseteq \mathbb{L}$ uma extensão finita de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de \mathbb{L} sobre \mathcal{A} , então $\mathcal{O}_{\mathbb{L}}$ é um \mathcal{A} -módulo finitamente gerado e $\mathcal{O}_{\mathbb{L}}$ é um anel noetheriano.*

Demonstração: Pelo Teorema (1.5.3), temos que $\mathcal{O}_{\mathbb{L}}$ é um submódulo do \mathcal{A} -módulo livre $\sum_{i=1}^n \mathcal{A}y_i$, de posto n . Desta forma, como \mathcal{A} é noetheriano segue, pelo Corolário (1.2.2), que $\sum_{i=1}^n \mathcal{A}y_i$ é um \mathcal{A} -módulo noetheriano. Como $\mathcal{O}_{\mathbb{L}}$ é um \mathcal{A} -submódulo de $\sum_{i=1}^n \mathcal{A}y_i$, segue que $\mathcal{O}_{\mathbb{L}}$ é finitamente gerado. ■

Proposição 1.5.7 *Se \mathcal{A} é um domínio, \mathbb{K} seu corpo de frações, \mathbb{L} uma extensão finita de \mathbb{K} de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de \mathbb{L} sobre \mathcal{A} , então $\mathcal{O}_{\mathbb{L}}$ é integralmente fechado.*

Demonstração: Seja \mathbb{M} o corpo das frações de $\mathcal{O}_{\mathbb{L}}$. Temos que $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$. Seja $x \in \mathbb{M}$ tal que x é inteiro sobre $\mathcal{O}_{\mathbb{L}}$. Como $\mathcal{O}_{\mathbb{L}}$ é inteiro sobre \mathcal{A} segue, da demonstração da Proposição (1.5.1), que x é inteiro sobre \mathcal{A} . Assim, se $\mathcal{O}_{\mathbb{M}}$ é o conjunto dos elementos de \mathbb{M} que são inteiros sobre $\mathcal{O}_{\mathbb{L}}$, então $\mathcal{O}_{\mathbb{M}} \subset \mathcal{O}_{\mathbb{L}}$. Como $\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{M}}$, temos que $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{M}}$, o que implica que $\mathcal{O}_{\mathbb{L}}$ é integralmente fechado. ■

1.6 Discriminante

Nesta seção, apresentamos o conceito de discriminante e alguns resultados que auxiliam no seu cálculo.

Definição 1.6.1 *Sejam $\mathcal{A} \subset \mathcal{B}$ anéis tal que \mathcal{B} é um \mathcal{A} -módulo livre de posto finito n e $(\alpha_1, \dots, \alpha_n) \in \mathcal{B}^n$. Definimos o **discriminante** de $(\alpha_1, \dots, \alpha_n)$ por*

$$D_{\mathcal{B}|\mathcal{A}}(\alpha_1, \dots, \alpha_n) = \det(\text{Tr}_{\mathcal{B}|\mathcal{A}}(\alpha_i \alpha_j)).$$

Proposição 1.6.1 *Sejam $\mathcal{A} \subset \mathcal{B}$ anéis e $(\alpha_1, \dots, \alpha_n) \in \mathcal{B}^n$. Se $(\beta_1, \dots, \beta_n) \in \mathcal{B}^n$ é tal que $\beta_i = \sum_{j=1}^n a_{ij}\alpha_j$, com $a_{ij} \in \mathcal{A}$, então*

$$D_{\mathcal{B}|\mathcal{A}}(\beta_1, \dots, \beta_n) = (\det(a_{ij}))^2 D_{\mathcal{B}|\mathcal{A}}(\alpha_1, \dots, \alpha_n).$$

Demonstração: Sejam $\beta_p = \sum_{i=1}^n a_{pi}\alpha_i$ e $\beta_q = \sum_{j=1}^n a_{qj}\alpha_j$, com $a_{pi}, a_{qj} \in \mathcal{A}$. Temos que

$$\beta_p\beta_q = \sum_{i=1}^n a_{pi}\alpha_i \sum_{j=1}^n a_{qj}\alpha_j = \sum_{i,j=1}^n a_{pi}a_{qj}\alpha_i\alpha_j \quad \text{e}$$

$$\text{Tr}(\beta_p\beta_q) = \text{Tr}\left(\sum_{i,j} a_{pi}a_{qj}\alpha_i\alpha_j\right) = \sum_{i,j} a_{pi}a_{qj}\text{Tr}(\alpha_i\alpha_j).$$

Na forma matricial, temos que

$$(\text{Tr}(\beta_p\beta_q))_{p,q=1}^n = (a_{pi})_{p,i=1}^n (\text{Tr}(\alpha_i\alpha_j))_{i,j=1}^n ((a_{qj})_{q,j=1}^n)^t.$$

Pela Definição (1.6.1), temos que $D_{\mathcal{B}|\mathcal{A}}(\beta_1, \dots, \beta_n) = \det(\text{Tr}_{\mathcal{B}|\mathcal{A}}(\beta_p\beta_q))$. Logo,

$$\begin{aligned} D_{\mathcal{B}|\mathcal{A}}(\beta_1, \dots, \beta_n) &= \det((a_{pi})(\text{Tr}_{\mathcal{B}|\mathcal{A}}(\alpha_i\alpha_j))(a_{qj})^t) = \det(a_{pi})\det(\text{Tr}_{\mathcal{B}|\mathcal{A}}(\alpha_i\alpha_j))\det(a_{qj})^t \\ &= \det(a_{ij})^2 D_{\mathcal{B}|\mathcal{A}}(\alpha_1, \dots, \alpha_n), \end{aligned}$$

o que demonstra a proposição. ■

Observação 1.6.1 *Sejam $\mathcal{A} \subset \mathcal{B}$ anéis tal que \mathcal{B} é um \mathcal{A} -módulo livre de posto n , $\{\alpha_1, \dots, \alpha_n\}$ e $\{\beta_1, \dots, \beta_n\}$ duas bases de \mathcal{B} sobre \mathcal{A} . A matriz (a_{ij}) que expressa uma base em termos da outra, admite matriz inversa com entradas em \mathcal{A} . Portanto, ambos $\det(a_{ij})$ e $\det(a_{ij})^{-1}$ são inversíveis em \mathcal{A} .*

Definição 1.6.2 *Sejam $\mathcal{A} \subset \mathcal{B}$ anéis tal que \mathcal{B} é um \mathcal{A} -módulo livre de posto finito n . O discriminante de \mathcal{B} sobre \mathcal{A} é um ideal principal em \mathcal{A} , definido por,*

$$D_{\mathcal{B}|\mathcal{A}} = \langle D_{\mathcal{B}|\mathcal{A}}(\alpha_1, \dots, \alpha_n) \rangle,$$

onde $\{\alpha_1, \dots, \alpha_n\}$ é uma base de \mathcal{B} sobre \mathcal{A} .

Observação 1.6.2 *Note que o ideal definido acima independe da base considerada, pois, pela*

Observação (1.6.1), temos que o discriminante de quaisquer duas bases são associados, logo eles geram o mesmo ideal.

Definição 1.6.3 Sejam \mathcal{A} um anel principal, \mathbb{K} seu corpo de frações, \mathbb{L} uma extensão finita de \mathbb{K} de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de \mathbb{L} sobre \mathcal{A} . Definimos o **discriminante absoluto de \mathbb{L} sobre \mathbb{K}** como

$$\text{Disc}(\mathbb{L}|\mathbb{K}) = D_{\mathbb{L}|\mathbb{K}}(\alpha_1, \dots, \alpha_n),$$

onde $\{\alpha_1, \dots, \alpha_n\}$ é uma \mathcal{A} -base de $\mathcal{O}_{\mathbb{L}}$.

Lema 1.6.1 (Lema de Dedekind) Se G é um grupo, \mathbb{K} um corpo e $\sigma_1, \dots, \sigma_n$ os homomorfismos distintos de G no grupo multiplicativo \mathbb{K}^* , então $\{\sigma_1, \dots, \sigma_n\}$ é linearmente independente sobre \mathbb{K} .

Demonstração: Suponhamos que os σ_i 's são linearmente dependentes. Seja $\sum_{i=1}^m a_i \sigma_i = 0$, com $a_i \in \mathbb{K}$, uma combinação linear com m mínimo e $a_i \neq 0$, para todo $i = 1, 2, \dots, m$. Logo, para qualquer $x \in G$, temos que

$$a_1 \sigma_1(x) + a_2 \sigma_2(x) + \dots + a_m \sigma_m(x) = 0.$$

Como os homomorfismos são distintos, segue que existe $c \in G$ tal que $\sigma_1(c) \neq \sigma_m(c)$. Agora, como $cx \in G$, segue que

$$a_1 \sigma_1(cx) + a_2 \sigma_2(cx) + \dots + a_m \sigma_m(cx) = 0$$

e, assim,

$$a_1 \sigma_1(c) \sigma_1(x) + a_2 \sigma_2(c) \sigma_2(x) + \dots + a_m \sigma_m(c) \sigma_m(x) = 0.$$

Multiplicando a primeira igualdade por $\sigma_1(c)$, obtemos

$$a_1 \sigma_1(c) \sigma_1(x) + a_2 \sigma_1(c) \sigma_2(x) + \dots + a_m \sigma_1(c) \sigma_m(x) = 0.$$

Subtraindo as igualdades, obtemos

$$a_2 \sigma_2(x) (\sigma_2(c) - \sigma_1(c)) + \dots + a_m \sigma_m(x) (\sigma_m(c) - \sigma_1(c)) = 0.$$

Como isto vale para todo $x \in G$ e m é mínimo, segue que $a_m (\sigma_m(c) - \sigma_1(c)) = 0$. Como $a_m \neq 0$, segue que $\sigma_m(c) = \sigma_1(c)$, o que é um absurdo. ■

Proposição 1.6.2 *Sejam \mathbb{K} um corpo, \mathbb{L} uma extensão finita de \mathbb{K} de grau n e $\{\sigma_1, \dots, \sigma_n\}$ os n \mathbb{K} -homomorfismos distintos de \mathbb{L} em um corpo algebricamente fechado F contendo \mathbb{K} . Se $\{\alpha_1, \dots, \alpha_n\}$ é uma base de \mathbb{L} sobre \mathbb{K} , então*

$$D_{\mathbb{L}|\mathbb{K}}(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2 \neq 0.$$

Demonstração: Temos que $D_{\mathbb{L}|\mathbb{K}}(\alpha_1, \dots, \alpha_n) = \det(\text{Tr}_{\mathbb{L}|\mathbb{K}}(\alpha_i \alpha_j))$. Como o traço de $\alpha_i \alpha_j$ é a soma dos seus conjugados, segue que $D_{\mathbb{L}|\mathbb{K}}(\alpha_1, \dots, \alpha_n) = \det(\text{Tr}_{\mathbb{L}|\mathbb{K}}(\alpha_i \alpha_j)) = \det\left(\sum_{k=1}^n \sigma_k(\alpha_i \alpha_j)\right) = \det(\sigma_k(\alpha_i)) \det(\sigma_k(\alpha_j)) = (\det(\sigma_i(\alpha_j)))^2$, uma vez que

$$\begin{bmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{bmatrix} \begin{bmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{bmatrix} = \left(\sum_{k=1}^n \sigma_k(\alpha_i \alpha_j)\right)_{i,j=1}^n.$$

Se $\det(\sigma_k(\alpha_j)) = 0$, então as colunas da matriz $(\sigma_k(\alpha_j))$ são linearmente dependentes. Desta forma, existem $a_1, \dots, a_n \in F$, não todos nulos, tal que $\sum_{i=1}^n a_i \sigma_i(\alpha_j) = 0$ para todo j . Se $\alpha \in \mathbb{L}$, então $\alpha = \sum_{i=1}^n b_i \alpha_i$, com $b_i \in \mathbb{K}$, e por linearidade concluímos que $\sum_{i=1}^n a_i \sigma_i(\alpha) = 0$. Mas isto contradiz o Lema de Dedekind e, portanto, $\det(\sigma_k(\alpha_j)) \neq 0$. ■

Proposição 1.6.3 *Se \mathbb{K} é um corpo, $\mathbb{L} = \mathbb{K}[\alpha]$ uma extensão finita de \mathbb{K} de grau n e $f(x)$ o polinômio minimal de α sobre \mathbb{K} , então,*

$$D_{\mathbb{L}|\mathbb{K}}(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N_{\mathbb{L}|\mathbb{K}}(f'(\alpha)),$$

onde $f'(\alpha)$ é a derivada de $f(x)$ aplicada a α .

Demonstração: Sejam $\alpha_1, \dots, \alpha_n$ as raízes de $f(x)$ em alguma extensão de \mathbb{K} . Pela Proposição (1.6.2), temos que $D_{\mathbb{L}|\mathbb{K}}(1, \alpha, \dots, \alpha^{n-1}) = (\det(\sigma_i(\alpha^j)))^2 = \det(\alpha_i^j)^2$, com $i = 1, \dots, n$ e $j = 0, \dots, n-1$. Como $\det(\alpha_i^j)$ é um determinante de Vandermonde, segue que

$$\begin{aligned} \det(\alpha_i^j)^2 &= \left[\prod_{1 \leq k < i \leq n} (\alpha_i - \alpha_k) \right]^2 = \prod_{1 \leq k < i \leq n} [(\alpha_i - \alpha_k)(\alpha_i - \alpha_k)] \\ &= (-1)^{\frac{1}{2}n(n-1)} \prod_{1 \leq k, i \leq n, i \neq k} (\alpha_i - \alpha_k) = (-1)^{\frac{1}{2}n(n-1)} \prod_{i=1}^n \left[\prod_{k=1, k \neq i}^n (\alpha_i - \alpha_k) \right] \\ &= (-1)^{\frac{1}{2}n(n-1)} \prod_{i=1}^n f'(\alpha_i) = (-1)^{\frac{1}{2}n(n-1)} N(f'(\alpha)), \end{aligned}$$

o que prova a proposição. ■

Lema 1.6.2 *Sejam \mathcal{A} um domínio e $\mathcal{B}_1, \dots, \mathcal{B}_g$ anéis contendo \mathcal{A} , tais que cada \mathcal{B}_i , para $i = 1, \dots, g$, sejam \mathcal{A} -módulos livres finitamente gerados. Se $\mathcal{B} = \prod_{i=1}^g \mathcal{B}_i$, então,*

$$D_{\mathcal{B}|\mathcal{A}} = \prod_{i=1}^g D_{\mathcal{B}_i|\mathcal{A}}.$$

Demonstração: Faremos a prova por indução sobre g . Para o caso $g = 2$, considere $\{x_1, \dots, x_n\}$ uma base de \mathcal{B}_1 sobre \mathcal{A} e $\{y_1, \dots, y_m\}$ uma base de \mathcal{B}_2 sobre \mathcal{A} . Com a identificação natural de \mathcal{B}_1 em $\mathcal{B}_1 \times \{0\}$ e \mathcal{B}_2 em $\{0\} \times \mathcal{B}_2$, podemos considerar $\{(x_1, 0), \dots, (x_n, 0), (0, y_1), \dots, (0, y_m)\}$ uma base de $\mathcal{B} = \mathcal{B}_1 \times \mathcal{B}_2$. Com $\bar{x}_i = (x_i, 0)$ e $\bar{y}_i = (0, y_i)$, segue que $\bar{x}_i \bar{y}_i = 0$ e, assim, $Tr_{\mathcal{B}|\mathcal{A}}(\bar{x}_i \bar{y}_i) = 0$. Como $Tr_{\mathcal{B}|\mathcal{A}}(\bar{x}_i \bar{x}_j) = Tr_{\mathcal{B}_1|\mathcal{A}}(x_i x_j)$ e $Tr_{\mathcal{B}|\mathcal{A}}(\bar{y}_i \bar{y}_j) = Tr_{\mathcal{B}_2|\mathcal{A}}(y_i y_j)$, segue que $D_{\mathcal{B}|\mathcal{A}}$ é o ideal gerado por

$$\begin{aligned} D_{\mathcal{B}|\mathcal{A}}(\bar{x}_1, \dots, \bar{x}_n, \bar{y}_1, \dots, \bar{y}_m) &= \det \begin{pmatrix} Tr_{\mathcal{B}_1|\mathcal{A}}(\bar{x}_i \bar{x}_j) & 0 \\ 0 & Tr_{\mathcal{B}_2|\mathcal{A}}(\bar{y}_k \bar{y}_l) \end{pmatrix} \\ &= \det(Tr_{\mathcal{B}_1|\mathcal{A}}(\bar{x}_i \bar{x}_j)) \det(Tr_{\mathcal{B}_2|\mathcal{A}}(\bar{y}_k \bar{y}_l)) \\ &= D_{\mathcal{B}_1|\mathcal{A}}(\bar{x}_1, \dots, \bar{x}_n) D_{\mathcal{B}_2|\mathcal{A}}(\bar{y}_1, \dots, \bar{y}_m) \\ &= D_{\mathcal{B}_1|\mathcal{A}}(x_1, \dots, x_n) D_{\mathcal{B}_2|\mathcal{A}}(y_1, \dots, y_m). \end{aligned}$$

Portanto, $D_{\mathcal{B}|\mathcal{A}} = D_{\mathcal{B}_1|\mathcal{A}} D_{\mathcal{B}_2|\mathcal{A}} = \prod_{i=1}^2 D_{\mathcal{B}_i|\mathcal{A}}$. Agora, suponhamos verdadeiro para $g - 1$, ou seja, se $C = \prod_{i=1}^{g-1} \mathcal{B}_i$, então $D_{C|\mathcal{A}} = \prod_{i=1}^{g-1} D_{\mathcal{B}_i|\mathcal{A}}$. Seja, $\mathcal{B} = C \times \mathcal{B}_g$. Identificando C com $C \times \{0\}$, \mathcal{B}_g com $\{0\} \times \mathcal{B}_g$ e usando o caso $g = 2$ temos, por hipótese de indução, que $D_{\mathcal{B}|\mathcal{A}} = D_{C|\mathcal{A}} D_{\mathcal{B}_g|\mathcal{A}} = \left(\prod_{i=1}^{g-1} D_{\mathcal{B}_i|\mathcal{A}} \right) D_{\mathcal{B}_g|\mathcal{A}} = \prod_{i=1}^g D_{\mathcal{B}_i|\mathcal{A}}$. ■

Observação 1.6.3 *Com as mesmas hipóteses do Lema (1.6.2), prova-se analogamente que se $\alpha \in \mathcal{B}$ então $m_{\mathcal{B}|\mathcal{A}}(\alpha) = \prod_{i=1}^g m_{\mathcal{B}_i|\mathcal{A}}(\alpha)$, $N_{\mathcal{B}|\mathcal{A}}(\alpha) = \prod_{i=1}^g N_{\mathcal{B}_i|\mathcal{A}}(\alpha)$ e $Tr_{\mathcal{B}|\mathcal{A}}(\alpha) = \prod_{i=1}^g Tr_{\mathcal{B}_i|\mathcal{A}}(\alpha)$.*

1.7 Ideais Fracionários

Nesta seção, apresentamos o conceito de ideais fracionários, juntamente com suas principais propriedades.

Definição 1.7.1 *Sejam \mathcal{A} um domínio, $\mathbb{K} = \left\{ \frac{a}{s}; a, s \in \mathcal{A}, s \neq 0 \right\}$ seu corpo de frações e $I \subset \mathbb{K}$ um conjunto. Dizemos que I é um **ideal fracionário** de \mathcal{A} , ou de \mathbb{K} em relação a \mathcal{A} , se I é um \mathcal{A} -módulo e existe $d \in \mathcal{A} - \{0\}$ tal que $dI \subseteq \mathcal{A}$.*

Observação 1.7.1 *Todo ideal de \mathcal{A} é também um ideal fracionário, basta tomar $d = 1$. Se necessário, passaremos a chamar tais ideais de **ideais inteiros**.*

Definição 1.7.2 *Sejam M, N ideais fracionários de \mathcal{A} . Definimos o produto de MN como o ideal fracionário*

$$MN = \left\{ \sum_{i=1}^n x_i y_i, n \geq 1, x_i \in M, y_i \in N \right\}.$$

Definição 1.7.3 *Dizemos que um ideal fracionário M de \mathcal{A} é **invertível** se existe um ideal fracionário N de \mathcal{A} tal que $MN = \mathcal{A}$.*

Definição 1.7.4 *Sejam \mathcal{A} um domínio, \mathbb{K} seu corpo de frações e I, J ideais fracionários de \mathcal{A} . Dizemos que I **divide** J se existe um ideal inteiro M de \mathcal{A} tal que $J = IM$.*

Lema 1.7.1 *Sejam \mathcal{A} um domínio, \mathbb{K} seu corpo de frações e I, J ideais fracionários invertíveis de \mathcal{A} . Temos que I divide J se, e somente se, $J \subseteq I$.*

Demonstração: Se I divide J , então existe um ideal $M \subseteq \mathcal{A}$ tal que $J = IM \subseteq I$. Por outro lado, se $J \subseteq I$, então $J I^{-1} \subseteq I I^{-1} = \mathcal{A}$. Mas, isto implica que $J I^{-1}$ é um ideal inteiro tal que $(J I^{-1}) I = J$. Portanto, I divide J . ■

Proposição 1.7.1 *Se \mathcal{A} é um domínio noetheriano, \mathbb{K} seu corpo de frações, \mathbb{L} uma extensão finita de \mathbb{K} e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de \mathbb{L} sobre \mathcal{A} , então todo ideal fracionário I de $\mathcal{O}_{\mathbb{L}}$ é um \mathcal{A} -módulo finitamente gerado.*

Demonstração: Como I é um ideal fracionário de \mathcal{A} , existe $d \in \mathcal{A} - \{0\}$ tal que $dI \subseteq \mathcal{A}$. Assim, $I \subseteq d^{-1}\mathcal{A}$. Agora, a aplicação $\varphi : \mathcal{A} \rightarrow d^{-1}\mathcal{A}$ tal que $\varphi(x) = d^{-1}x$, $x \in \mathcal{A}$ é um isomorfismo. Assim, \mathcal{A} é isomorfo a $d^{-1}\mathcal{A}$. Como \mathcal{A} noetheriano, segue que $d^{-1}\mathcal{A}$ é um \mathcal{A} -módulo noetheriano. Logo, I é um \mathcal{A} -módulo finitamente gerado. ■

Corolário 1.7.1 *Se \mathcal{A} é um anel principal, \mathbb{K} seu corpo de frações, \mathbb{L} uma extensão finita de \mathbb{K} e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de \mathbb{L} sobre \mathcal{A} , então todo ideal fracionário não nulo I de $\mathcal{O}_{\mathbb{L}}$ é um \mathcal{A} -módulo livre de posto n .*

Demonstração: Seja I um ideal fracionário não nulo de $\mathcal{O}_{\mathbb{L}}$. Temos que, existe $d \in \mathcal{O}_{\mathbb{L}} - \{0\}$ tal que $dI \subset \mathcal{O}_{\mathbb{L}}$. Seja $R = dI$. Temos que R é um ideal inteiro de $\mathcal{O}_{\mathbb{L}}$. Pelo Corolário (1.5.7), temos que R é um \mathcal{A} -módulo livre de posto n . Seja $\{w_1, \dots, w_n\}$ uma \mathcal{A} -base de R . Temos que $\{d^{-1}w_1, \dots, d^{-1}w_n\}$ é uma \mathcal{A} -base de I . De fato, temos que $\{d^{-1}w_1, \dots, d^{-1}w_n\}$ gera I . Agora, suponha que $\sum_{i=1}^n a_i d^{-1}w_i = 0$, para $a_i \in \mathcal{A}$, para $i = 1, \dots, n$. Temos que $\sum_{i=1}^n a_i d^{-1}w_i = d^{-1} \sum_{i=1}^n a_i w_i = 0$, o que implica que $\sum_{i=1}^n a_i w_i = 0$ e, como $\{w_1, \dots, w_n\}$ uma \mathcal{A} -base, segue que $a_i = 0$, para todo $i = 1, \dots, n$. Logo, I é um \mathcal{A} -módulo livre de posto n . ■

1.8 Anéis de Dedekind

Nesta seção, apresentamos os anéis de Dedekind juntamente com algumas de suas propriedades. Destaca-se o fato de que todo ideal fracionário não nulo de um anel de Dedekind pode ser expresso de forma única como produto de ideais primos do anel.

Definição 1.8.1 Dizemos que um anel \mathcal{A} é um **anel de Dedekind** se satisfaz as seguintes condições:

- \mathcal{A} é integralmente fechado;
- \mathcal{A} é noetheriano;
- Todo ideal primo não nulo de \mathcal{A} é maximal.

Teorema 1.8.1 Se \mathcal{A} é um anel de Dedekind, \mathbb{K} seu corpo de frações, $\mathbb{K} \subseteq \mathbb{L}$ uma extensão finita de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros de \mathbb{L} sobre \mathcal{A} , então $\mathcal{O}_{\mathbb{L}}$ é um anel Dedekind.

Demonstração: Pelas Proposições (1.5.7) e (1.5.6), temos que $\mathcal{O}_{\mathbb{L}}$ é integralmente fechado e noetheriano, respectivamente. Falta mostrar que todo ideal primo não nulo de $\mathcal{O}_{\mathbb{L}}$ é maximal. Seja $P \subset \mathcal{O}_{\mathbb{L}}$ um ideal primo não nulo. Como $\mathcal{A} \subset \mathcal{O}_{\mathbb{L}}$ segue, pela Proposição (1.1.3), que $P \cap \mathcal{A}$ é um ideal primo de \mathcal{A} . Vamos mostrar que $P \cap \mathcal{A}$ é não nulo. Seja $\alpha \in P$ tal que $\alpha \neq 0$. Como $P \subset \mathcal{O}_{\mathbb{L}}$ segue que $\alpha \in \mathcal{O}_{\mathbb{L}}$. Assim, existem $a_i \in \mathcal{A}$, para $i = 0, \dots, n-1$, não todos nulos, tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 = 0$, e que n seja mínimo. Logo, $a_0 \neq 0$, pois caso contrário, obteríamos uma equação de grau menor. Assim,

$$a_0 = \alpha(-\alpha^{n-1} - a_{n-1}\alpha^{n-2} - \dots - a_1) \in \alpha\mathcal{O}_{\mathbb{L}} \cap \mathcal{A} \subset P \cap \mathcal{A}.$$

Portanto, $P \cap \mathcal{A} \neq 0$. Como $P \cap \mathcal{A}$ é um ideal primo de \mathcal{A} e \mathcal{A} é Dedekind segue que $P \cap \mathcal{A}$ é um ideal maximal de \mathcal{A} e, assim, $\frac{\mathcal{A}}{P \cap \mathcal{A}}$ é um corpo. Seja a aplicação $\varphi : \mathcal{A} \xrightarrow{i} \mathcal{O}_{\mathbb{L}} \xrightarrow{\pi} \frac{\mathcal{O}_{\mathbb{L}}}{P}$, onde i é a inclusão e π é a projeção. Temos que

$$\frac{\mathcal{A}}{P \cap \mathcal{A}} \simeq \text{Im}(\varphi) \subset \frac{\mathcal{O}_{\mathbb{L}}}{P}.$$

Como $\mathcal{O}_{\mathbb{L}}$ é inteiro sobre \mathcal{A} , segue que $\frac{\mathcal{O}_{\mathbb{L}}}{P}$ é inteiro sobre $\frac{\mathcal{A}}{P \cap \mathcal{A}}$. Pela Proposição (1.5.2), temos que $\frac{\mathcal{O}_{\mathbb{L}}}{P}$ é um corpo. Portanto, P é maximal. ■

Lema 1.8.1 *Se \mathcal{A} é um anel de Dedekind que não é corpo, \mathbb{K} seu corpo de frações e M um ideal maximal de \mathcal{A} , então o conjunto $N = \{x \in \mathbb{K} : xM \subset \mathcal{A}\}$ é um ideal fracionário de \mathcal{A} .*

Demonstração: Seja M um ideal maximal de \mathcal{A} . Como \mathcal{A} não é um corpo, segue que $M \neq \{0\}$. Consideremos $N = \{x \in \mathbb{K} : xM \subset \mathcal{A}\}$. Temos que N é um ideal fracionário, pois N é um \mathcal{A} -módulo tal que $N \subseteq \mathbb{K}$ e se $c \in M$, $c \neq 0$, temos que $cN \subseteq \mathcal{A}$. ■

Proposição 1.8.1 *Se \mathcal{A} é um anel de Dedekind que não é um corpo e \mathbb{K} é o seu corpo de frações, então todo ideal maximal M de \mathcal{A} é inversível.*

Demonstração: Considere o ideal fracionário

$$N = \{x \in \mathbb{K} : xM \subset \mathcal{A}\}.$$

Vamos mostrar que $NM = \mathcal{A}$. Pela definição de N , temos $NM \subset \mathcal{A}$. Por outro lado, $\mathcal{A} \subset N$, pois M é um ideal de \mathcal{A} . Assim, $M = M\mathcal{A} \subset MN \subset \mathcal{A}$. Como M é maximal, segue que $M = NM$ ou $NM = \mathcal{A}$. Suponhamos que $M = NM$ e consideremos $\alpha \in N$. Assim, $\alpha M \subset M$, $\alpha^2 M \subset \alpha M \subset M$ e $\alpha^n M \subset M$, para todo $n \in \mathbb{N}$. Agora, se $d \in M$, $d \neq 0$, então, $d\alpha^n \in \mathcal{A}$, $\forall n$. Portanto, $\mathcal{A}[\alpha]$ é um ideal fracionário. Como \mathcal{A} é noetheriano, pela Proposição (1.7.1), segue que $\mathcal{A}[\alpha]$ é um \mathcal{A} -módulo finitamente gerado. Pelo Teorema (1.5.1), segue que α é inteiro sobre \mathcal{A} . Sendo \mathcal{A} integralmente fechado, segue que $\alpha \in \mathcal{A}$. Assim, $N \subset \mathcal{A}$ e como $\mathcal{A} \subset N$ segue que $N = \mathcal{A}$. Falta mostrar que essa igualdade é impossível. Seja $a \in M$. Pela Proposição (1.2.4), temos que $\langle a \rangle = a\mathcal{A} \supset P_1 P_2 \cdots P_n$, onde os P_i 's são ideais primos não nulos de \mathcal{A} , com n o menor valor possível. Assim, $M \supset a\mathcal{A} \supset P_1 P_2 \cdots P_n$. Pelo Lema (1.1.4), M contém um dos P_i 's, para algum $i = 1, \dots, n$. Sem perda de generalidade, digamos que seja P_1 , isto é, $M \supset P_1$. Como \mathcal{A} é Dedekind, segue que $M = P_1$, pois P_1 é maximal. Agora, se $Q = P_2 \cdots P_n$, então $a\mathcal{A} \supset MQ$ e $a\mathcal{A} \not\supset Q$, pela minimalidade de n . Assim, existe $b \in Q$ e $b \notin \langle a \rangle$ tal que $Mb \subset \langle a \rangle$.

Logo, $\frac{b}{a}M \subseteq \mathcal{A}$ e assim, pela definição de N , temos que $\frac{b}{a} \in N$. Como $b \notin \langle a \rangle$, segue que $\frac{b}{a} \notin \mathcal{A}$. Assim, $N \neq \mathcal{A}$. Portanto, $MN = \mathcal{A}$. ■

Teorema 1.8.2 *Se \mathcal{A} é um anel de Dedekind que não é um corpo, então todo ideal fracionário I não nulo de \mathcal{A} é escrito de modo único como um produto de ideais primos de \mathcal{A} , isto é, $I = \prod_{i=1}^n P_i^{e_i}$, onde e_1, \dots, e_n são inteiros e P_i 's são ideais primos não nulos de \mathcal{A} .*

Demonstração: Se I é um ideal fracionário de \mathcal{A} , então existe $d \in \mathcal{A} - \{0\}$ tal que $dI \subseteq \mathcal{A}$. Como $I = (dI)(d\mathcal{A})^{-1}$, é suficiente mostrar o resultado para ideais inteiros. Seja F a família dos ideais inteiros de \mathcal{A} , não nulos, que não são um produto de ideais primos de \mathcal{A} . Suponhamos que $F \neq \emptyset$. Como \mathcal{A} é noetheriano, segue que F tem um elemento maximal M . Temos que $M \neq \mathcal{A}$, então $M \subseteq P$, onde P é um ideal maximal de \mathcal{A} . Pela Proposição (1.8.1), temos que $Q = \{x \in \mathbb{K} : xP \subset \mathcal{A}\}$ é tal que $PQ = \mathcal{A}$. Como $M \subseteq P$ segue que $MQ \subseteq PQ = \mathcal{A}$. Além disso, como $\mathcal{A} \subset Q$, segue que $M = MA \subset MQ \subset \mathcal{A}$. Além disso, $M \subsetneq MQ$, pois se $M = MQ$ e se $\alpha \in Q$, então $\alpha M \subset M$, $\alpha^2 M \subset \alpha M \subset M$ e $\alpha^n M \subset M$, para todo $n \in \mathbb{N}$. Assim, se $d \in M - \{0\}$, então $d\alpha^n \in M \subseteq \mathcal{A}$, $\forall n$. Portanto, $\mathcal{A}[\alpha]$ é um ideal fracionário de \mathcal{A} . Como \mathcal{A} é noetheriano, pela Proposição (1.7.1), segue que $\mathcal{A}[\alpha]$ é um \mathcal{A} -módulo finitamente gerado. Pelo Teorema (1.5.1), segue que α é inteiro sobre \mathcal{A} e, sendo \mathcal{A} integralmente fechado, segue que $\alpha \in \mathcal{A}$. Portanto, $Q \subset \mathcal{A}$ e assim $Q = \mathcal{A}$. Mas isso é impossível, pois se $Q = \mathcal{A}$, então $P = P\mathcal{A} = PQ = \mathcal{A}$, o que é um absurdo, pois P é um ideal primo. Pela maximalidade de M e como $M \subsetneq MQ$, temos que $MQ \notin F$, ou seja, $MQ = P_1 \cdots P_n$, onde P_i 's, para $i = 1, \dots, n$, são ideais primos de \mathcal{A} . Multiplicando por P ambos os lados, temos que $M = P_1 \cdots P_n P$, o que é um absurdo, pois $M \in F$. Portanto, $F = \emptyset$. Logo, todo ideal de \mathcal{A} é escrito como produto de ideais primos de \mathcal{A} . ■

Observação 1.8.1 *Notemos que se M for um ideal inteiro de \mathcal{A} , então os e_i 's, $i = 1, \dots, n$ são inteiros positivos. Já se M for fracionário podem haver expoentes negativos. O expoente negativo indica o inverso do ideal primo e este inverso sempre existe, visto que num anel de Dedekind todo ideal primo não nulo é maximal e, pela Proposição (1.8.1), todo ideal maximal é inversível.*

Corolário 1.8.1 *Se \mathcal{A} é um anel de Dedekind que não é um corpo, então todo ideal fracionário de \mathcal{A} é inversível.*

Demonstração: Pela Proposição (1.8.1), temos que todo ideal maximal M de \mathcal{A} é inversível. Seja I um ideal fracionário de \mathcal{A} . Pelo Teorema (1.8.2), temos que $I = \prod_{i=1}^n P_i^{e_i}$, onde P_i 's são

ideais primos de \mathcal{A} e e'_i s são inteiros. Como \mathcal{A} é um anel de Dedekind, temos que todo ideal primo de \mathcal{A} é maximal, logo todo ideal primo de \mathcal{A} é inversível. Agora, se Q_i é o inverso de P_i , para todo $i = 1, \dots, n$, então $J = \prod_{i=1}^n Q_i^{e_i}$ é um ideal fracionário de \mathcal{A} tal que $IJ = \mathcal{A}$. ■

Corolário 1.8.2 *Se $\mathcal{A} = \mathbb{Z}$, $\mathbb{K} = \mathbb{Q}$ e \mathbb{L} é uma extensão finita de \mathbb{Q} , então todo ideal fracionário de $\mathcal{O}_{\mathbb{L}}$ é escrito de forma única como um produto de ideais primos não nulos de $\mathcal{O}_{\mathbb{L}}$.*

Demonstração: Vimos que $\mathcal{O}_{\mathbb{L}}$ é um anel de Dedekind e não é um corpo. Logo, o resultado segue do Teorema (1.8.2). ■

1.9 Norma de um Ideal

Nesta seção, apresentamos os conceitos de norma de um ideal inteiro e de um ideal fracionário, juntamente com suas principais propriedades. Para isto, sejam \mathbb{K} um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de \mathbb{K} sobre \mathbb{Z} .

Definição 1.9.1 *Seja I um ideal inteiro não nulo de $\mathcal{O}_{\mathbb{K}}$. A **norma** de I é definida como a cardinalidade do anel quociente $\mathcal{O}_{\mathbb{K}}/I$, isto é,*

$$N(I) = \# \left(\frac{\mathcal{O}_{\mathbb{K}}}{I} \right).$$

Proposição 1.9.1 *Se $\alpha \in \mathcal{O}_{\mathbb{K}}$; $\alpha \neq 0$ e $I = \alpha\mathcal{O}_{\mathbb{K}}$ é um ideal de $\mathcal{O}_{\mathbb{K}}$, então $N(I) = \# \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha} \right) = |N_{\mathbb{K}|\mathbb{Q}}(\alpha)|$.*

Demonstração: Como $\alpha \in \mathcal{O}_{\mathbb{K}}$ e $\alpha \neq 0$, segue, pelo Corolário (1.5.5), que $N_{\mathbb{K}|\mathbb{Q}}(\alpha) \in \mathbb{Z}$. Pelo Corolário (1.5.6), temos que $\mathcal{O}_{\mathbb{K}}$ é um \mathbb{Z} -módulo livre de posto n . Como $\varphi : \mathcal{O}_{\mathbb{K}} \rightarrow \mathcal{O}_{\mathbb{K}}\alpha$, definida por $\varphi(a) = a\alpha$, onde $\alpha \in \mathcal{O}_{\mathbb{K}}$, é um isomorfismo, segue que $\mathcal{O}_{\mathbb{K}}\alpha$ é um \mathbb{Z} -módulo livre de posto n . Como \mathbb{Z} é um anel principal e $\mathcal{O}_{\mathbb{K}}$ é um \mathbb{Z} -módulo livre segue, pelo Teorema (1.2.1), que existe uma \mathbb{Z} -base $\{e_1, \dots, e_n\}$ de $\mathcal{O}_{\mathbb{K}}$ e inteiros c_1, \dots, c_n tal que $\{c_1e_1, \dots, c_n e_n\}$ é \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}}\alpha$. A aplicação $\psi : \mathcal{O}_{\mathbb{K}} \rightarrow \frac{\mathbb{Z}}{c_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{c_n\mathbb{Z}}$, definida por $\psi(\sum_{i=1}^n a_i e_i) = (\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n)$, é um homomorfismo sobrejetor e $\text{Ker}(\psi) = \mathcal{O}_{\mathbb{K}}\alpha$, pois $a \in \text{Ker}(\psi)$ se, e somente se, $\psi(a) = \bar{0}$ se, e somente se, $\bar{a}_i = \bar{0}$, para $i = 1, \dots, n$, se, e somente se, $a_i \in c_i\mathbb{Z}$, se, e somente se, c_i divide a_i se, e somente se, $a = \sum_{i=1}^n a_i e_i = \sum_{i=1}^n b_i c_i e_i \in \mathcal{O}_{\mathbb{K}}\alpha$. Assim,

$$\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha} \simeq \frac{\mathbb{Z}}{c_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{c_n\mathbb{Z}}.$$

Logo $\# \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha} \right) = c_1 c_2 \dots c_n$. Seja a aplicação \mathbb{Z} -linear $\mu : \mathcal{O}_{\mathbb{K}} \longrightarrow \mathcal{O}_{\mathbb{K}}\alpha$, definida por $\mu(e_i) = c_i e_i$, para $i = 1, \dots, n$. Logo, $\mu(e_1) = c_1 e_1 + 0e_2 + \dots + 0e_n, \dots, \mu(e_n) = 0e_1 + \dots + c_n e_n$ e $\det(\mu) = c_1 c_2 \dots c_n$. Por outro lado, temos que $B = \{c_1 e_1, \dots, c_n e_n\}$ e $C = \{\alpha e_1, \dots, \alpha e_n\}$ são \mathbb{Z} -bases de $\mathcal{O}_{\mathbb{K}}\alpha$. Portanto existe um automorfismo $\varphi : \mathcal{O}_{\mathbb{K}}\alpha \longrightarrow \mathcal{O}_{\mathbb{K}}\alpha$ tal que $\varphi(c_i e_i) = \alpha e_i$, para $i = 1, \dots, n$. Como a matriz mudança de base é inversível, segue que $\det(\varphi)$ é inversível em \mathbb{Z} , isto é, $\det(\varphi) = \pm 1$. Também, $(\varphi \circ \mu)(e_i) = \varphi(\mu(e_i)) = \varphi(c_i e_i) = \alpha e_i$, para $i = 1, \dots, n$. Assim, $(\varphi \circ \mu)(a) = \alpha a$, para todo $a \in \mathcal{O}_{\mathbb{K}}$. Finalmente, pela Definição (1.4.1), temos que $N_{\mathbb{K}|\mathbb{Q}}(\alpha) = \det(\varphi \circ \mu) = \det(\varphi) \det(\mu) = \pm 1 c_1 c_2 \dots c_n = \pm \# \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha} \right)$. Portanto, $|N(\alpha)| = \# \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha} \right) = N(I)$. ■

Proposição 1.9.2 *Se I é um ideal inteiro não nulo de $\mathcal{O}_{\mathbb{K}}$, então $N(I)$ é finita.*

Demonstração: Se $\alpha \in I$ é um elemento não nulo, então $\mathcal{O}_{\mathbb{K}}\alpha \subset I$. Consideremos a aplicação

$$\varphi : \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha} \right) \longrightarrow \left(\frac{\mathcal{O}_{\mathbb{K}}}{I} \right)$$

$$x + \mathcal{O}_{\mathbb{K}}\alpha \longmapsto x + I.$$

Temos que φ é um homomorfismo sobrejetor e $\text{Ker}(\varphi) = \left(\frac{I}{\mathcal{O}_{\mathbb{K}}\alpha} \right)$. De fato, $x + \mathcal{O}_{\mathbb{K}}\alpha \in \text{Ker}(\varphi)$ se, e somente se, $\varphi(x + \mathcal{O}_{\mathbb{K}}\alpha) = x + I = \bar{0}$ se, e somente se, $x \in I$. Desta forma, pelo Teorema (1.1.1), segue que

$$\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha} \right) / \left(\frac{I}{\mathcal{O}_{\mathbb{K}}\alpha} \right) \simeq \left(\frac{\mathcal{O}_{\mathbb{K}}}{I} \right).$$

Assim, segue que

$$\# \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha} \right) = \# \left(\frac{\mathcal{O}_{\mathbb{K}}}{I} \right) \# \left(\frac{I}{\mathcal{O}_{\mathbb{K}}\alpha} \right).$$

Pela Proposição (1.9.1), temos que $\# \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha} \right)$ é finito. Portanto, $\# \left(\frac{\mathcal{O}_{\mathbb{K}}}{I} \right)$ é finito. ■

Proposição 1.9.3 *Se I e J são ideais inteiros não nulos de $\mathcal{O}_{\mathbb{K}}$, então $N(IJ) = N(I)N(J)$.*

Demonstração: Como $\mathcal{O}_{\mathbb{K}}$ é um anel de Dedekind e J é um ideal inteiro de $\mathcal{O}_{\mathbb{K}}$, pelo Teorema (1.8.2), segue que $J = \prod_{i=1}^n P_i^{e_i}$, onde os P_i 's são ideais primos não nulos de $\mathcal{O}_{\mathbb{K}}$ e $e_i \geq 0$, $i = 1, \dots, n$. Além disso, como $\mathcal{O}_{\mathbb{K}}$ é um domínio de Dedekind, segue que os ideais P_i 's são maximais. Seja $P_i = M$, para algum $i = 1, \dots, n$. Por indução sobre o número de fatores, é suficiente provar que $N(IM) = N(I)N(M)$. Segue, da definição de norma de ideal, que a

igualdade anterior se verifica se, e somente se,

$$\# \left(\frac{\mathcal{O}_{\mathbb{K}}}{IM} \right) = \# \left(\frac{\mathcal{O}_{\mathbb{K}}}{I} \right) \# \left(\frac{\mathcal{O}_{\mathbb{K}}}{M} \right).$$

Temos que o homomorfismo $\phi : \frac{\mathcal{O}_{\mathbb{K}}}{IM} \rightarrow \frac{\mathcal{O}_{\mathbb{K}}}{I}$, definido por $\phi(x + IM) = x + I$, é sobrejetor e $\text{Ker}(\phi) = \frac{I}{IM}$. Assim, pelo Teorema (1.1.1), temos que $\left(\frac{\mathcal{O}_{\mathbb{K}}}{IM} \right) / \left(\frac{I}{IM} \right) \simeq \left(\frac{\mathcal{O}_{\mathbb{K}}}{I} \right)$. Logo,

$$\# \left(\frac{\mathcal{O}_{\mathbb{K}}}{IM} \right) = \# \left(\frac{\mathcal{O}_{\mathbb{K}}}{I} \right) \# \left(\frac{I}{IM} \right).$$

Podemos, então, concluir que $N(IM) = N(I)N(M)$ se verifica se, e somente se, $\# \left(\frac{\mathcal{O}_{\mathbb{K}}}{M} \right) = \# \left(\frac{I}{IM} \right)$. Agora, temos que $\frac{I}{IM}$ é um espaço vetorial sobre $\frac{\mathcal{O}_{\mathbb{K}}}{M}$ mediante as operações:

$$\begin{aligned} + : \frac{I}{IM} \times \frac{I}{IM} &\longrightarrow \frac{I}{IM} & \cdot : \frac{\mathcal{O}_{\mathbb{K}}}{M} \times \frac{I}{IM} &\longrightarrow \frac{I}{IM} \\ (x + IM, y + IM) &\longrightarrow (x + y) + IM & (\alpha + M, x + IM) &\longrightarrow (\alpha x) + IM. \end{aligned}$$

Além disso, temos que os $\frac{\mathcal{O}_{\mathbb{K}}}{M}$ -submódulos de $\frac{I}{IM}$ são ideais e são do tipo $\frac{B}{IM}$, onde B é um ideal tal que $IM \subseteq B \subseteq I$. Mas, como todo ideal num domínio de Dedekind admite inverso, segue que $I^{-1}IM \subseteq I^{-1}B \subseteq I^{-1}I$, ou seja, $M \subseteq I^{-1}B \subseteq \mathcal{O}_{\mathbb{K}}$. Como M é maximal, segue que $M = I^{-1}B$ ou $I^{-1}B = \mathcal{O}_{\mathbb{K}}$. Assim, $IM = B$ ou $B = I$. Portanto, não existe B tal que $IM \subsetneq B \subsetneq I$. Assim, os $\frac{\mathcal{O}_{\mathbb{K}}}{M}$ -submódulos de $\frac{I}{IM}$, ou os subespaços do espaço vetorial $\frac{I}{IM}$, são apenas os triviais. Portanto, $\dim_{\frac{\mathcal{O}_{\mathbb{K}}}{M}} \frac{I}{IM} = 1$ e, deste modo, $\# \left(\frac{\mathcal{O}_{\mathbb{K}}}{M} \right) = \# \left(\frac{I}{IM} \right)$, o que implica que $N(IM) = N(I)N(M)$. ■

Proposição 1.9.4 *Se I é um ideal inteiro não nulo de $\mathcal{O}_{\mathbb{K}}$, então:*

- (1) - $N(I) = 1$ se, e somente se, $I = \mathcal{O}_{\mathbb{K}}$.
- (2) - Se $N(I)$ for um número primo então o ideal I é primo.

Demonstração: (1) - Temos que $N(I) = 1$ se, e somente se, $\# \left(\frac{\mathcal{O}_{\mathbb{K}}}{I} \right) = 1$ se, e somente se, $I = \mathcal{O}_{\mathbb{K}}$.

(2) - Suponhamos que I não seja um ideal primo. Assim, $I = \mathcal{O}_{\mathbb{K}}$ ou $I = Q_1Q_2$, onde Q_1, Q_2 são ideais não nulos distintos de $\mathcal{O}_{\mathbb{K}}$. Se $I = \mathcal{O}_{\mathbb{K}}$, pelo item (1), temos que $N(I) = 1$, o que é contra a hipótese. Se $I = Q_1Q_2$ temos, pela Proposição (1.9.3), que $N(I) = N(Q_1)N(Q_2)$ e, como por hipótese, $N(I) = p$, p primo, segue que $N(Q_1) = 1$ e $N(Q_2) = p$ ou $N(Q_1) = p$ e

$N(Q_2) = 1$. Logo, $Q_1 = \mathcal{O}_{\mathbb{K}}$ ou $Q_2 = \mathcal{O}_{\mathbb{K}}$, o que é contra a hipótese. Portanto, I é um ideal primo de $\mathcal{O}_{\mathbb{K}}$. ■

Proposição 1.9.5 *Se I é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$ tal que $\{w_1, \dots, w_n\}$ seja uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}}$ e $\{e_1 w_1, \dots, e_n w_n\}$ é uma \mathbb{Z} -base de I , onde e_1, \dots, e_n são inteiros não nulos, então $N(I) = |e_1 \cdots e_n|$.*

Demonstração: Consideremos a aplicação:

$$\psi : \mathcal{O}_{\mathbb{K}} \longrightarrow \frac{\mathbb{Z}}{e_1 \mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{e_n \mathbb{Z}}$$

$$\sum_{i=1}^n a_i w_i \longmapsto (a_1 + e_1 \mathbb{Z}, \dots, a_n + e_n \mathbb{Z}).$$

Temos que ψ é um homomorfismo sobrejetor. Agora, $\text{Ker}(\psi) = I$. De fato, se $x = \sum_{i=1}^n a_i w_i \in \text{Ker}(\psi)$, então $\psi(x) = (a_1 + e_1 \mathbb{Z}, \dots, a_n + e_n \mathbb{Z}) = (0 + e_1 \mathbb{Z}, \dots, 0 + e_n \mathbb{Z})$. Logo, segue que $a_i \in e_i \mathbb{Z}$, para todo $i = 1, \dots, n$ e, assim, existem $b_1, \dots, b_n \in \mathbb{Z}$ tal que $a_i = e_i b_i$, para todo i , o que implica que $x = \sum_{i=1}^n a_i w_i = \sum_{i=1}^n b_i e_i w_i \in I$. Portanto, $\text{Ker}(\psi) \subset I$. Analogamente, se $x \in I$, então $x = \sum_{i=1}^n b_i e_i w_i$; $b_i \in \mathbb{Z}$. Desta forma, $\psi(x) = (b_1 e_1 + e_1 \mathbb{Z}, \dots, b_n e_n + e_n \mathbb{Z}) = (0 + e_1 \mathbb{Z}, \dots, 0 + e_n \mathbb{Z})$, o que mostra que $I \subset \text{Ker}(\psi)$. Pelo Teorema (1.1.1), temos que $\frac{\mathcal{O}_{\mathbb{K}}}{I} \simeq \frac{\mathbb{Z}}{e_1 \mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{e_n \mathbb{Z}}$. Portanto, $N(I) = |\mathcal{O}_{\mathbb{K}}/I| = |e_1 \cdots e_n|$. ■

Proposição 1.9.6 *Seja $\bar{\cdot} : \mathbb{K} \longrightarrow \mathbb{K}$ a conjugação complexa. Se I é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então $N(I) = N(\bar{I})$.*

Demonstração: Consideremos a aplicação:

$$\psi : \left(\frac{\mathcal{O}_{\mathbb{K}}}{I} \right) \longrightarrow \left(\frac{\mathcal{O}_{\mathbb{K}}}{\bar{I}} \right)$$

$$x + I \longmapsto \bar{x} + \bar{I}.$$

Temos que ψ está bem definida. De fato, primeiro notemos que se $x \in \mathcal{O}_{\mathbb{K}}$, então $\bar{x} \in \mathcal{O}_{\mathbb{K}}$. Agora, se $x + I = y + I$, então $x - y \in I$. Logo, $\overline{x - y} \in \bar{I}$. Assim, $\bar{x} + \bar{I} = \bar{y} + \bar{I}$. Além disso, ψ é um homomorfismo sobrejetor, pois se $\bar{x} + \bar{I} \in \mathcal{O}_{\mathbb{K}}/\bar{I}$, então existe $x = \bar{x} \in \mathcal{O}_{\mathbb{K}}$ tal que $\psi(x + I) = \bar{x} + \bar{I}$. Notemos também que ψ é injetora, pois se $\bar{x} + \bar{I} = \bar{y} + \bar{I}$, então $\bar{x} - \bar{y} \in \bar{I}$ e,

assim, $x - y \in I$. Logo, $x + I = y + I$. Portanto, ψ é um isomorfismo. Desta forma, temos que $N(I) = \# \left(\frac{\mathcal{O}_{\mathbb{K}}}{I} \right) = \# \left(\frac{\mathcal{O}_{\mathbb{K}}}{\bar{I}} \right) = N(\bar{I})$. ■

Consideremos, agora, I um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$. Temos que existe $d \in \mathcal{O}_{\mathbb{K}} - \{0\}$ e R um ideal inteiro de $\mathcal{O}_{\mathbb{K}}$ tal que $dI = R$. Vamos definir a norma do ideal fracionário I .

Definição 1.9.2 *Seja I um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$ tal que $dI = R$, onde R é um ideal inteiro de $\mathcal{O}_{\mathbb{K}}$ e $d \in \mathcal{O}_{\mathbb{K}} - \{0\}$. Definimos a **norma do ideal fracionário** I como*

$$N(I) = N(R)N_{\mathbb{K}|\mathbb{Q}}(d^{-1}),$$

onde d^{-1} é o inverso multiplicativo de d .

Proposição 1.9.7 *Se I, J são ideais fracionários não nulos de $\mathcal{O}_{\mathbb{K}}$, então $N(IJ) = N(I)N(J)$.*

Demonstração Como I e J são ideais fracionários de $\mathcal{O}_{\mathbb{K}}$, segue que existem $a, b \in \mathcal{O}_{\mathbb{K}} - \{0\}$ e R, S ideais inteiros de $\mathcal{O}_{\mathbb{K}}$ tais que $I = a^{-1}R$ e $J = b^{-1}S$. Isto implica que $IJ = \frac{RS}{ab}$. Assim, segue que $N(IJ) = N(RS)N_{\mathbb{K}|\mathbb{Q}}((ab)^{-1}) = N(R)N(S)N_{\mathbb{K}|\mathbb{Q}}(a^{-1})N_{\mathbb{K}|\mathbb{Q}}(b^{-1})$, onde a última igualdade segue da Proposição (1.9.3) e das propriedades da norma de um elemento. Logo,

$$N(IJ) = [N(R)N_{\mathbb{K}|\mathbb{Q}}(a^{-1})][N(S)N_{\mathbb{K}|\mathbb{Q}}(b^{-1})] = N(I)N(J),$$

o que prova a proposição. ■

Proposição 1.9.8 *Se I é um ideal fracionário não nulo de $\mathcal{O}_{\mathbb{K}}$, então $N(I)$ é finita.*

Demonstração Temos, por definição, que se $I = d^{-1}R$, com $d \in \mathcal{O}_{\mathbb{K}} - \{0\}$ e R um ideal inteiro de $\mathcal{O}_{\mathbb{K}}$, então $N(I) = N(R)N_{\mathbb{K}|\mathbb{Q}}(d^{-1})$. Pela Proposição (1.9.2), temos que $N(R)$ é finita e como $N_{\mathbb{K}|\mathbb{Q}}(d^{-1})$ é finita, segue que $N(I)$ é finita. ■

Observação 1.9.1 *Como $\mathcal{O}_{\mathbb{K}}$ é um anel de Dedekind, todo ideal fracionário não nulo de $\mathcal{O}_{\mathbb{K}}$ é inversível. Assim, se I é um ideal fracionário não nulo de $\mathcal{O}_{\mathbb{K}}$, então existe um ideal fracionário I^{-1} de $\mathcal{O}_{\mathbb{K}}$ tal que $II^{-1} = \mathcal{O}_{\mathbb{K}}$. Desta forma, pela Proposição (1.9.7), temos que $N(I)N(I^{-1}) = N(II^{-1}) = N(\mathcal{O}_{\mathbb{K}}) = 1$. Logo, $N(I^{-1}) = (N(I))^{-1}$.*

1.10 Anéis de Frações

Nesta seção, apresentamos os conceitos básicos sobre anéis de frações. Para isto, sejam \mathcal{A} um domínio, \mathbb{K} seu corpo de frações e S um subconjunto de $\mathcal{A} - \{0\}$ que é fechado na multiplicação com $1 \in S$. Veremos algumas propriedades do subconjunto $S^{-1}\mathcal{A}$ de \mathbb{K} , que será definido a seguir. Entre as propriedades estudadas, destaca-se o fato de que se \mathcal{A} é um anel de Dedekind, então $S^{-1}\mathcal{A}$ também o é.

Proposição 1.10.1 *Seja S um subconjunto de $\mathcal{A} - \{0\}$ que é fechado na multiplicação com $1 \in S$ e $S^{-1}\mathcal{A} = \left\{ \frac{a}{s}, \text{ tal que } a \in \mathcal{A} \text{ e } s \in S \right\}$ um subconjunto de \mathbb{K} . Temos que:*

(1) - $S^{-1}\mathcal{A}$ é um anel comutativo.

(2) - $\mathcal{A} \subset S^{-1}\mathcal{A}$.

(3) - Se $S = \mathcal{A} - \{0\}$ então $S^{-1}\mathcal{A} = \mathbb{K}$.

(4) - Se $S = \{1\}$ ou S é formado somente pelas unidades de \mathcal{A} então $S^{-1}\mathcal{A} = \mathcal{A}$.

Demonstração: (1) - O fato de S ser fechado na multiplicação garante que $S^{-1}\mathcal{A}$ é fechado na multiplicação e na adição. Além disso, $S^{-1}\mathcal{A}$ com as operações de adição e multiplicação satisfaz as propriedades de anel. Mostremos, agora, que a multiplicação é comutativa. De fato, seja $x, y \in S^{-1}\mathcal{A}$, então $x = \frac{a_1}{s_1}$ e $y = \frac{a_2}{s_2}$, com $a_1, a_2 \in \mathcal{A}$ e $s_1, s_2 \in S$. Assim, $xy = \frac{a_1 a_2}{s_1 s_2} = \frac{a_2 a_1}{s_2 s_1} = yx$. Logo, temos que $S^{-1}\mathcal{A}$ é um anel comutativo.

(2) - Como, por definição, $1 \in S$, segue que para todo $x \in \mathcal{A}$, tem-se $x = \frac{x}{1} \in S^{-1}\mathcal{A}$. Portanto, $\mathcal{A} \subset S^{-1}\mathcal{A}$.

(3) - Temos que $\mathbb{K} = \left\{ \frac{a}{b}; a, b \in \mathcal{A} \text{ e } b \neq 0 \right\}$. Agora, se $S = \mathcal{A} - \{0\}$, então $S^{-1}\mathcal{A} = \left\{ \frac{a}{s}; a \in \mathcal{A} \text{ e } s \in \mathcal{A} - \{0\} \right\} = \left\{ \frac{a}{s}; a, s \in \mathcal{A} \text{ e } s \neq 0 \right\} = \mathbb{K}$.

(4) - Seja $S = \{u_1, \dots, u_r\}$ onde $u_i \in U(\mathcal{A})$ para todo $i = 1, \dots, r$. Temos que $S^{-1}\mathcal{A} = \left\{ \frac{a}{s}; a \in \mathcal{A} \text{ e } s \in S \subset U(\mathcal{A}) \right\} = \{a; a \in \mathcal{A}\} = \mathcal{A}$, pois $\frac{a}{s} = a, \forall s \in S$. ■

Definição 1.10.1 *Nas condições da Proposição (1.10.1), temos que o anel*

$$S^{-1}\mathcal{A} = \left\{ \frac{a}{s}, \text{ tal que } a \in \mathcal{A} \text{ e } s \in S \right\}$$

é chamado de anel de frações de \mathcal{A} com relação a S .

Exemplo 1.10.1 *Sejam $\mathcal{A} = \mathbb{Z}$, $\mathbb{K} = \mathbb{Q}$ e $S = \{x \in \mathcal{A} \text{ tal que } x = 2k + 1, \text{ para algum } k \in \mathbb{Z}\}$. Temos que $S \subset \mathcal{A} - \{0\}$, $1 \in S$ e S é fechado na multiplicação. O anel de frações de \mathcal{A} com relação a S é $S^{-1}\mathcal{A} = \left\{ \frac{a}{s}; a \in \mathbb{Z} \text{ e } s \in S \right\}$.*

Proposição 1.10.2 *Sejam \mathcal{A} um domínio, S um subconjunto de $\mathcal{A} - \{0\}$ fechado na multiplicação com $1 \in S$ e $\mathcal{A}' = S^{-1}\mathcal{A}$. Temos que:*

(1) - *Se $B' \subset \mathcal{A}'$ é um ideal de \mathcal{A}' , então $B' \cap \mathcal{A}$ é um ideal de \mathcal{A} e $(B' \cap \mathcal{A})\mathcal{A}' = B'$.*

(2) - *Se $P' \subset \mathcal{A}'$ é um ideal primo de \mathcal{A}' , então $P = P' \cap \mathcal{A}$ é um ideal primo de \mathcal{A} com $P \cap S = \emptyset$.*

(3) - *Se $P \subset \mathcal{A}$ é um ideal primo de \mathcal{A} tal que $P \cap S = \emptyset$, então $P\mathcal{A}' \subset \mathcal{A}'$ é um ideal primo de \mathcal{A}' e $P\mathcal{A}' \cap \mathcal{A} = P$.*

Demonstração: (1) - Como \mathcal{A} e \mathcal{A}' são anéis e $\mathcal{A} \subseteq \mathcal{A}'$, segue que se B' é um ideal de \mathcal{A}' , então $B' \cap \mathcal{A}$ é um ideal de \mathcal{A} . Mostremos que $(B' \cap \mathcal{A})\mathcal{A}' = B'$. Como $B' \cap \mathcal{A} \subseteq B'$, segue que $(B' \cap \mathcal{A})\mathcal{A}' \subseteq B'\mathcal{A}' = B'$. Por outro lado, se $x \in B' \subset \mathcal{A}'$, então $x = \frac{a}{s}$; $a \in \mathcal{A}$, $s \in S$. Mas, como $S \subset \mathcal{A} \subseteq \mathcal{A}'$ e B' é um ideal de \mathcal{A}' , segue que $sx = a \in B'$. Logo, $a \in B' \cap \mathcal{A}$. Assim, $x = \frac{a}{s} = a \frac{1}{s} \in (B' \cap \mathcal{A})\mathcal{A}'$. Desta forma, $B' \subseteq (B' \cap \mathcal{A})\mathcal{A}'$. Portanto, temos que $B' = (B' \cap \mathcal{A})\mathcal{A}'$.

(2) - Como \mathcal{A} e \mathcal{A}' são anéis e $\mathcal{A} \subseteq \mathcal{A}'$ segue, pela Proposição (1.1.3), que se P' é um ideal primo de \mathcal{A}' , então $P' \cap \mathcal{A}$ é um ideal primo de \mathcal{A} . Mostremos que $P \cap S = \emptyset$, onde $P = P' \cap \mathcal{A}$. Suponhamos que exista $s \in P \cap S$. Assim, $s \in P$ e $s \in S$. Como $P = P' \cap \mathcal{A} \subseteq P'$, segue que $s \in P'$ e $\frac{1}{s} \in \mathcal{A}'$, pois $s \in S$. Desta forma, $1 = s \frac{1}{s} \in P'\mathcal{A}' = P'$. Assim, $P' = \mathcal{A}'$, o que é um absurdo, pois P' é um ideal primo de \mathcal{A}' . Portanto, $P \cap S = \emptyset$.

(3) - Seja $P \subset \mathcal{A}$ um ideal primo de \mathcal{A} tal que $P \cap S = \emptyset$. Mostremos que $P\mathcal{A}'$ é um ideal primo de \mathcal{A}' . Temos que $P\mathcal{A}' = \left\{ \frac{p}{s}; p \in P \text{ e } s \in S \right\}$. De fato, temos que $\left\{ \frac{p}{s}; p \in P \text{ e } s \in S \right\} \subset P\mathcal{A}'$ e se $x \in P\mathcal{A}'$ então $x = \sum_{i=1}^n p_i \frac{a_i}{s_i} = \frac{p_1 a_1 (s_2 \cdots s_n) + \cdots + p_n a_n (s_1 \cdots s_{n-1})}{s_1 \cdots s_n} = \frac{p}{s}$, onde $p = p_1 a_1 (s_2 \cdots s_n) + \cdots + p_n a_n (s_1 \cdots s_{n-1}) \in P$ e $s_1 \cdots s_n \in S$. Agora, sejam $x = \frac{a}{s} \in \mathcal{A}'$ e $y = \frac{b}{t} \in \mathcal{A}'$ tal que $xy = \frac{ab}{st} \in P\mathcal{A}'$. Como $xy \in P\mathcal{A}'$, segue que $xy = \frac{ab}{st} = \frac{p}{u}$ com $p \in P$, $u \in S$. Logo, $abu = pst \in P$ e como P é um ideal primo, segue que $ab \in P$ ou $u \in P$. Mas, $u \in S$ e $S \cap P = \emptyset$, o que implica que $ab \in P$. Novamente, como P é primo, temos que $a \in P$ ou $b \in P$. Assim, $\frac{a}{s} \in P\mathcal{A}'$ ou $\frac{b}{t} \in P\mathcal{A}'$. Portanto, $P\mathcal{A}'$ é um ideal primo de \mathcal{A}' . Mostremos agora que $P\mathcal{A}' \cap \mathcal{A} = P$. Como $P \subset \mathcal{A}$ e $P \subset P\mathcal{A}'$, segue que $P \subset P\mathcal{A}' \cap \mathcal{A}$. Por outro lado, se $x \in P\mathcal{A}' \cap \mathcal{A}$, então $x \in P\mathcal{A}'$ e $x \in \mathcal{A}$. Como $x \in P\mathcal{A}'$, segue que $x = \frac{p}{s}$; $p \in P$ e $s \in S$, o que implica que $xs \in P$. Como P é primo e $s \notin P$, segue que $x \in P$. Portanto $P\mathcal{A}' \cap \mathcal{A} \subset P$. Desta forma, temos que $P\mathcal{A}' \cap \mathcal{A} = P$. ■

Proposição 1.10.3 *Sejam \mathcal{A} um domínio, S um subconjunto de $\mathcal{A} - \{0\}$ fechado na multiplicação com $1 \in S$ e $\mathcal{A}' = S^{-1}\mathcal{A}$. Temos que:*

(1) - A aplicação $\varphi : \{\text{Ideais de } \mathcal{A}'\} \longrightarrow \{\text{Ideais de } \mathcal{A}\}$, definida por $\varphi(B') = B' \cap \mathcal{A}$, é uma injeção crescente com relação a inclusão.

(2) - A aplicação $\psi : \{\text{Ideais primos de } \mathcal{A}'\} \longrightarrow \{\text{Ideais primos } P \text{ de } \mathcal{A}; P \cap S = \emptyset\}$, definida por $\psi(P') = P' \cap \mathcal{A}$, é uma bijeção crescente com relação a inclusão e a aplicação inversa é dada por ϕ onde $\phi(P) = P\mathcal{A}'$, com P ideal primo de \mathcal{A} tal que $P \cap S = \emptyset$.

Demonstração: Notemos que, pela Proposição (1.10.2), as aplicações φ e ψ , de (1) e (2), respectivamente, estão bem definidas.

(1) - Mostremos que φ é injetora e crescente. Sejam B'_1, B'_2 ideais de \mathcal{A}' tal que $\varphi(B'_1) = \varphi(B'_2)$. Assim, $B'_1 \cap \mathcal{A} = B'_2 \cap \mathcal{A}$, o que implica que $(B'_1 \cap \mathcal{A})\mathcal{A}' = (B'_2 \cap \mathcal{A})\mathcal{A}'$ e, pelo item (1) da Proposição (1.10.2), segue que $B'_1 = B'_2$. Agora, se $B'_1 \subseteq B'_2$, então $B'_1 \cap \mathcal{A} \subseteq B'_2 \cap \mathcal{A}$ e, assim, $\varphi(B'_1) \subseteq \varphi(B'_2)$.

(2) - De forma análoga ao que foi feito em (1), temos que ψ é uma injeção crescente. Mostremos que ϕ é a inversa de ψ . Pelo item (3) da Proposição (1.10.2), temos que ϕ está bem definida. Agora, notemos que se P é um ideal primo de \mathcal{A} tal que $P \cap S = \emptyset$, então

$$(\psi \circ \phi)(P) = \psi(\phi(P)) = \psi(P\mathcal{A}') = P\mathcal{A}' \cap \mathcal{A} = P,$$

onde a última igualdade segue do item (3) da Proposição (1.10.2). Também, se P' é um ideal primo de \mathcal{A}' , então

$$(\phi \circ \psi)(P') = \phi(\psi(P')) = \phi(P' \cap \mathcal{A}) = (P' \cap \mathcal{A})\mathcal{A}' = P',$$

onde a última igualdade segue do item (1) da Proposição (1.10.2). Desta forma, temos que $\psi = \phi^{-1}$ e assim, segue que ψ é uma bijeção crescente em relação a inclusão. ■

Corolário 1.10.1 *Com as mesmas notações da Proposição (1.10.3), se \mathcal{A} é um anel noetheriano, então $\mathcal{A}' = S^{-1}\mathcal{A}$ é um anel noetheriano.*

Demonstração: Consideremos a aplicação:

$$\varphi : \{\text{Ideais de } \mathcal{A}'\} \longrightarrow \{\text{Ideais de } \mathcal{A}\}$$

$$\varphi(B') \longmapsto B' \cap \mathcal{A}.$$

Seja $(B'_n)_{n>0}$ uma sequência crescente de ideais de \mathcal{A}' . Pelo item (1) da Proposição (1.10.3), temos que $(\varphi(B'_n))_{n>0}$ é uma sequência crescente de ideais de \mathcal{A} . Como \mathcal{A} é noetheriano, segue

que existe $n_0 \in \mathbb{N}$ tal que $\varphi(B'_n) = \varphi(B'_{n+1}), \forall n \geq n_0$. Novamente, pelo item (1) da Proposição (1.10.3), temos que φ é injetora. Desta forma, $B'_n = B'_{n+1}, \forall n \geq n_0$. Assim, $(B'_n)_{n>0}$ é estacionária, o que implica que \mathcal{A}' é noetheriano. ■

Corolário 1.10.2 *Se \mathcal{A} é um domínio de Dedekind, $P \subset \mathcal{A}$ um ideal primo, $S = \mathcal{A} - P$ e I um ideal de \mathcal{A} tal que $I = \prod_{i=1}^r P_i^{e_i}$, onde os P_i 's, para $i = 1, \dots, r$, são ideais primos de \mathcal{A} , então a decomposição do ideal $\mathcal{A}'I$ em produto de ideais primos de $\mathcal{A}' = S^{-1}\mathcal{A}$ é dada por $\mathcal{A}'I = \prod_{P_i \cap S = \emptyset} (\mathcal{A}'P_i)^{e_i}$.*

Demonstração: Como $I = \prod_{i=1}^r P_i^{e_i}$, segue que

$$\mathcal{A}'I = \mathcal{A}' \left(\prod_{i=1}^r P_i^{e_i} \right) = \prod_{i=1}^r \mathcal{A}'P_i^{e_i} = \prod_{i=1}^r (\mathcal{A}'P_i)^{e_i}.$$

Agora, se $P_i \cap S \neq \emptyset$, então $\mathcal{A}'P_i = \mathcal{A}'$. De fato, se $P_i \cap S \neq \emptyset$ então existe $s \in P_i \cap S$. Assim, $s \in P_i$ e $s \in S$. Logo $\frac{s}{s} \in \mathcal{A}'P_i$, o que implica que $1 \in \mathcal{A}'P_i$. Portanto, $\mathcal{A}'P_i = \mathcal{A}'$. Se $P_i \cap S = \emptyset$, pelo item (3) da Proposição (1.10.2), temos que $\mathcal{A}'P_i$ é um ideal primo de \mathcal{A}' , para $i = 1, \dots, r$. Portanto, $\mathcal{A}'I = \prod_{P_i \cap S = \emptyset} (\mathcal{A}'P_i)^{e_i}$ é a decomposição de $\mathcal{A}'I$ em um produto de ideais primos de \mathcal{A}' . ■

Proposição 1.10.4 *Sejam \mathcal{B} um domínio, $\mathcal{A} \subset \mathcal{B}$ um subanel e $S \subset \mathcal{A} - \{0\}$ um subconjunto com $1 \in S$ e fechado no produto. Se $\mathcal{O}_{\mathcal{B}}$ é o anel dos inteiros de \mathcal{B} sobre \mathcal{A} , então $\mathcal{O}_{\mathcal{B}'} = S^{-1}\mathcal{O}_{\mathcal{B}}$ é o anel dos inteiros de $\mathcal{B}' = S^{-1}\mathcal{B}$ sobre $\mathcal{A}' = S^{-1}\mathcal{A}$.*

Demonstração: Se $x \in \mathcal{O}_{\mathcal{B}'}$, então $x = \frac{b}{s}$ com $b \in \mathcal{O}_{\mathcal{B}}$ e $s \in S$. Como $\mathcal{O}_{\mathcal{B}}$ é inteiro sobre \mathcal{A} , segue que existem $a_i \in \mathcal{A}$, para $i = 0, 1, \dots, n-1$, não todos nulos, tal que

$$b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0.$$

Assim, dividindo a equação acima por s^n , obtemos que

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s} \left(\frac{b}{s}\right)^{n-1} + \dots + \frac{a_0}{s^n} = 0.$$

Como $\frac{a_i}{s^{n-i}} \in \mathcal{A}'$ e não são todos nulos, segue que $x = \frac{b}{s}$ é inteiro sobre \mathcal{A}' . Mostremos agora que todo elemento de \mathcal{B}' que é inteiro sobre \mathcal{A}' pertence a $\mathcal{O}_{\mathcal{B}'}$. Para isto, se $x \in \mathcal{B}'$ é inteiro

sobre \mathcal{A}' , então existem $\frac{a_i}{s_i} \in \mathcal{A}'$, para $i = 0, 1, \dots, n-1$, não todos nulos, tal que

$$x^n + \frac{a_{n-1}}{s_{n-1}}x^{n-1} + \dots + \frac{a_0}{s_0} = 0.$$

Multiplicando a igualdade acima por s^n , com $s = s_0s_1 \dots s_{n-1}$, obtemos que $(sx)^n + a_{n-1}(s_0s_1 \dots s_{n-2})(sx)^{n-1} + \dots + a_0(s_1 \dots s_n)s^{n-1} = (sx)^n + b_{n-1}(sx)^{n-1} + b_{n-2}(sx)^{n-2} + \dots + b_0$, onde $b_{n-j} = \frac{a_{n-j}s^j}{s_{n-j}} \in \mathcal{A}$, para $i = 1, \dots, n$, não são todos nulos. Logo, $sx \in \mathcal{O}_{\mathcal{B}}$ e assim $sx = b$, com $b \in \mathcal{O}_{\mathcal{B}}$. Portanto, $x = \frac{b}{s}$ onde $b \in \mathcal{O}_{\mathcal{B}}$ e $s \in S$. Desta forma, $x \in \mathcal{O}'_{\mathcal{B}}$. Portanto, concluímos que $\mathcal{O}'_{\mathcal{B}}$ é o anel de inteiros de \mathcal{B}' sobre \mathcal{A}' . ■

Corolário 1.10.3 *Se \mathcal{A} é um anel integralmente fechado e $S \subset \mathcal{A} - \{0\}$ um subconjunto com $1 \in S$ e fechado no produto, então $\mathcal{A}' = S^{-1}\mathcal{A}$ é integralmente fechado.*

Demonstração: Sejam \mathbb{K} o corpo de frações do anel \mathcal{A} e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de \mathbb{K} sobre \mathcal{A} . Como \mathcal{A} é integralmente fechado, temos que $\mathcal{A} = \mathcal{O}_{\mathbb{K}}$ e, assim, pela Proposição (1.10.4), temos que $\mathcal{O}'_{\mathbb{K}} = S^{-1}\mathcal{O}_{\mathbb{K}}$ é o anel dos inteiros de $\mathbb{K}' = S^{-1}\mathbb{K} = \mathbb{K}$ sobre $\mathcal{A}' = S^{-1}\mathcal{A}$. Agora, $\mathcal{O}'_{\mathbb{K}} = S^{-1}\mathcal{O}_{\mathbb{K}} = S^{-1}\mathcal{A} = \mathcal{A}'$. Portanto, \mathcal{A}' é integralmente fechado. ■

Teorema 1.10.1 *Se \mathcal{A} é um anel de Dedekind e $S \subset \mathcal{A} - \{0\}$ um subconjunto com $1 \in S$ e fechado no produto, então $\mathcal{A}' = S^{-1}\mathcal{A}$ é um anel de Dedekind.*

Demonstração: Temos pelos Corolários (1.10.1) e (1.10.3), que \mathcal{A}' é um anel noetheriano e integralmente fechado, respectivamente. Deste modo, falta mostrar que todo ideal primo não nulo de \mathcal{A}' é maximal. Seja $P' \subset \mathcal{A}'$ um ideal primo não nulo. Temos, pela Proposição (1.1.3), que $P' \cap \mathcal{A}$ é um ideal primo não nulo de \mathcal{A} e como \mathcal{A} é Dedekind, temos que $P' \cap \mathcal{A}$ é maximal. Pelo item (1) da Proposição (1.10.3), temos que se \mathcal{M} é um ideal de \mathcal{A}' tal que $P' \subseteq \mathcal{M}' \subseteq \mathcal{A}'$, então $\varphi(P') \subseteq \varphi(\mathcal{M}') \subseteq \varphi(\mathcal{A}')$. Como \mathcal{A} é Dedekind e $\varphi(P') = P' \cap \mathcal{A}$ é maximal, segue que $\varphi(P') = \varphi(\mathcal{M}')$ ou $\varphi(\mathcal{M}') = \varphi(\mathcal{A}')$. Como φ é injetora, segue que $P' = \mathcal{M}'$ ou $\mathcal{M}' = \mathcal{A}'$, o que implica que P' é maximal. Assim, temos que \mathcal{A}' é um anel de Dedekind. ■

Proposição 1.10.5 *Se \mathcal{A} é um domínio de Dedekind e $S \subset \mathcal{A}$ é um subconjunto tal que $S = \mathcal{A} - P$, onde $P \subset \mathcal{A}$ é um ideal primo, então $\mathcal{A}' = S^{-1}\mathcal{A}$ é principal. Mais ainda, existe $p \in \mathcal{A}'$ tal que os ideais de \mathcal{A}' são da forma $\langle p^n \rangle$, onde $n \in \mathbb{N}$.*

Demonstração: Temos que $P \subset \mathcal{A}$ é o único ideal primo não nulo de \mathcal{A} tal que $P \cap S = \emptyset$, pois se existisse um outro ideal primo $Q \subset \mathcal{A}$ tal que $Q \cap S = \emptyset$, teríamos que $Q \subset P$. Como

\mathcal{A} é Dedekind, segue que $Q = P$. Pelo item (2) da Proposição (1.10.3), temos que $P\mathcal{A}' = B$ é o único ideal primo de \mathcal{A}' . Mas, como \mathcal{A}' é Dedekind, segue, pelo Teorema (1.8.2), que todo ideal de \mathcal{A}' se fatora de forma única como produto de ideais primos de \mathcal{A}' . Assim, todo ideal de \mathcal{A}' é da forma B^n , onde $n \in \mathbb{N}$. Considere a seguinte sequência de ideais

$$\dots \subseteq B^n \subseteq B^{n-1} \subseteq \dots \subseteq B^2 \subseteq B \subseteq \mathcal{A}'.$$

Se $p \in B - B^2$ então $\langle p \rangle = B^{n_0}$, para algum $n_0 \in \mathbb{N}$, e $\langle p \rangle \not\subseteq B^2$. Logo, $n_0 = 1$ e, portanto, $\langle p \rangle = B$. Assim, todo ideal de \mathcal{A}' é da forma $B^n = \langle p^n \rangle$, com $n \in \mathbb{N}$. Portanto, \mathcal{A}' é principal. ■

Teorema 1.10.2 *Sejam \mathcal{A} um domínio, $S \subset \mathcal{A} - \{0\}$ um subconjunto, fechado no produto com $1 \in S$. Se M é um ideal maximal de \mathcal{A} tal que $M \cap S = \emptyset$, então $\mathcal{A}'/M\mathcal{A}' \simeq \mathcal{A}/M$.*

Demonstração: Se M é um ideal maximal de \mathcal{A} , então M também é um ideal primo de \mathcal{A} . Assim, pelo item (3) da Proposição (1.10.2), temos que $M\mathcal{A}'$ é um ideal primo de \mathcal{A}' . Considere a aplicação $\varphi : \mathcal{A} \xrightarrow{i} \mathcal{A}' \xrightarrow{\pi} \mathcal{A}'/M\mathcal{A}'$, onde i é a inclusão e π é a projeção. Temos que $\text{Ker}(\varphi) = M\mathcal{A}' \cap \mathcal{A}$, pois $\varphi(x) = \bar{0}$ se, e somente se, $x + M\mathcal{A}' = \bar{0}$. Isto equivale a $x \in M\mathcal{A}'$ e $x \in \mathcal{A}$. Portanto, $\text{Ker}(\varphi) = M\mathcal{A}' \cap \mathcal{A} = M$, onde a última igualdade segue do item (3) da Proposição (1.10.2). Falta mostrar que φ é sobrejetora. Para isto, se $\bar{x} \in \mathcal{A}'/M\mathcal{A}'$, então $\bar{x} = x + M\mathcal{A}'$, com $x = \frac{a}{s}$, $a \in \mathcal{A}$ e $s \in S$. Como $M \cap S = \emptyset$, segue que $s \notin M$ e, como M é maximal, segue que \mathcal{A}/M é um corpo. Logo, $\bar{s} = s + M \neq 0$ é inversível, ou seja, existe $\bar{b} \in \mathcal{A}/M$ tal que $\bar{s}\bar{b} = \bar{1}$. Assim, $sb - 1 \in M$. Deste modo, $\frac{a}{s} - ab = \frac{a}{s}(1 - sb) \in M\mathcal{A}'$, o que implica que $\frac{a}{s} + M\mathcal{A}' = ab + M\mathcal{A}'$, ou seja, $x + M\mathcal{A}' = ab + M\mathcal{A}'$. Desta forma, $\varphi(ab) = ab + M\mathcal{A}' = \bar{x}$. Portanto, φ é sobrejetora. Pelo Teorema (1.1.1), temos que $\mathcal{A}'/M\mathcal{A}' \simeq \mathcal{A}/M$. ■

Capítulo 2

Corpos Quadráticos e Ciclotômicos

Neste capítulo apresentamos os conceitos de corpos quadráticos e corpos ciclotômicos. Visto que um corpo de números é uma extensão finita de \mathbb{Q} , temos que os corpos quadráticos são corpos de números de grau 2 e os ciclotômicos são corpos de números gerados por uma raiz n -ésima primitiva da unidade. Focalizamos nosso estudo sobre algumas propriedades destes corpos que serão utilizadas nos próximos capítulos. Na Seção 2.1, apresentaremos os conceitos de corpos quadráticos e na Seção 2.2 os conceitos de corpos ciclotômicos.

2.1 Corpos Quadráticos

Nesta seção apresentamos o conceito de corpos quadráticos, encontramos o seu grupo de Galois, seu anel de inteiros e seu discriminante. Alguns resultados seguem sem demonstração por se tratarem de resultados clássicos de teoria algébrica dos números.

Definição 2.1.1 *Um corpo quadrático \mathbb{K} é uma extensão de \mathbb{Q} de grau 2.*

Proposição 2.1.1 *Todo corpo quadrático \mathbb{K} é da forma $\mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados.*

Demonstração: Pelo Teorema (1.3.2), temos que $\mathbb{K} = \mathbb{Q}(\alpha)$, para algum $\alpha \in \mathbb{K}$. Como $[\mathbb{K} : \mathbb{Q}] = 2$, segue que o polinômio minimal de α sobre \mathbb{Q} tem grau 2. Seja $p(x) = x^2 + bx + c = \min_{\mathbb{Q}} \alpha$. Resolvendo a equação quadrática $\alpha^2 + b\alpha + c = 0$, temos que $2\alpha = -b \pm \sqrt{b^2 - 4c}$. Desta maneira, $\mathbb{K} = \mathbb{Q}(\alpha) = \mathbb{Q}[\sqrt{b^2 - 4c}]$, e observando que $b^2 - 4c$ é um número racional da forma $\frac{u}{v} = \frac{uv}{v^2}$, com $u, v \in \mathbb{Z}$, $\text{mdc}(u, v) = 1$, temos que $\mathbb{Q}(\sqrt{b^2 - 4c}) = \mathbb{Q}(\sqrt{uv})$. Como $uv \in \mathbb{Z}$, segue que uv é fatorado em produtos de primos. Assim, $\mathbb{Q}(\sqrt{uv}) = \mathbb{Q}(\sqrt{d})$, onde d é inteiro livre de quadrados. ■

Exemplo 2.1.1 Seja $\mathbb{K} = \mathbb{Q}(i)$ um corpo quadrático. Temos que $\min_{\mathbb{Q}}(i) = x^2 + 1$. Logo, pela Proposição (2.1.1), temos que $\mathbb{K} = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$.

Teorema 2.1.1 ([3], pag. 35) Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, com $d \in \mathbb{Z}$ livre de quadrados e $d \not\equiv 0 \pmod{4}$.

(1) - Se $d \equiv 2$ ou $d \equiv 3 \pmod{4}$, então o anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ de \mathbb{K} sobre \mathbb{Z} é $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$ e uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}}$ é $\{1, \sqrt{d}\}$.

(2) - Se $d \equiv 1 \pmod{4}$, então o anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ de \mathbb{K} sobre \mathbb{Z} é $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ e uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}}$ é $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$. ■

Proposição 2.1.2 Seja d um inteiro livre de quadrados. Os homomorfismos de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ em \mathbb{C} são dados por $\{\sigma_1, \sigma_2\}$, onde $\sigma_1(\sqrt{d}) = \sqrt{d}$ e $\sigma_2(\sqrt{d}) = -\sqrt{d}$.

Demonstração: Segue do Teorema (1.3.3). ■

Observação 2.1.1 Segue da Proposição (2.1.2) que $\mathbb{Q}(\sqrt{d})|\mathbb{Q}$ é uma extensão de Galois.

Proposição 2.1.3 Seja d um inteiro livre de quadrados. O discriminante de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ sobre \mathbb{Q} é dado por:

(1) - $Disc(\mathbb{K}|\mathbb{Q}) = d$, se $d \equiv 1 \pmod{4}$;

(2) - $Disc(\mathbb{K}|\mathbb{Q}) = 4d$, se $d \equiv 2$ ou $3 \pmod{4}$.

Demonstração: Temos que:

(1) - Se $d \equiv 1 \pmod{4}$, então

$$Disc(\mathbb{K}|\mathbb{Q}) = D_{\mathbb{K}|\mathbb{Q}}\left(1, \frac{1+\sqrt{d}}{2}\right) = \left(\det \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1\left(\frac{1+\sqrt{d}}{2}\right) & \sigma_2\left(\frac{1+\sqrt{d}}{2}\right) \end{pmatrix}\right)^2 = d.$$

(2) - Se $d \equiv 2$ ou $3 \pmod{4}$, então

$$Disc(\mathbb{K}|\mathbb{Q}) = D_{\mathbb{K}|\mathbb{Q}}\left(1, \sqrt{d}\right) = \left(\det \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\sqrt{d}) & \sigma_2(\sqrt{d}) \end{pmatrix}\right)^2 = \left(\det \begin{pmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{pmatrix}\right)^2 = 4d,$$

o que prova a proposição. ■

Exemplo 2.1.2 Sejam $\mathbb{K}_1 = \mathbb{Q}(\sqrt{5})$ e $\mathbb{K}_2 = \mathbb{Q}(\sqrt{14})$. Como $5 \equiv 1 \pmod{4}$ e $14 \equiv 2 \pmod{4}$, pelo Teorema (2.1.1), temos que $\mathcal{O}_{\mathbb{K}_1} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ e $\mathcal{O}_{\mathbb{K}_2} = \mathbb{Z}[\sqrt{14}]$. Agora, pela Proposição (2.1.3), temos que $Disc(\mathbb{K}_1|\mathbb{Q}) = 5$ e $Disc(\mathbb{K}_2|\mathbb{Q}) = 4(14) = 56$.

2.2 Corpos Ciclotômicos

Nesta seção, apresentamos a definição de corpos ciclotômicos, encontramos o grau de uma extensão ciclotômica, seu grupo de Galois, seu anel de inteiros e seu discriminante. Além disso, veremos o subcorpo real maximal de um corpo ciclotômico e algumas de suas propriedades que serão utilizadas neste trabalho. Omitimos algumas demonstrações por se tratarem de resultados clássicos de teoria algébrica dos números e por algumas serem muito longas.

Definição 2.2.1 *Sejam $\zeta \in \mathbb{C}$ e $n \in \mathbb{N}^*$. Dizemos que ζ é uma **raiz n -ésima da unidade** se $\zeta^n = 1$.*

Observação 2.2.1 *Notemos que existem exatamente n raízes n -ésimas distintas da unidade. De fato, consideremos o polinômio $p(x) = x^n - 1$. Temos que toda raiz n -ésima da unidade é raiz de $p(x)$. Mas, $p(x)$ admite n raízes distintas, pois qualquer raiz de $p(x)$ não é raiz de $p'(x)$. Notemos também que o conjunto $\{\zeta_{n_k} = \cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n}), \text{ para } k = 0, 1, \dots, n-1\}$ contém as n raízes n -ésimas distintas da unidade e que este conjunto forma um grupo cíclico em relação a multiplicação com ζ_{n_1} um gerador.*

Definição 2.2.2 *Dizemos que ζ é uma **raiz n -ésima primitiva da unidade** se $\zeta^n = 1$ e $\zeta^m \neq 1$ para $1 < m < n$, ou seja, se ζ gera o grupo da raízes n -ésimas da unidade.*

Definição 2.2.3 *Seja ζ_n uma raiz n -ésima primitiva da unidade. Um **corpo ciclotômico** \mathbb{K} é uma extensão de \mathbb{Q} gerada por ζ_n , isto é, $\mathbb{K} = \mathbb{Q}(\zeta_n)$.*

Definição 2.2.4 *Chamamos de **n -ésimo polinômio ciclotômico** o polinômio*

$$\phi_n(x) = \prod_{i=1}^r (x - \eta_i),$$

onde η_i é uma raiz n -ésima primitiva da unidade, para $i = 1, \dots, r$.

Proposição 2.2.1 *Temos que $\phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d < n} \phi_d(x)}$, $n > 1$ e $\phi_1(x) = x - 1$.*

Demonstração: Sendo $f(x) = x^n - 1$, temos que suas raízes são $1, \omega, \omega^2, \dots, \omega^{n-1}$. Logo $x^n - 1 = (x - 1)(x - \omega) \dots (x - \omega^{n-1})$. Analisando as ordens de cada raiz de $f(x)$, e escrevendo todas de mesma ordem como um polinômio da forma $\phi_d(x) = \prod_{\text{ordem de } \omega=d} (x - \omega)$, temos que

$$x^n - 1 = \prod_{d|n} \phi_d(x). \quad \blacksquare$$

Exemplo 2.2.1 Se $n = p$, com p um número primo, então

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1$$

é o p -ésimo polinômio ciclotômico. Se $n = p^r$, com p um número primo e r um inteiro positivo, então

$$x^{p^r} - 1 = \phi_1(x)\phi_p(x)\phi_{p^2}(x)\cdots\phi_{p^{r-1}}(x)\phi_{p^r}(x) \text{ e}$$

$$x^{p^{r-1}} - 1 = \phi_1(x)\phi_p(x)\phi_{p^2}(x)\cdots\phi_{p^{r-1}}(x).$$

Logo $\phi_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = x^{(p-1)p^{r-1}} + x^{(p-2)p^{r-1}} + \cdots + x^{p^{r-1}} + 1$ é o p^r -ésimo polinômio ciclotômico.

Teorema 2.2.1 Se ζ_n é uma raiz n -ésima primitiva da unidade, então $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, onde φ é a função de Euler.

Demonstração: Seja $f(x)$ o polinômio minimal de ζ_n sobre \mathbb{Q} . Logo, $x^n - 1 = f(x)h(x)$, com $h(x) \in \mathbb{Q}[x]$. Pelo Lema de Gauss, temos que $f(x), h(x) \in \mathbb{Z}[x]$. Se p é um número primo tal que $p \nmid n$, então, ζ_n^p é uma raiz n -ésima primitiva da unidade. Logo, $(\zeta_n^p)^n - 1 = f(\zeta_n^p)h(\zeta_n^p)$, ou seja, $0 = f(\zeta_n^p)h(\zeta_n^p)$. Assim, se ζ_n^p não for raiz de $f(x)$, então ζ_n^p é raiz de $h(x)$ e, portanto, ζ_n é raiz de $h(x^p)$. Pela forma que tomamos $f(x)$, segue que $f(x) \mid h(x^p)$. Pelo Lema de Gauss, segue que $h(x^p) = f(x)g(x)$, com $g(x) \in \mathbb{Z}[x]$. Como consequência do pequeno Teorema de Fermat, temos que $a^p \equiv a \pmod{p}$, e assim, $h(x^p) \equiv h(x)^p \pmod{p}$. Portanto, $f(x)g(x) \equiv h(x)^p \pmod{p}$ o que é equivalente a $h(x)^p \equiv f(x)g(x) \pmod{p}$. Logo, $\bar{h}(\zeta_n)^p = \bar{0}$, pois ζ_n é raiz de $f(x)$. E recursivamente, chegamos que $\bar{h}(\zeta_n) = 0$. Portanto \bar{f} e \bar{h} tem uma raiz em comum. Assim, $x^n - \bar{1} = \bar{f}(x)\bar{h}(x)$ tem uma raiz múltipla. Logo, $n\lambda^{n-1} = \bar{0}$ e assim, para qualquer $\lambda \in \mathbb{Z}_p$, temos que $n\lambda^{n-1} = \bar{0}$. Como a característica de \mathbb{Z}_p é p , segue que $p \mid n$, o que contradiz o fato de termos suposto que $p \nmid n$. Portanto, ζ_n^p é raiz de $f(x)$, $\forall p \nmid n$ e $\text{mdc}(p, n) = 1$. Logo $\text{grau}(f(x)) \geq \text{grau}(\phi_n(x))$, pois toda raiz de $\phi_n(x)$ é raiz de $f(x)$, e como $f(x) \mid \phi_n(x)$, segue que $\text{grau}(\phi_n(x)) \geq \text{grau}(f(x))$. Portanto, $\text{grau}(\phi_n(x)) = \text{grau}(f(x)) = \varphi(n)$. ■

Observação 2.2.2 Pela demonstração do Teorema (2.2.1), notemos que o polinômio minimal de ζ_n é $\phi(n)$ e ele possui $\varphi(n)$ raízes distintas e estas são exatamente as raízes n -ésimas primitivas da unidade.

Teorema 2.2.2 ([7], pag. 11) Se ζ_n é uma raiz n -ésima primitiva da unidade, então o anel dos inteiros de $\mathbb{Q}(\zeta_n)$ sobre \mathbb{Z} é $\mathbb{Z}[\zeta_n]$ e uma \mathbb{Z} -base de $\mathbb{Z}[\zeta_n]$ é $\{1, \zeta_n, \dots, \zeta_n^{\varphi(n)-1}\}$. ■

Proposição 2.2.2 *Os homomorfismos de $\mathbb{Q}(\zeta_n)$ sobre \mathbb{C} são dados por $\{\sigma_i, \text{mdc}(i, n) = 1, i = 1, \dots, n-1, \sigma_i(\zeta) = \zeta^i\}$.*

Demonstração: Segue do Teorema (1.3.3). ■

Observação 2.2.3 *Segue da Proposição (2.2.2) que $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ é uma extensão de Galois, pois $[\mathbb{Q}(\zeta_n)|\mathbb{Q}] = \varphi(n) = |\mathbb{Z}_n^*|$. Além disso, $\text{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) = \{\sigma_i; \text{mdc}(i, n) = 1 \text{ e } \sigma_i(\zeta_n) = \zeta_n^i\}$.*

A seguir, veremos o cálculo do discriminante de corpos ciclotômicos para $n = p^r$, com p um número primo e r um inteiro positivo. O caso geral será feito no Capítulo 3, pois no momento ainda faltam ferramentas para fazê-lo.

Proposição 2.2.3 *Se p é um número primo ímpar e $\zeta = \zeta_{p^r}$ uma raiz p^r -ésima primitiva da unidade, com r um inteiro positivo, então o discriminante de $\mathbb{Q}(\zeta_{p^r})$ sobre \mathbb{Q} satisfaz*

$$D_{\mathbb{K}|\mathbb{Q}}(1, \zeta_{p^r}, \dots, \zeta_{p^r}^{\varphi(p^r)-1}) = \pm p^{p^{r-1}(r(p-1)-1)}.$$

Demonstração: Pela Proposição (1.6.3), temos que

$$D_{\mathbb{K}|\mathbb{Q}}(1, \zeta_{p^r}, \dots, \zeta_{p^r}^{\varphi(p^r)-1}) = \pm N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(f'(\zeta_{p^r})).$$

Derivando ambos os lados de $f(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1}$, temos que

$$f'(x) = \frac{p^r x^{p^r-1}(x^{p^{r-1}} - 1) - (x^{p^r} - 1)p^{r-1}x^{p^{r-1}-1}}{(x^{p^{r-1}} - 1)^2}, \quad (2.1)$$

e substituindo x por ζ_{p^r} na equação (2.1), temos que

$$f'(\zeta_{p^r}) = \frac{p^r \zeta_{p^r}^{p^r-1}(\zeta_{p^r}^{p^{r-1}} - 1) - (\zeta_{p^r}^{p^r} - 1)p^{r-1}\zeta_{p^r}^{p^{r-1}-1}}{(\zeta_{p^r}^{p^{r-1}} - 1)^2}.$$

Como $\zeta_{p^r}^{p^r} = 1$, segue que $f'_{p^r}(\zeta_{p^r}) = \frac{p^r \zeta_{p^r}^{-1}}{\zeta_{p^r}^{p^{r-1}} - 1} = \frac{-p^r}{(1 - \zeta_{p^r}^{p^{r-1}})\zeta_{p^r}}$, pois $\zeta_{p^r}^{p^{r-1}} = (e^{\frac{2\pi i}{p^r}})^{p^{r-1}} = e^{\frac{2\pi i}{p}} = \zeta_p$. Aplicando a função norma em ambos os membros e usando sua linearidade, temos que

$$N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(f'(\zeta_{p^r})) = \frac{N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(-p^r)}{N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(1 - \zeta_p)N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(\zeta_{p^r})}.$$

Temos que $N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(\zeta_{p^r}) = \pm 1$. Também, $N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(-p^r) = (-p^r)^{(p-1)p^{r-1}}$ e $N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(1 - \zeta_p) = N_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}(\zeta_p)}(1 - \zeta_p) = (N_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(1 - \zeta_p))^{p^{r-1}} = p^{p^{r-1}}$. Portanto, $D_{\mathbb{K}|\mathbb{Q}}(1, \zeta_{p^r}, \dots, \zeta_{p^r}^{\varphi(p^r)-1}) =$

$$\frac{\pm p^{r(p-1)p^{r-1}}}{p^{p^{r-1}}} = \pm p^{p^{r-1}(r(p-1)-1)}.$$

■

Observação 2.2.4 Quando $r = 1$, o corpo ciclotômico $\mathbb{Q}(\zeta_{p^r})$ é $\mathbb{Q}(\zeta_p)$, com p primo e seu discriminante satisfaz $\text{Disc}(\mathbb{Q}(\zeta_p)|\mathbb{Q}) = \pm p^{p-2}$.

Vamos, agora, ver o subcorpo real maximal dos corpos ciclotômicos.

Proposição 2.2.4 Se $n \in \mathbb{N}^*$, ζ_n é uma raiz n -ésima primitiva da unidade e $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, então \mathbb{K} é totalmente real e $[\mathbb{Q}(\zeta_n) : \mathbb{K}] = 2$.

Demonstração: Seja $f(x) = x^2 - (\zeta_n + \zeta_n^{-1})x + 1 \in \mathbb{K}[x]$. Temos que $f(\zeta_n) = 0$. Além disso, como $\zeta_n \notin \mathbb{K}$, segue que f é irredutível sobre \mathbb{K} . Logo, $f = \min_{\mathbb{K}} \zeta_n$. Desta forma, $[\mathbb{Q}(\zeta_n) : \mathbb{K}] = \text{grau}(f) = 2$.

■

$$\varphi(n) \begin{pmatrix} \mathbb{Q}(\zeta_n) \\ |2 \\ \mathbb{Q}(\zeta_n + \zeta_n^{-1}) \\ |\frac{\varphi(n)}{2} \\ \mathbb{Q} \end{pmatrix}$$

Definição 2.2.5 Nas condições da Proposição (2.2.4), o corpo $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é chamado de subcorpo maximal real de $\mathbb{Q}(\zeta_n)$.

Teorema 2.2.3 ([7], pag. 16) O anel dos inteiros de $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ e uma \mathbb{Z} -base de $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ é $\{1, \zeta_n + \zeta_n^{-1}, \zeta_n^2 + \zeta_n^{-2}, \dots, \zeta_n^{\frac{\varphi(n)}{2}-1} + \zeta_n^{\frac{\varphi(n)}{2}+1}\}$.

■

Capítulo 3

Codiferente e Diferente

Neste capítulo, apresentamos os conceitos de codiferente, diferente e algumas de suas propriedades. Veremos que o codiferente de \mathbb{L} sobre \mathbb{K} é um ideal fracionário de $\mathcal{O}_{\mathbb{L}}$ enquanto que o diferente de \mathbb{L} sobre \mathbb{K} é um ideal inteiro de $\mathcal{O}_{\mathbb{L}}$. Baseados nestes conceitos, apresentamos também algumas relações entre o diferente e o discriminante. Na Seção 3.1 apresentamos o conceito de codiferente de um conjunto, codiferente de uma extensão e algumas propriedades. Na Seção 3.2, apresentamos os conceitos de diferente de uma extensão e alguns resultados envolvendo este conceito, como a relação entre a norma do diferente e o discriminante da extensão.

3.1 Codiferente

Nesta seção, apresentamos o conceito de codiferente e suas principais propriedades. Para isto, sejam \mathcal{A} um anel de Dedekind, \mathbb{K} seu corpo de frações, \mathbb{L} uma extensão separável de \mathbb{K} de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros de \mathbb{L} sobre \mathcal{A} .

Definição 3.1.1 *Seja M um subconjunto de \mathbb{L} . O conjunto $M^* = \{x \in \mathbb{L} : Tr_{\mathbb{L}|\mathbb{K}}(xy) \in \mathcal{A}, \forall y \in M\}$ é definido como o **codiferente de M sobre \mathbb{K}** . Em particular, quando $M = \mathcal{O}_{\mathbb{L}}$ chamamos de **codiferente de \mathbb{L} sobre \mathbb{K}** ao conjunto $\mathcal{O}_{\mathbb{L}}^* = \{x \in \mathbb{L} : Tr_{\mathbb{L}|\mathbb{K}}(xy) \in \mathcal{A}, \forall y \in \mathcal{O}_{\mathbb{L}}\}$. Neste caso, denotamos $\mathcal{O}_{\mathbb{L}}^*$ por $\Delta(\mathbb{L}|\mathbb{K})^{-1}$.*

Exemplo 3.1.1 *Sejam $\mathcal{A} = \mathbb{Z}$, $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados e $d \equiv 2$ ou $3 \pmod{4}$. Vimos que $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d}; x, y \in \mathbb{Z}\}$ é o anel de inteiros de \mathbb{L} sobre \mathbb{Z} . Temos que*

$$\Delta(\mathbb{L}|\mathbb{K})^{-1} = \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}].$$

De fato:

i-) Se $x \in \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]$, então $x = \frac{1}{2\sqrt{d}}(a+b\sqrt{d})$; $a, b \in \mathbb{Z}$. Dado $y = c+e\sqrt{d} \in \mathcal{O}_{\mathbb{L}}$, temos que $Tr_{\mathbb{L}|\mathbb{K}}(xy) = Tr_{\mathbb{L}|\mathbb{K}}\left(\left(\frac{1}{2\sqrt{d}}(a+b\sqrt{d})\right)(c+e\sqrt{d})\right) = Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{1}{2\sqrt{d}}ac + \frac{ae}{2} + \frac{bc}{2} + \frac{be\sqrt{d}}{2}\right) = ae + bc \in \mathbb{Z}$. Assim, $x \in \Delta(\mathbb{L}|\mathbb{K})^{-1}$. Logo, $\frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}] \subset \Delta(\mathbb{L}|\mathbb{K})^{-1}$.

ii-) Se $x = a + b\sqrt{d} \in \Delta(\mathbb{L}|\mathbb{K})^{-1}$, então $a, b \in \mathbb{Q}$, $x \in \mathbb{L}$ e $Tr_{\mathbb{L}|\mathbb{K}}(xy) \in \mathbb{Z}$, $\forall y \in \mathbb{Z}[\sqrt{d}]$. Tomando $y = 1$, temos que $Tr_{\mathbb{L}|\mathbb{K}}(xy) = Tr_{\mathbb{L}|\mathbb{K}}(a + b\sqrt{d}) = 2a \in \mathbb{Z}$. Assim, $a = \frac{m}{2}$; $m \in \mathbb{Z}$. Tomando $y = \sqrt{d}$, temos que $Tr_{\mathbb{L}|\mathbb{K}}(xy) = Tr_{\mathbb{L}|\mathbb{K}}(a\sqrt{d} + bd) = 2db \in \mathbb{Z}$. Assim, $b = \frac{n}{2d}$; $n \in \mathbb{Z}$. Logo $x = \frac{m}{2} + \frac{n}{2d}\sqrt{d} = \frac{1}{2\sqrt{d}}(n + m\sqrt{d}) \in \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]$. Desta forma, $\Delta(\mathbb{L}|\mathbb{K})^{-1} \subset \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]$.

Assim, de (i) e (ii), segue a igualdade $\Delta(\mathbb{L}|\mathbb{K})^{-1} = \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]$.

Exemplo 3.1.2 Sejam $\mathcal{A} = \mathbb{Z}$, $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados e $d \equiv 2$ ou $3 \pmod{4}$. Se $M = \mathbb{Z}[\sqrt{d}]$, então, pelo Exemplo (3.1.1), temos que $M^* = \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]$. Mostremos que $M^{**} = M = \mathbb{Z}[\sqrt{d}]$. De fato:

i-) Se $x = a + b\sqrt{d} \in M^{**}$, então $a, b \in \mathbb{Q}$, $x \in \mathbb{L}$ e $Tr_{\mathbb{L}|\mathbb{K}}(xy) \in \mathbb{Z}$, $\forall y \in M^* = \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]$. Tomando $y = \frac{\sqrt{d}}{2\sqrt{d}} \in M^*$, temos que $Tr_{\mathbb{L}|\mathbb{K}}(xy) = Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{a}{2} + \frac{bd}{2\sqrt{d}}\right) = Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{a}{2} + \frac{b\sqrt{d}}{2}\right) = a \in \mathbb{Z}$. Tomando $y = \frac{1}{2\sqrt{d}} \in M^*$, temos que $Tr_{\mathbb{L}|\mathbb{K}}(xy) = Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{a}{2\sqrt{d}} + \frac{b}{2}\right) = b \in \mathbb{Z}$. Logo, $x = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Desta forma, $M^{**} \subset \mathbb{Z}[\sqrt{d}]$.

ii-) Se $x \in \mathbb{Z}[\sqrt{d}]$, então $x = a + b\sqrt{d}$; $a, b \in \mathbb{Z}$. Dado $y = \frac{1}{2\sqrt{d}}(c + d\sqrt{d}) \in \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]$, temos que $Tr_{\mathbb{L}|\mathbb{K}}(xy) \in \mathbb{Z}$, pois $y \in M^* = \Delta(\mathbb{L}|\mathbb{K})^{-1}$. Logo, $\mathbb{Z}[\sqrt{d}] \subset M^{**}$. Assim, de (i) e (ii), segue que $M^{**} = \mathbb{Z}[\sqrt{d}] = M$.

Proposição 3.1.1 Sejam M um subconjunto de \mathbb{L} e M^* o codiferente de M sobre \mathbb{K} . Temos que:

- (1) - Se $\mathcal{O}_{\mathbb{L}}M \subseteq M$, então M^* é um $\mathcal{O}_{\mathbb{L}}$ -módulo.
- (2) - Se $M_1 \subseteq M_2 \subseteq \mathbb{L}$, então $M_2^* \subseteq M_1^* \subseteq \mathbb{L}$.
- (3) - $\mathcal{O}_{\mathbb{L}} \subseteq \Delta(\mathbb{L}|\mathbb{K})^{-1}$.

Demonstração: (1) - Suponhamos que $\mathcal{O}_{\mathbb{L}}M \subseteq M$. Vamos mostrar que se $b \in \mathcal{O}_{\mathbb{L}}$ e $x \in M^*$ então $bx \in M^*$. Se $b \in \mathcal{O}_{\mathbb{L}}$, $x \in M^*$ e $y \in M$, temos que $Tr_{\mathbb{L}|\mathbb{K}}((bx)y) = Tr_{\mathbb{L}|\mathbb{K}}(x(by)) \in \mathcal{A}$, pois $by \in \mathcal{O}_{\mathbb{L}}M \subseteq M$. Assim, $bx \in M^*$. As demais propriedades seguem de forma análoga. Logo,

M^* é um $\mathcal{O}_{\mathbb{L}}$ -módulo.

(2) - Seja $M_1 \subseteq M_2$. Dado $x_2 \in M_2^*$, então $x_2 \in \mathbb{L}$ e $Tr_{\mathbb{L}|\mathbb{K}}(x_2 y) \in \mathcal{A}$, para todo $y \in M_2$. Como $M_1 \subset M_2$, segue que $Tr_{\mathbb{L}|\mathbb{K}}(x_2 y) \in \mathcal{A}$, para todo $y \in M_1$. Logo, $x_2 \in M_1^*$. Portanto, $M_2^* \subseteq M_1^* \subseteq \mathbb{L}$.

(3) - Como $\mathcal{O}_{\mathbb{L}}$ é inteiro sobre \mathcal{A} e \mathcal{A} é integralmente fechado segue que $Tr_{\mathbb{L}|\mathbb{K}}(\mathcal{O}_{\mathbb{L}}) \subset \mathcal{A}$. Assim, se $x, y \in \mathcal{O}_{\mathbb{L}}$, então $Tr_{\mathbb{L}|\mathbb{K}}(xy) \in \mathcal{A}$ e, deste modo, $x \in \Delta(\mathbb{L}|\mathbb{K})^{-1}$. Portanto, $\mathcal{O}_{\mathbb{L}} \subseteq \Delta(\mathbb{L}|\mathbb{K})^{-1}$. ■

A seguir faremos algumas considerações que serão utilizadas nos próximos teoremas.

Seja \mathbb{L}_1 o espaço dual de \mathbb{L} . Pelo Corolário (1.5.4), temos que existe um isomorfismo

$$\varphi : \mathbb{L} \longrightarrow \mathbb{L}_1, \text{ tal que } \varphi(x) = S_x, \text{ onde } x \in \mathbb{L} \text{ e } S_x(y) = Tr_{\mathbb{L}|\mathbb{K}}(xy), \text{ para } y \in \mathbb{L}.$$

Sejam $\{x_1, \dots, x_n\}$ uma \mathbb{K} -base de \mathbb{L} e $\{x_1^*, \dots, x_n^*\}$ um conjunto de elementos de \mathbb{L} tal que $\{\varphi_{x_1^*}, \dots, \varphi_{x_n^*}\}$ seja uma base dual de $\{x_1, \dots, x_n\}$, isto é, $\varphi_{x_i^*}(x_j) = Tr_{\mathbb{L}|\mathbb{K}}(x_i^* x_j) = \delta_{ij}$, onde $\delta_{ii} = 1$ e $\delta_{ij} = 0$ se $i \neq j$. Temos que, $\{x_1^*, \dots, x_n^*\}$ é também uma base de \mathbb{L} , chamada de **base complementar** de $\{x_1, \dots, x_n\}$.

Proposição 3.1.2 *Com as notações acima, se $\{x_1, \dots, x_n\}$ é uma \mathbb{K} -base de \mathbb{L} e $\{x_1^*, \dots, x_n^*\}$ uma base complementar de $\{x_1, \dots, x_n\}$, então $D_{\mathbb{L}|\mathbb{K}}(x_1, \dots, x_n) D_{\mathbb{L}|\mathbb{K}}(x_1^*, \dots, x_n^*) = 1$.*

Demonstração: Sejam $\sigma_1, \dots, \sigma_n$ os \mathbb{K} -homomorfismos de \mathbb{L} . Tomando

$$X = (\sigma_i(x_j))_{i,j=1}^n \text{ e } X^* = (\sigma_i(x_j^*))_{i,j=1}^n$$

e denotando por X^t a matriz transposta de X , temos que

$$(X^*)^t X = \begin{pmatrix} \sigma_1(x_1^*) & \cdots & \sigma_n(x_1^*) \\ \vdots & \ddots & \vdots \\ \sigma_1(x_n^*) & \cdots & \sigma_n(x_n^*) \end{pmatrix} \begin{pmatrix} \sigma_1(x_1) & \cdots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(x_1) & & \sigma_n(x_n) \end{pmatrix} = (Tr(x_i^* x_j))_{i,j=1}^n = I_n.$$

Assim, $\det(X^*)^t \det(X) = 1$. Pela Proposição (1.6.2), temos que

$$D_{\mathbb{L}|\mathbb{K}}(x_1, \dots, x_n) = \det(X)^2 \text{ e } D_{\mathbb{L}|\mathbb{K}}(x_1^*, \dots, x_n^*) = \det(X^*)^2.$$

Portanto, $D_{\mathbb{L}|\mathbb{K}}(x_1, \dots, x_n) D_{\mathbb{L}|\mathbb{K}}(x_1^*, \dots, x_n^*) = 1$. ■

Proposição 3.1.3 *Sejam M um subconjunto de \mathbb{L} e M^* o codiferente de M sobre \mathbb{K} . Então:*

(1) - M^* é um \mathcal{A} -módulo.

(2) - Se M é um \mathcal{A} -módulo livre com base $\{x_1, \dots, x_n\}$ então M^* é um \mathcal{A} -módulo livre com base $\{x_1^*, \dots, x_n^*\}$, onde $\{x_1^*, \dots, x_n^*\}$ é uma base de \mathbb{L} sobre \mathbb{K} tal que $Tr_{\mathbb{L}|\mathbb{K}}(x_i^* x_j) = \delta_{ij}$; $\delta_{ij} = 0$, se $i \neq j$ e $\delta_{ij} = 1$, se $i = j$.

(3) - $M^{**} = M$.

Demonstração: (1) - Mostraremos o fechamento. Sejam x_1 e $x_2 \in M^*$. Se $y \in M$, temos que

$$Tr_{\mathbb{L}|\mathbb{K}}((x_1 + x_2)y) = Tr_{\mathbb{L}|\mathbb{K}}(x_1 y) + Tr_{\mathbb{L}|\mathbb{K}}(x_2 y) \in \mathcal{A}.$$

Assim, $x_1 + x_2 \in M^*$. Agora se $a \in \mathcal{A}$, $x \in M^*$, dado $y \in M$, temos que

$$Tr_{\mathbb{L}|\mathbb{K}}((ax)y) = a Tr_{\mathbb{L}|\mathbb{K}}(xy) \in \mathcal{A}.$$

Assim $ax \in M^*$. As demais propriedades seguem de forma análoga. Portanto, M^* é um \mathcal{A} -módulo.

(2) - Sejam $\{x_1, \dots, x_n\}$ uma \mathcal{A} -base de M e $\{x_1^*, \dots, x_n^*\}$ uma \mathbb{K} -base de \mathbb{L} tal que $Tr_{\mathbb{L}|\mathbb{K}}(x_i^* x_j) = 0$ se $i \neq j$, e $Tr_{\mathbb{L}|\mathbb{K}}(x_i^* x_i) = 1$. Se $x = \sum_{i=1}^n a_i x_i^* \in \sum_{i=1}^n \mathcal{A} x_i^*$, então

$$Tr_{\mathbb{L}|\mathbb{K}}(x x_j) = Tr_{\mathbb{L}|\mathbb{K}}\left(\left(\sum_{i=1}^n a_i x_i^*\right) x_j\right) = \sum_{i=1}^n a_i Tr_{\mathbb{L}|\mathbb{K}}(x_i^* x_j) = a_j \in \mathcal{A}, \text{ para } j = 1, \dots, n.$$

Desta forma, pela linearidade da função traço, segue que $Tr_{\mathbb{L}|\mathbb{K}}(xy) \in \mathcal{A}, \forall y \in M$. Portanto, $\sum_{i=1}^n \mathcal{A} x_i^* \subseteq M^*$. Reciprocamente, se $\sum_{i=1}^n a_i x_i^* \in M^*$, com $a_i \in \mathbb{K}$, para $i = 1, \dots, n$, então,

$$a_j = Tr_{\mathbb{L}|\mathbb{K}}\left(\left(\sum_{i=1}^n a_i x_i^*\right) x_j\right) \in \mathcal{A}, \text{ para } j = 1, \dots, n,$$

e, deste modo, $M^* \subseteq \sum_{i=1}^n \mathcal{A} x_i^*$. Assim, $M^* = \sum_{i=1}^n \mathcal{A} x_i^*$. Portanto, M^* é um \mathcal{A} -módulo livre com base $\{x_1^*, \dots, x_n^*\}$.

(3) - Visto que $\{x_1^*, \dots, x_n^*\}$ é uma base de M^* e $\{x_1, \dots, x_n\}$ é uma base de \mathbb{L} sobre \mathbb{K} que satisfaz $Tr_{\mathbb{L}|\mathbb{K}}(x_i^* x_j) = \delta_{ij}$, de forma análoga ao que foi feito anteriormente, mostramos que

$$M^{**} = \sum_{i=1}^n \mathcal{A} x_i = M. \quad \blacksquare$$

Proposição 3.1.4 *Seja \mathbb{L} uma extensão separável de \mathbb{K} de grau n tal que $\mathbb{L} = \mathbb{K}[\alpha]$, para algum $\alpha \in \mathbb{L}$. Se $g(x) = x^n + c_{n-1}x^{n-1} + \dots + c_0 \in \mathcal{A}[X]$ é o polinômio minimal de α sobre \mathbb{K} , então $Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{\alpha^i}{g'(\alpha)}\right) = 0$, para $i = 0, 1, \dots, n-2$, e $Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{\alpha^{n-1}}{g'(\alpha)}\right) = 1$.*

Demonstração: Sejam $\alpha = \alpha_1, \dots, \alpha_n$ os conjugados de α sobre \mathbb{K} , onde $\alpha_i \neq \alpha_j$, se $i \neq j$, pois $\mathbb{L}|\mathbb{K}$ é separável. Temos que,

$$Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{\alpha^i}{g'(\alpha)}\right) = \sum_{k=1}^n \frac{\alpha_k^i}{g'(\alpha_k)}, \text{ para } i = 0, \dots, n-1.$$

Como $g(x)$ é o polinômio minimal de α , segue que $g(x) = \prod_{k=1}^n (x - \alpha_k)$. Assim, $\frac{1}{g(x)} = \prod_{k=1}^n \frac{1}{x - \alpha_k}$.

Podemos expressar este produto como a soma $\sum_{k=1}^n \frac{\beta_k}{x - \alpha_k}$, para certos elementos β_k . Assim,

$$\frac{1}{g(x)} = \sum_{k=1}^n \frac{\beta_k}{x - \alpha_k} \quad \text{e} \quad 1 = \sum_{k=1}^n \frac{\beta_k g(x)}{x - \alpha_k} = \sum_{k=1}^n \beta_k \left(\prod_{i \neq k} (x - \alpha_i) \right), \text{ para } i = 1, \dots, n.$$

Desta forma, para $j = 1, \dots, n$, temos que

$$1 = \sum_{k=1}^n \beta_k \left(\prod_{i \neq k} (\alpha_j - \alpha_i) \right) = \beta_1 \prod_{i \neq 1} (\alpha_j - \alpha_i) + \beta_2 \prod_{i \neq 2} (\alpha_j - \alpha_i) + \dots = \beta_j \prod_{i \neq j} (\alpha_j - \alpha_i).$$

Logo, $\beta_j = \frac{1}{\prod_{i \neq j} (\alpha_j - \alpha_i)} = \frac{1}{g'(\alpha_j)}$, para $j = 1, 2, \dots, n$. E assim,

$$\frac{1}{g(x)} = \sum_{k=1}^n \frac{1}{g'(\alpha_k)(x - \alpha_k)}.$$

Pelo algoritmo da divisão longa de Euclides, temos que

$$\frac{1}{g(x)} = \frac{1}{x^n} + c_1 \frac{1}{x^{n+1}} + c_2 \frac{1}{x^{n+2}} + c_3 \frac{1}{x^{n+3}} + \dots \text{ e}$$

$$\sum_{k=1}^n \frac{1}{g'(\alpha_k)(x - \alpha_k)} = \sum_{k=1}^n \frac{1}{g'(\alpha_k)} \left[\frac{1}{x} + \frac{\alpha_k}{x^2} + \frac{\alpha_k^2}{x^3} + \frac{\alpha_k^3}{x^4} + \dots \right].$$

Assim, temos que $\sum_{k=1}^n \frac{1}{g'(\alpha_k)} \left[\frac{1}{x} + \frac{\alpha_k}{x^2} + \frac{\alpha_k^2}{x^3} + \dots \right] = \frac{1}{x^n} + c_1 \frac{1}{x^{n+1}} + c_2 \frac{1}{x^{n+2}} + \dots$.

Comparando esta última igualdade, temos que $\sum_{k=1}^n \left(\frac{\alpha_k^i}{g'(\alpha_k)} \right) = 0$, para $i = 0, 1, \dots, n-2$ e $\sum_{k=1}^n \left(\frac{\alpha_k^{n-1}}{g'(\alpha_k)} \right) = 1$. ■

Corolário 3.1.1 *Com as mesmas hipóteses da Proposição (3.1.4), o conjunto $B = \left\{ \frac{1}{g'(\alpha)}, \frac{\alpha}{g'(\alpha)}, \dots, \frac{\alpha^{n-1}}{g'(\alpha)} \right\}$ é uma base de \mathbb{L} sobre \mathbb{K} .*

Demonstração: Temos que $[\mathbb{L} : \mathbb{K}] = n$. Resta mostrar que B é linearmente independente.

Suponha $y = \sum_{j=0}^{n-1} a_j \left(\frac{\alpha^j}{g'(\alpha)} \right) = 0$, com $a_j \in \mathbb{K}$, para $j = 0, \dots, n-1$. Assim,

$$0 = Tr_{\mathbb{L}|\mathbb{K}}(y) = Tr_{\mathbb{L}|\mathbb{K}} \left(\sum_{j=0}^{n-1} a_j \left(\frac{\alpha^j}{g'(\alpha)} \right) \right) = a_{n-1}.$$

Tomando $y\alpha = \sum_{j=0}^{n-2} a_j \left(\frac{\alpha^{j+1}}{g'(\alpha)} \right)$, temos que

$$0 = Tr_{\mathbb{L}|\mathbb{K}}(y\alpha) = Tr_{\mathbb{L}|\mathbb{K}} \left(\sum_{j=0}^{n-2} a_j \left(\frac{\alpha^{j+1}}{g'(\alpha)} \right) \right) = a_{n-2}.$$

Assim, de modo análogo, temos que $a_j = 0$, para todo $j = 0, 1, \dots, n-1$. Deste modo, B é uma base de \mathbb{L} sobre \mathbb{K} . ■

O próximo teorema nos fornece um critério para determinar $\mathcal{A}[\alpha]^*$ quando \mathbb{L} é uma extensão finita separável de \mathbb{K} e $\mathbb{L} = \mathbb{K}[\alpha]$, para algum $\alpha \in \mathbb{L}$.

Teorema 3.1.1 *Seja \mathbb{L} uma extensão separável de \mathbb{K} de grau n tal que $\mathbb{L} = \mathbb{K}[\alpha]$. Se $g(x) \in \mathcal{A}[x]$ é o polinômio minimal de α sobre \mathbb{K} então $\mathcal{A}[\alpha]^* = \frac{1}{g'(\alpha)} \mathcal{A}[\alpha]$.*

Demonstração: Se $y \in \mathcal{A}[\alpha]$, então $y = \sum_{i=0}^{n-1} a_i \alpha^i$; $a_i \in \mathcal{A}$. Mostremos que $\forall x \in \mathcal{A}[\alpha]$, temos que $Tr_{\mathbb{L}|\mathbb{K}} \left(\frac{xy}{g'(\alpha)} \right) \in \mathcal{A}$. Primeiro, notemos que

$$Tr_{\mathbb{L}|\mathbb{K}} \left(\frac{\alpha^j y}{g'(\alpha)} \right) = \sum_{i=0}^{n-1} a_i Tr_{\mathbb{L}|\mathbb{K}} \left(\frac{\alpha^{j+i}}{g'(\alpha)} \right) = a_{n-1-j} \in \mathcal{A}, \text{ para } j = 0, \dots, n-1.$$

Assim, para todo $x = \sum_{i=0}^{n-1} b_i \alpha^i \in \mathcal{A}[\alpha]$, segue que

$$\text{Tr}_{\mathbb{L}|\mathbb{K}}\left(\frac{xy}{g'(\alpha)}\right) = \sum_{i=0}^{n-1} b_i \text{Tr}_{\mathbb{L}|\mathbb{K}}\left(\frac{\alpha^i y}{g'(\alpha)}\right) \in \mathcal{A}.$$

Logo $y \in \mathcal{A}[\alpha]^*$, o que implica que $\frac{1}{g'(\alpha)}\mathcal{A}[\alpha] \subseteq \mathcal{A}[\alpha]^*$. Para mostrar a outra inclusão, se $y \in \mathcal{A}[\alpha]^*$, então, pelo Corolário (3.1.1), como $\left\{\frac{1}{g'(\alpha)}, \frac{\alpha}{g'(\alpha)}, \dots, \frac{\alpha^{n-1}}{g'(\alpha)}\right\}$ é uma base de \mathbb{L} sobre \mathbb{K} , segue que $y = \sum_{j=0}^{n-1} a_j \left(\frac{\alpha^j}{g'(\alpha)}\right)$, com $a_j \in \mathbb{K}$ para $j = 0, \dots, n-1$. Assim, pela Proposição (3.1.4), temos que

$$\text{Tr}_{\mathbb{L}|\mathbb{K}}(y) = \sum_{j=0}^{n-1} a_j \text{Tr}_{\mathbb{L}|\mathbb{K}}\left(\frac{\alpha^j}{g'(\alpha)}\right) = a_{n-1} \in \mathcal{A},$$

pois $y \in \mathcal{A}[\alpha]^*$. Analogamente,

$$\text{Tr}_{\mathbb{L}|\mathbb{K}}(y\alpha) = \sum_{j=0}^{n-1} a_j \text{Tr}_{\mathbb{L}|\mathbb{K}}\left(\frac{\alpha^{j+1}}{g'(\alpha)}\right) = a_{n-2} - a_{n-1} \text{Tr}_{\mathbb{L}|\mathbb{K}}\left(\frac{\alpha^n}{g'(\alpha)}\right).$$

Como $\alpha^n = -(c_1 \alpha^{n-1} + c_2 \alpha^{n-2} + \dots + c_n)$, segue que $\text{Tr}_{\mathbb{L}|\mathbb{K}}\left(\frac{\alpha^n}{g'(\alpha)}\right) = -c_1 \in \mathcal{A}$. Assim, $\text{Tr}_{\mathbb{L}|\mathbb{K}}(y\alpha) = a_{n-2} - a_{n-1} c_1 \in \mathcal{A}$. Como $a_{n-1}, c_1 \in \mathcal{A}$ segue que $a_{n-2} \in \mathcal{A}$. Continuando desta forma, $a_i \in \mathcal{A}$, para todo $i = 0, \dots, n-1$. Portanto, $\mathcal{A}[\alpha]^* = \frac{1}{g'(\alpha)}\mathcal{A}[\alpha]$. ■

Exemplo 3.1.3 *Sejam $\mathbb{L} = \mathbb{Q}(\zeta_p)$, o p -ésimo corpo ciclotômico, com p primo e $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_p]$ o anel de inteiros de \mathbb{L} sobre \mathbb{Z} . O polinômio minimal de ζ_p sobre \mathbb{Q} é $g(x) = x^{p-1} + \dots + x + 1$. Pelo Teorema (3.1.1), temos que*

$$\Delta(\mathbb{L}|\mathbb{K})^{-1} = \frac{1}{((p-1)\zeta_p^{p-2} + \dots + 2\zeta_p + 1)} \mathbb{Z}[\zeta_p].$$

Exemplo 3.1.4 *Sejam $\mathcal{A} = \mathbb{Z}$, $\mathbb{K} = \mathbb{Q}$ e $\mathbb{L} = \mathbb{Q}(\sqrt{17})$. Pelo Teorema (3.1.1), temos que*

$$\mathcal{A}[\alpha]^* = \mathbb{Z}[\sqrt{17}]^* = \frac{1}{g'(\alpha)} \mathbb{Z}[\sqrt{17}],$$

onde $g(x) = x^2 - 17 = \min_{\mathbb{Q}} \sqrt{17}$. Logo, $\mathbb{Z}[\sqrt{17}]^* = \frac{1}{2\sqrt{17}} \mathbb{Z}[\sqrt{17}]$. Note que $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}\left[\frac{1 + \sqrt{17}}{2}\right] \neq$

$\mathcal{A}[\alpha]$.

Proposição 3.1.5 *Se $\mathbb{L} = \mathbb{K}(\alpha)$, onde α é inteiro sobre \mathbb{K} e $[\mathbb{K}(\alpha) : \mathbb{K}] = n$, então $\Delta(\mathbb{L}|\mathbb{K})^{-1}$ é um $\mathcal{O}_{\mathbb{L}}$ -módulo finitamente gerado.*

Demonstração: Temos que $\mathcal{A}[\alpha] \subset \mathcal{O}_{\mathbb{L}}$. Assim, pelo item (2) da Proposição (3.1.1), temos que $\Delta(\mathbb{L}|\mathbb{K})^{-1} = \mathcal{O}_{\mathbb{L}}^* \subset \mathcal{A}[\alpha]^*$. Agora, como α é inteiro sobre \mathcal{A} , temos que $\mathcal{A}[\alpha]$ é um \mathcal{A} -módulo finitamente gerado por $\{1, \alpha, \dots, \alpha^{n-1}\}$. Como $\{1, \alpha, \dots, \alpha^{n-1}\}$ é uma base de \mathbb{L} sobre \mathbb{K} , segue que $\{1, \alpha, \dots, \alpha^{n-1}\}$ é linearmente independente sobre \mathcal{A} . Logo, $\mathcal{A}[\alpha]$ é um \mathcal{A} -módulo livre. Pelo item (2) da Proposição (3.1.3), temos que $\mathcal{A}[\alpha]^*$ é um \mathcal{A} -módulo livre finitamente gerado. Logo, como \mathcal{A} é noetheriano segue, pelo Corolário (1.2.2), que $\mathcal{A}[\alpha]^*$ é um \mathcal{A} -módulo noetheriano. Como $\Delta(\mathbb{L}|\mathbb{K})^{-1}$ é um $\mathcal{O}_{\mathbb{L}}$ -módulo, pelo item (1) da Proposição (3.1.1), segue que $\Delta(\mathbb{L}|\mathbb{K})^{-1}$ é um \mathcal{A} -módulo. Desta forma, temos que $\Delta(\mathbb{L}|\mathbb{K})^{-1}$ é um \mathcal{A} -submódulo de um \mathcal{A} -módulo noetheriano $\mathcal{A}[\alpha]^*$. Portanto, $\Delta(\mathbb{L}|\mathbb{K})^{-1}$ é um \mathcal{A} -módulo finitamente gerado. Desta forma, existem $x_1, \dots, x_m \in \Delta(\mathbb{L}|\mathbb{K})^{-1}$ tal que $\Delta(\mathbb{L}|\mathbb{K})^{-1} = \sum_{i=1}^m \mathcal{A}x_i$. Em particular, como $\Delta(\mathbb{L}|\mathbb{K})^{-1}$ é um $\mathcal{O}_{\mathbb{L}}$ -módulo, temos que $\Delta(\mathbb{L}|\mathbb{K})^{-1} \subset \sum_{i=1}^m \mathcal{O}_{\mathbb{L}}x_i \subset \Delta(\mathbb{L}|\mathbb{K})^{-1}$. Logo, $\Delta(\mathbb{L}|\mathbb{K})^{-1}$ é um $\mathcal{O}_{\mathbb{L}}$ -módulo finitamente gerado. ■

Corolário 3.1.2 *Se $\mathbb{L} = \mathbb{K}[\alpha]$, onde α é inteiro sobre \mathbb{K} e $[\mathbb{K}[\alpha] : \mathbb{K}] = n$, então $\Delta(\mathbb{L}|\mathbb{K})^{-1}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{L}}$.*

Demonstração: Pela Proposição (3.1.5), temos que $\Delta(\mathbb{L}|\mathbb{K})^{-1}$ é um $\mathcal{O}_{\mathbb{L}}$ -módulo finitamente gerado. Assim, se tomarmos d um fator comum entre os denominadores dos geradores de $\Delta(\mathbb{L}|\mathbb{K})^{-1}$, temos que $d\Delta(\mathbb{L}|\mathbb{K})^{-1} \subseteq \mathcal{O}_{\mathbb{L}}$. Portanto, $\Delta(\mathbb{L}|\mathbb{K})^{-1}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{L}}$. ■

3.2 Diferente

Nesta seção veremos o conceito de diferente e suas propriedades. Para isto, sejam \mathcal{A} um domínio de Dedekind, \mathbb{K} seu corpo de frações, \mathbb{L} uma extensão separável de \mathbb{K} de grau n , $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros de \mathbb{L} sobre \mathcal{A} e $\Delta(\mathbb{L}|\mathbb{K})^{-1}$ o codiferente de \mathbb{L} sobre \mathbb{K} .

3.2.1 Definição e Propriedades

Apresentamos aqui a definição de diferente de uma extensão e alguns resultados envolvendo este conceito.

Definição 3.2.1 *O ideal de $\mathcal{O}_{\mathbb{L}}$ igual ao inverso do ideal fracionário $\Delta(\mathbb{L}|\mathbb{K})^{-1}$ é chamado diferente de \mathbb{L} sobre \mathbb{K} e denotado por $\Delta(\mathbb{L}|\mathbb{K})$.*

Observação 3.2.1 Notemos que como $\mathcal{O}_{\mathbb{L}}$ é um anel de Dedekind, segue que todo ideal fracionário de $\mathcal{O}_{\mathbb{L}}$ admite inverso. Em particular, $\Delta(\mathbb{L}|\mathbb{K})^{-1}$ é inversível. Ainda, temos que $\Delta(\mathbb{L}|\mathbb{K})$ é um ideal inteiro de $\mathcal{O}_{\mathbb{L}}$. De fato, visto que $\mathcal{O}_{\mathbb{L}} \subseteq \Delta(\mathbb{L}|\mathbb{K})^{-1}$, temos que $\mathcal{O}_{\mathbb{L}}\Delta(\mathbb{L}|\mathbb{K}) \subseteq \Delta(\mathbb{L}|\mathbb{K})\Delta(\mathbb{L}|\mathbb{K})^{-1} = \mathcal{O}_{\mathbb{L}}$. Logo, $\Delta(\mathbb{L}|\mathbb{K}) \subseteq \mathcal{O}_{\mathbb{L}}$.

Exemplo 3.2.1 Sejam $\mathcal{A} = \mathbb{Z}$, $\mathbb{K} = \mathbb{Q}$ e $\mathbb{L} = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados e $d \equiv 2$ ou $3 \pmod{4}$. Pelo Exemplo (3.1.1), temos que $\Delta(\mathbb{L}|\mathbb{K})^{-1} = \frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]$. Assim, pela Definição (3.2.1), temos que o diferente de \mathbb{L} sobre \mathbb{K} é $\Delta(\mathbb{L}|\mathbb{K}) = (2\sqrt{d})\mathbb{Z}[\sqrt{d}]$, pois $\left(\frac{1}{2\sqrt{d}}\mathbb{Z}[\sqrt{d}]\right)(2\sqrt{d}\mathbb{Z}[\sqrt{d}]) = \mathbb{Z}[\sqrt{d}]$.

Proposição 3.2.1 Se $\mathbb{L} = \mathbb{K}[\alpha]$, onde $\alpha \in \mathcal{O}_{\mathbb{L}}$ e se $g(x) \in \mathcal{A}[x]$ é o polinômio minimal de α sobre \mathbb{K} , então $\Delta(\mathbb{L}|\mathbb{K}) = \mathcal{O}_{\mathbb{L}}g'(\alpha)$ se, e somente se, $\mathcal{O}_{\mathbb{L}} = \mathcal{A}[\alpha]$.

Demonstração: Se $\mathcal{O}_{\mathbb{L}} = \mathcal{A}[\alpha]$ temos, pelo Teorema (3.1.1), que $\Delta(\mathbb{L}|\mathbb{K})^{-1} = \frac{1}{g'(\alpha)}\mathcal{O}_{\mathbb{L}}$. Assim,

$$\Delta(\mathbb{L}|\mathbb{K}) = (\Delta(\mathbb{L}|\mathbb{K})^{-1})^{-1} = \left(\frac{1}{g'(\alpha)}\mathcal{O}_{\mathbb{L}}\right)^{-1} = g'(\alpha)\mathcal{O}_{\mathbb{L}}.$$

Reciprocamente, suponha que $\Delta(\mathbb{L}|\mathbb{K}) = g'(\alpha)\mathcal{O}_{\mathbb{L}}$. Se $z \in \mathcal{O}_{\mathbb{L}}$, então existe um polinômio $h(x) \in \mathbb{K}[x]$, de grau menor que $n = [\mathbb{L} : \mathbb{K}]$, tal que $z = h(\alpha)$, pois $\{1, \alpha, \dots, \alpha^{n-1}\}$ é base de \mathbb{L} sobre \mathbb{K} . Na demonstração da Proposição (3.1.4), vimos que

$$1 = \sum_{k=1}^n \frac{g(x)}{g'(\alpha_k)(x - \alpha_k)} = \sum_{k=1}^n \prod_{i \neq k} \frac{x - \alpha_i}{\alpha_k - \alpha_i},$$

onde $\alpha = \alpha_1, \dots, \alpha_n$, são os conjugados de α sobre \mathbb{K} . O polinômio

$$h_1(x) = \sum_{k=1}^n h(\alpha_k) \prod_{i \neq k} \frac{x - \alpha_i}{\alpha_k - \alpha_i}$$

tem grau menor que n e $h_1(\alpha_j) = \sum_{k=1}^n h(\alpha_k) \prod_{i \neq k} \frac{\alpha_j - \alpha_i}{\alpha_k - \alpha_i} = h(\alpha_j)$, pois se $k \neq j$ temos que

$\prod_{i \neq k} \frac{\alpha_j - \alpha_i}{\alpha_k - \alpha_i} = 0$. Como grau $(h - h_1)$ é menor que n e $h - h_1$ tem α_i , para $i = 1, \dots, n$, como raízes, segue que $h(x) - h_1(x) = 0$, o que implica que $h(x) = h_1(x)$. Mas,

$$Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{zg(x)}{g'(\alpha)(x - \alpha)}\right) = Tr_{\mathbb{L}|\mathbb{K}}\left(z \prod_{i \neq k} \frac{x - \alpha_i}{\alpha - \alpha_i}\right) = \sum_{k=1}^n h(\alpha_k) \prod_{i \neq k} \frac{x - \alpha_i}{\alpha_k - \alpha_i} = h(x).$$

Como os coeficientes de $\frac{g(x)}{x-\alpha}$ pertencem a \mathbb{L} e são inteiros sobre \mathcal{A} , segue que $\frac{g(x)}{x-\alpha} \in \mathcal{O}_{\mathbb{L}}[x]$ e como $\frac{z}{g'(\alpha)} \in \Delta(\mathbb{L}|\mathbb{K})^{-1}$ segue que $h(x) = \text{Tr}_{\mathbb{L}|\mathbb{K}}\left(\frac{zg(x)}{g'(\alpha)(x-\alpha)}\right) \in \mathcal{A}[x]$. Assim, $z = h(\alpha) \in \mathcal{A}[\alpha]$ e, portanto, $\mathcal{O}_{\mathbb{L}} \subset \mathcal{A}[\alpha]$. Como $\mathcal{A}[\alpha] \subset \mathcal{O}_{\mathbb{L}}$, segue que $\mathcal{O}_{\mathbb{L}} = \mathcal{A}[\alpha]$. ■

Exemplo 3.2.2 Para corpos quadráticos $\mathbb{L} = \mathbb{Q}(\sqrt{d})$, com d livre de quadrados, temos:

i)- Se $d \equiv 2$ ou $d \equiv 3 \pmod{4}$, então $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\sqrt{d}]$. Pela Proposição (3.2.1), temos que $\Delta(\mathbb{L}|\mathbb{Q}) = \mathbb{Z}[\sqrt{d}]g'(\sqrt{d})$, onde $g(x)$ é o polinômio minimal de \sqrt{d} sobre \mathbb{Q} .

ii)- Se $d \equiv 1 \pmod{4}$, então $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Ainda, temos que $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}\left(\frac{1+\sqrt{d}}{2}\right)$

e, pela Proposição (3.2.1), temos que $\Delta(\mathbb{L}|\mathbb{Q}) = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]g'\left(\frac{1+\sqrt{d}}{2}\right)$, onde $g(x)$ é o polinômio minimal de $\frac{1+\sqrt{d}}{2}$ sobre \mathbb{Q} .

Exemplo 3.2.3 Sejam p um primo, ζ_p é uma raiz p -ésima primitiva da unidade e $\mathbb{L} = \mathbb{Q}(\zeta_p)$. Pela Proposição (3.2.1), temos que $\Delta(\mathbb{L}|\mathbb{Q}) = \mathbb{Z}[\zeta_p]g'(\zeta_p)$, onde $g(x)$ é o polinômio minimal de ζ_p sobre \mathbb{Q} .

Proposição 3.2.2 Seja J um ideal fracionário de $\mathcal{O}_{\mathbb{L}}$. Tem-se que $\text{Tr}_{\mathbb{L}|\mathbb{K}}(J) \subseteq \mathcal{A}$ se, e somente se, $J \subseteq \Delta(\mathbb{L}|\mathbb{K})^{-1}$.

Demonstração: Suponha $\text{Tr}_{\mathbb{L}|\mathbb{K}}(J) \subseteq \mathcal{A}$. Se $x \in \mathcal{O}_{\mathbb{L}}$ e $y \in J$, temos que $xy \in \mathcal{O}_{\mathbb{L}}J = J$. Como $\text{Tr}_{\mathbb{L}|\mathbb{K}}(J) \subseteq \mathcal{A}$, segue $\text{Tr}_{\mathbb{L}|\mathbb{K}}(xy) \in \mathcal{A}$. Portanto, $y \in \Delta(\mathbb{L}|\mathbb{K})^{-1}$. Logo, $J \subset \Delta(\mathbb{L}|\mathbb{K})^{-1}$. Reciprocamente, se $J \subset \Delta(\mathbb{L}|\mathbb{K})^{-1}$, então $\text{Tr}_{\mathbb{L}|\mathbb{K}}(J\mathcal{O}_{\mathbb{L}}) \subseteq \mathcal{A}$. ■

Lema 3.2.1 Sejam I, J ideais fracionários de $\mathcal{O}_{\mathbb{L}}$. Se para todo M ideal fracionário de \mathbb{L} tem-se que $M \subseteq I$ se, e somente se, $M \subseteq J$, então $I = J$.

Demonstração: Se $x \in I$, então $M = \langle x \rangle \subset I$. Assim, $M \subset J$, ou seja, $x \in J$. Logo, $I \subseteq J$. De modo análogo, temos que $J \subseteq I$. Portanto, $I = J$. ■

Proposição 3.2.3 Sejam \mathcal{A} um anel de Dedekind, \mathbb{K} seu corpo de frações, \mathbb{L} uma extensão separável de \mathbb{K} de grau finito e \mathbb{N} uma extensão separável de \mathbb{L} de grau finito. Se $\mathcal{O}_{\mathbb{N}}$ e $\mathcal{O}_{\mathbb{L}}$ são os anéis de inteiros de \mathbb{N} e \mathbb{L} , respectivamente, então

$$\Delta(\mathbb{N}|\mathbb{K}) = \mathcal{O}_{\mathbb{N}}\Delta(\mathbb{L}|\mathbb{K})\Delta(\mathbb{N}|\mathbb{L}).$$

Demonstração: Seja M um ideal fracionário de \mathcal{O}_N tal que $M \subseteq \Delta(N|\mathbb{L})^{-1}$. Mostremos que $M \subseteq \mathcal{O}_N \Delta(\mathbb{L}|\mathbb{K}) \Delta(N|\mathbb{L})^{-1}$. Pela Proposição (3.2.2), temos que $Tr_{N|\mathbb{L}}(M) \subseteq \mathcal{O}_L$, o que implica que

$$\Delta(\mathbb{L}|\mathbb{K})^{-1} Tr_{N|\mathbb{L}}(M) \subseteq \Delta(\mathbb{L}|\mathbb{K})^{-1} \mathcal{O}_L = \Delta(\mathbb{L}|\mathbb{K})^{-1}.$$

Assim, temos que $Tr_{N|\mathbb{L}}(\Delta(\mathbb{L}|\mathbb{K})^{-1} M) \subseteq \Delta(\mathbb{L}|\mathbb{K})^{-1}$. Como $M = M \mathcal{O}_N$, pois M é um ideal fracionário de \mathcal{O}_N , temos que

$$Tr_{N|\mathbb{L}}(\mathcal{O}_N \Delta(\mathbb{L}|\mathbb{K})^{-1} M) \subseteq \Delta(\mathbb{L}|\mathbb{K})^{-1}.$$

Agora, $Tr_{N|\mathbb{K}}(\mathcal{O}_N \Delta(\mathbb{L}|\mathbb{K})^{-1} M) = Tr_{L|\mathbb{K}}(Tr_{N|\mathbb{L}}(\mathcal{O}_N \Delta(\mathbb{L}|\mathbb{K})^{-1} M)) \subseteq Tr_{L|\mathbb{K}}(\Delta(\mathbb{L}|\mathbb{K})^{-1}) \subseteq \mathcal{A}$. Assim, pela Proposição (3.2.2), temos que

$$\mathcal{O}_N \Delta(\mathbb{L}|\mathbb{K})^{-1} M \subseteq \Delta(N|\mathbb{K})^{-1}.$$

Isto implica que $M \subseteq \mathcal{O}_N \Delta(\mathbb{L}|\mathbb{K}) \Delta(N|\mathbb{K})^{-1}$. Agora, seja $M \subseteq \mathcal{O}_N \Delta(\mathbb{L}|\mathbb{K}) \Delta(N|\mathbb{K})^{-1}$ e mostremos que $M \subseteq \Delta(N|\mathbb{L})^{-1}$. Temos que $\mathcal{O}_N \Delta(\mathbb{L}|\mathbb{K})^{-1} M \subseteq \Delta(N|\mathbb{K})^{-1}$. Pela Proposição (3.2.2), segue que

$$Tr_{N|\mathbb{K}}(\mathcal{O}_N \Delta(\mathbb{L}|\mathbb{K})^{-1} M) \subseteq \mathcal{A}.$$

Como $Tr_{N|\mathbb{K}}(\mathcal{O}_N \Delta(\mathbb{L}|\mathbb{K})^{-1} M) = Tr_{L|\mathbb{K}}(Tr_{N|\mathbb{L}}(\mathcal{O}_N \Delta(\mathbb{L}|\mathbb{K})^{-1} M)) \subseteq \mathcal{A}$, pela Proposição (3.2.2), segue que $Tr_{N|\mathbb{L}}(\mathcal{O}_N \Delta(\mathbb{L}|\mathbb{K})^{-1} M) \subseteq \Delta(\mathbb{L}|\mathbb{K})^{-1}$. Assim,

$$\Delta(\mathbb{L}|\mathbb{K})^{-1} Tr_{N|\mathbb{L}}(M) \subseteq \Delta(\mathbb{L}|\mathbb{K})^{-1}.$$

Desta forma, $Tr_{N|\mathbb{L}}(M) \subseteq \mathcal{O}_L$ e assim $M \subseteq \Delta(N|\mathbb{L})^{-1}$. Portanto, pelo Lema (3.2.1), temos que $\Delta(N|\mathbb{L})^{-1} = \mathcal{O}_N \Delta(\mathbb{L}|\mathbb{K}) \Delta(N|\mathbb{K})^{-1}$ e, assim, $\Delta(N|\mathbb{K}) = \mathcal{O}_N \Delta(\mathbb{L}|\mathbb{K}) \Delta(N|\mathbb{L})$. ■

Exemplo 3.2.4 *Sejam $n = 15$, $\zeta = \zeta_{15}$ uma raiz 15-ésima primitiva da unidade, $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{Q}(\zeta + \zeta^{-1})$ e $\mathbb{N} = \mathbb{Q}(\zeta)$.*

$$8 \left(\begin{array}{c} \mathbb{N} = \mathbb{Q}(\zeta) \\ |2 \\ \mathbb{L} = \mathbb{Q}(\zeta + \zeta^{-1}) \\ |4 \\ \mathbb{K} = \mathbb{Q} \end{array} \right)$$

Temos que:

i-) Seja ψ o polinômio minimal de $\zeta + \zeta^{-1}$ sobre \mathbb{Q} e ψ' a derivada de ψ . Como $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta + \zeta^{-1}]$, pela Proposição (3.2.1), temos que

$$\Delta(\mathbb{L}|\mathbb{K}) = \psi'(\zeta + \zeta^{-1})\mathbb{Z}[\zeta + \zeta^{-1}].$$

ii-) Seja $g(x) = x^2 - (\zeta + \zeta^{-1})x + 1$ o polinômio minimal de ζ sobre \mathbb{L} . Temos que $g'(\zeta) = \zeta - \zeta^{-1}$. Assim, como $\mathcal{O}_{\mathbb{N}} = \mathbb{Z}[\zeta]$, pela Proposição (3.2.1), segue que

$$\Delta(\mathbb{N}|\mathbb{L}) = (\zeta - \zeta^{-1})\mathbb{Z}[\zeta].$$

Segue, de (i), (ii) e da Proposição (3.2.3), que

$$\Delta(\mathbb{L}|\mathbb{K}) = \mathbb{Z}[\zeta]\Delta(\mathbb{L}|\mathbb{K})\Delta(\mathbb{N}|\mathbb{L}) = (\zeta - \zeta^{-1})\psi'(\zeta + \zeta^{-1})\mathbb{Z}[\zeta].$$

Observação 3.2.2 Sejam \mathcal{A} um anel de Dedekind, \mathbb{K} seu corpo de frações, \mathbb{L} uma extensão finita de \mathbb{K} e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de \mathbb{L} sobre \mathcal{A} . Seja P um ideal primo de \mathcal{A} , $S = \mathcal{A} - P$, $\mathcal{A}' = S^{-1}\mathcal{A}$ e $\mathcal{O}'_{\mathbb{L}} = S^{-1}\mathcal{O}_{\mathbb{L}}$. Visto que \mathcal{A} é um anel de Dedekind, pelo Teorema (1.10.1), temos que $\mathcal{A}' = S^{-1}\mathcal{A}$ é um anel de Dedekind. Agora, pela Proposição (1.10.4), temos que como $\mathcal{O}_{\mathbb{L}}$ é o anel de inteiros de \mathbb{L} sobre \mathcal{A} , segue que $\mathcal{O}'_{\mathbb{L}} = S^{-1}\mathcal{O}_{\mathbb{L}}$ é o anel de inteiros de \mathbb{L} sobre \mathcal{A}' . Pelo Teorema (1.8.1), temos que como $S^{-1}\mathcal{A}$ é um anel de Dedekind, segue que $\mathcal{O}'_{\mathbb{L}} = S^{-1}\mathcal{O}_{\mathbb{L}}$ é um anel de Dedekind. Logo, todo ideal fracionário de $\mathcal{O}'_{\mathbb{L}}$ admite inverso. Temos que o conjunto

$$\Delta_P(\mathbb{L}|\mathbb{K})^{-1} = \{x \in \mathbb{L}; Tr_{\mathbb{L}|\mathbb{K}}(xy) \in \mathcal{A}' \text{ para todo } y \in \mathcal{O}'_{\mathbb{L}}\}$$

é um ideal fracionário de $\mathcal{O}'_{\mathbb{L}}$, logo admite inverso.

Definição 3.2.2 Nas condições da Observação (3.2.2), chamamos de **diferente de $\mathbb{L}|\mathbb{K}$ sobre P** e denotamos por $\Delta_P(\mathbb{L}|\mathbb{K})$ o inverso do ideal $\Delta_P(\mathbb{L}|\mathbb{K})^{-1}$.

Proposição 3.2.4 Com as notações da Definição (3.2.2), tem-se que $\mathcal{O}'_{\mathbb{L}}\Delta(\mathbb{L}|\mathbb{K}) = \Delta_P(\mathbb{L}|\mathbb{K})$.

Demonstração: Se $x \in \mathcal{O}'_{\mathbb{L}}\Delta(\mathbb{L}|\mathbb{K})$, então x é da forma $\frac{y}{s}$, com $y \in \Delta(\mathbb{L}|\mathbb{K})$ e $s \in S$. Seja $z \in \Delta_P(\mathbb{L}|\mathbb{K})^{-1} = \{x \in \mathbb{L}; Tr_{\mathbb{L}|\mathbb{K}}(xy) \in \mathcal{A}' \text{ para todo } y \in \mathcal{O}'_{\mathbb{L}}\}$. Temos que $Tr_{\mathbb{L}|\mathbb{K}}(z\mathcal{O}'_{\mathbb{L}}) \subset \mathcal{A}'$. Pela Proposição (1.5.6), temos que $\mathcal{O}_{\mathbb{L}}$ é um \mathcal{A} -módulo finitamente gerado. Sejam $\{t_1, \dots, t_m\}$

um conjunto de geradores do \mathcal{A} -módulo $\mathcal{O}_{\mathbb{L}}$. Para todo $i = 1, \dots, m$, temos que $zt_i \in z\mathcal{O}'_{\mathbb{L}}$ e, assim, $Tr_{\mathbb{L}|\mathbb{K}}(zt_i) = \frac{a_i}{s_i}$, com $a_i \in \mathcal{A}$ e $s_i \in S$. Se $s_0 = s_1 \cdots s_m \in S$, então

$$Tr_{\mathbb{L}|\mathbb{K}}(zs_0t_i) = s_0Tr_{\mathbb{L}|\mathbb{K}}(zt_i) = s_0 \frac{a_i}{s_i} = a_i(s_0 \cdots s_{i-1}s_{i+1} \cdots s_m) \in \mathcal{A}, \quad \text{para } i = 1, 2, \dots, m.$$

Desta forma, $Tr_{\mathbb{L}|\mathbb{K}}(zs_0\mathcal{O}_{\mathbb{L}}) \subseteq \mathcal{A}$, pois se $w \in \mathcal{O}_{\mathbb{L}}$, então $w = \sum_{i=1}^m \alpha_i t_i$; $\alpha_i \in \mathcal{A}$ e assim

$$Tr_{\mathbb{L}|\mathbb{K}}(zs_0w) = \sum_{i=1}^m \alpha_i Tr_{\mathbb{L}|\mathbb{K}}(zs_0t_i) \in \mathcal{A}. \text{ Como } Tr_{\mathbb{L}|\mathbb{K}}(zs_0\mathcal{O}_{\mathbb{L}}) \subseteq \mathcal{A}, \text{ segue que } zs_0 \in \Delta(\mathbb{L}|\mathbb{K})^{-1},$$

isto é, $yzs_0 \in \Delta(\mathbb{L}|\mathbb{K})\Delta(\mathbb{L}|\mathbb{K})^{-1} = \mathcal{O}_{\mathbb{L}}$. Logo, $xz = \frac{yz}{s} = \frac{yzs_0}{ss_0} \in \mathcal{O}'_{\mathbb{L}}$. Como $z \in \Delta_P(\mathbb{L}|\mathbb{K})^{-1}$,

segue que $x \in \Delta_P(\mathbb{L}|\mathbb{K})$. Logo, $\mathcal{O}'_{\mathbb{L}}\Delta(\mathbb{L}|\mathbb{K}) \subseteq \Delta_P(\mathbb{L}|\mathbb{K})$. Por outro lado, seja $x \in \Delta_P(\mathbb{L}|\mathbb{K})$.

Temos que $\Delta(\mathbb{L}|\mathbb{K})^{-1}$ é um \mathcal{A} -módulo finitamente gerado. Sejam $\{z_1, \dots, z_m\}$ um conjunto de geradores do \mathcal{A} -módulo $\Delta(\mathbb{L}|\mathbb{K})^{-1}$. Temos que $Tr_{\mathbb{L}|\mathbb{K}}(z_i\mathcal{O}_{\mathbb{L}}) \subseteq \mathcal{A}$, para $i = 1, \dots, m$. Assim, segue que $Tr_{\mathbb{L}|\mathbb{K}}(z_i\mathcal{O}'_{\mathbb{L}}) \subseteq \mathcal{A}'$.

De fato, se $t \in \mathcal{O}'_{\mathbb{L}}$, então $t = \frac{a}{b}$; $a \in \mathcal{O}_{\mathbb{L}}$, $b \in S$. Assim $Tr_{\mathbb{L}|\mathbb{K}}(z_it) = Tr_{\mathbb{L}|\mathbb{K}}(z_i \frac{a}{b}) = \frac{1}{b}Tr_{\mathbb{L}|\mathbb{K}}(z_ia) \in \mathcal{A}'$, pois $b \in S \subset \mathbb{K}$ e $\frac{1}{b}\mathcal{A} \subset \mathcal{A}'$.

Desta forma, $z_i \in \Delta_P(\mathbb{L}|\mathbb{K})^{-1}$. Assim, $xz_i \in \Delta_P(\mathbb{L}|\mathbb{K})\Delta_P(\mathbb{L}|\mathbb{K})^{-1} = \mathcal{O}'_{\mathbb{L}}$, ou seja, $xz_i = \frac{b_i}{s_i}$ com

$b_i \in \mathcal{O}_{\mathbb{L}}$ e $s_i \in S$. Se $s = s_1 \cdots s_m \in S$, então $sxz_i \in \mathcal{O}_{\mathbb{L}}$, para todo $i = 1, \dots, m$ e, assim, $sx\Delta_P(\mathbb{L}|\mathbb{K})^{-1} \subseteq \mathcal{O}_{\mathbb{L}}$. Portanto, $sx \in \Delta(\mathbb{L}|\mathbb{K})$ e $x \in \mathcal{O}'_{\mathbb{L}}\Delta(\mathbb{L}|\mathbb{K})$. Logo, $\Delta_P(\mathbb{L}|\mathbb{K}) \subseteq \mathcal{O}'_{\mathbb{L}}\Delta(\mathbb{L}|\mathbb{K})$.

Portanto, $\mathcal{O}'_{\mathbb{L}}\Delta(\mathbb{L}|\mathbb{K}) = \Delta_P(\mathbb{L}|\mathbb{K})$. ■

3.2.2 Diferente e Discriminante

Nesta seção apresentamos algumas relações que envolvem o diferente e o discriminante de uma extensão. Se destaca o fato de que a norma do diferente é o módulo do discriminante. Para isto, sejam \mathcal{A} um domínio de Dedekind, \mathbb{K} seu corpo de frações, \mathbb{L} uma extensão finita de \mathbb{K} de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de \mathbb{L} sobre \mathcal{A} .

Teorema 3.2.1 ([11], pag. 44) *Se \mathcal{A} é um anel de Dedekind, \mathbb{K} seu corpo de frações e \mathbb{L} uma extensão finita de \mathbb{K} , então*

$$N(\Delta(\mathbb{L}|\mathbb{K})) = |\text{Disc}(\mathbb{L}|\mathbb{K})|.$$

■

Exemplo 3.2.5 *Sejam $\mathcal{A} = \mathbb{Z}$, $\mathbb{K} = \mathbb{Q}$ e $\mathbb{L} = \mathbb{Q}(\zeta_{3^4})$. Pela Proposição (2.2.3), temos que $|\text{Disc}(\mathbb{L}|\mathbb{K})| = 3^{3^{4-1}(4(3-1)-1)} = 3^{3^3(8-1)} = 3^{27(7)} = 3^{189}$. Assim, pelo Teorema (3.2.1), segue que $N(\Delta(\mathbb{L}|\mathbb{K})) = 3^{189}$.*

Proposição 3.2.5 *Sejam $\mathbb{K}_1, \mathbb{K}_2$ extensões finitas de \mathbb{Q} tal que $\mathbb{K}_2|\mathbb{Q}$ é de Galois e $\mathbb{K}_1 \cap \mathbb{K}_2 = \mathbb{Q}$. Se $\mathbb{L} = \mathbb{K}_1\mathbb{K}_2$, então $[\mathbb{L} : \mathbb{Q}] = [\mathbb{K}_1 : \mathbb{Q}][\mathbb{K}_2 : \mathbb{Q}]$.*

Demonstração: Como $\mathbb{K}_2|\mathbb{Q}$ é de Galois e separável, segue que $\mathbb{K}_2|\mathbb{Q}$ é normal. Pelo Teorema (1.3.2), temos que existe $\alpha \in \mathbb{K}_2$ tal que $\mathbb{K}_2 = \mathbb{Q}(\alpha)$. Sejam $g(x) = \min_{\mathbb{Q}}(\alpha)$ e $\{\alpha = \alpha_1, \dots, \alpha_n\}$ as raízes de g . Como $\mathbb{K}_2|\mathbb{Q}$ é normal e $\alpha \in \mathbb{K}_2$, segue que $\{\alpha = \alpha_1, \dots, \alpha_n\} \subset \mathbb{K}_2$. Por outro lado, temos que $\mathbb{L} = \mathbb{K}_1(\alpha)$ e $g(x) = \min_{\mathbb{K}_1} \alpha$. De fato, se $g(x) = h(x)f(x)$; com $h(x), f(x) \in \mathbb{K}_1[x]$, então os coeficientes de h, f são elementos de $\mathbb{K}_1 \cap \mathbb{K}_2$, visto que os coeficientes de h, f são somas de produtos de $\{\alpha = \alpha_1, \dots, \alpha_n\} \subset \mathbb{K}_2$. Logo, $h(x), f(x) \in (\mathbb{K}_1 \cap \mathbb{K}_2)[x] = \mathbb{Q}[x]$, o que é um absurdo, pois g é irredutível sobre \mathbb{Q} . Portanto, $[\mathbb{L} : \mathbb{K}_1] = \text{grau}(g) = [\mathbb{K}_2 : \mathbb{Q}]$. Assim, $[\mathbb{L} : \mathbb{Q}] = [\mathbb{L} : \mathbb{K}_1][\mathbb{K}_1 : \mathbb{Q}] = [\mathbb{K}_2 : \mathbb{Q}][\mathbb{K}_1 : \mathbb{Q}]$. ■

A próxima proposição segue sem demonstração pois necessita de alguns pré-requisitos que resolvemos omitir neste trabalho para não torná-lo muito extenso.

Proposição 3.2.6 ([11], pag. 48) *Se $\mathbb{K}_1, \mathbb{K}_2$ são extensões finitas de \mathbb{Q} tal que $\mathbb{K}_2|\mathbb{Q}$ é de Galois e $\text{mdc}(\text{Disc}(\mathbb{K}_1|\mathbb{Q}), \text{Disc}(\mathbb{K}_2|\mathbb{Q})) = 1$, então $\mathbb{K}_1 \cap \mathbb{K}_2 = \mathbb{Q}$.* ■

Corolário 3.2.1 *Se $\mathbb{K}_1, \mathbb{K}_2$ são extensões finitas de \mathbb{Q} tal que $\mathbb{K}_2|\mathbb{Q}$ é de Galois e $\text{mdc}(\text{Disc}(\mathbb{K}_1|\mathbb{Q}), \text{Disc}(\mathbb{K}_2|\mathbb{Q})) = 1$, então $[\mathbb{L} : \mathbb{Q}] = [\mathbb{K}_1 : \mathbb{Q}][\mathbb{K}_2 : \mathbb{Q}]$.*

Demonstração: Como $\text{mdc}(\text{Disc}(\mathbb{K}_1|\mathbb{Q}), \text{Disc}(\mathbb{K}_2|\mathbb{Q})) = 1$, segue que $\mathbb{K}_1 \cap \mathbb{K}_2 = \mathbb{Q}$. Agora, pela Proposição (3.2.5), temos que $[\mathbb{L} : \mathbb{Q}] = [\mathbb{K}_1 : \mathbb{Q}][\mathbb{K}_2 : \mathbb{Q}]$. ■

Exemplo 3.2.6 *Sejam $\mathbb{K} = \mathbb{Q}$, $\mathbb{K}_1 = \mathbb{Q}(\sqrt{2})$ e $\mathbb{K}_2 = \mathbb{Q}(\zeta_3)$. Temos que $\text{Disc}(\mathbb{K}_1|\mathbb{K}) = 8$ e $\text{Disc}(\mathbb{K}_2|\mathbb{K}) = -3$. Assim, como $\text{mdc}(\text{Disc}(\mathbb{K}_1|\mathbb{K}), \text{Disc}(\mathbb{K}_2|\mathbb{K})) = 1$ segue, pelo Corolário (3.2.1), que se $\mathbb{L} = \mathbb{Q}(\sqrt{2}, \zeta_3) = \mathbb{K}_1\mathbb{K}_2$, então $[\mathbb{L} : \mathbb{Q}] = [\mathbb{K}_1 : \mathbb{Q}][\mathbb{K}_2 : \mathbb{Q}] = 2 \cdot 2 = 4$.*

Proposição 3.2.7 ([5], pag. 218) *Sejam $\mathbb{K}_1, \mathbb{K}_2$ extensões finitas de \mathbb{Q} de graus n_1, n_2 , respectivamente, tal que $\mathbb{K}_2|\mathbb{Q}$ é de Galois e $\text{mdc}(\text{Disc}(\mathbb{K}_1|\mathbb{Q}), \text{Disc}(\mathbb{K}_2|\mathbb{Q})) = 1$. Se $\mathbb{L} = \mathbb{K}_1\mathbb{K}_2$, então*

$$\text{Disc}(\mathbb{L}|\mathbb{K}) = \text{Disc}(\mathbb{K}_1|\mathbb{Q})^{n_2} \text{Disc}(\mathbb{K}_2|\mathbb{Q})^{n_1}.$$

Exemplo 3.2.7 *Com as mesmas hipóteses do Exemplo (3.2.6), como $\text{mdc}(\text{Disc}(\mathbb{Q}(\sqrt{2})|\mathbb{Q}), \text{Disc}(\mathbb{Q}(\zeta_3)|\mathbb{Q})) = 1$ segue, pela Proposição (3.2.7), que*

$$\text{Disc}(\mathbb{Q}(\sqrt{2}, \zeta_3)|\mathbb{Q}) = \text{Disc}(\mathbb{Q}(\sqrt{2})|\mathbb{Q})^2 \text{Disc}(\mathbb{Q}(\zeta_3)|\mathbb{Q})^2 = 8^2(-3)^2.$$

Teorema 3.2.2 *Sejam $\mathbb{K}_1, \mathbb{K}_2$ extensões de \mathbb{Q} com discriminantes primos entre si, tal que $\mathbb{K}_2|\mathbb{Q}$ é de Galois e $\mathbb{L} = \mathbb{K}_1\mathbb{K}_2$. Se $\mathcal{O}_{\mathbb{L}}, \mathcal{O}_{\mathbb{K}_1}$ e $\mathcal{O}_{\mathbb{K}_2}$ são os anéis de inteiros de \mathbb{L}, \mathbb{K}_1 e \mathbb{K}_2 , sobre \mathbb{Z} , respectivamente, então o produto de uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}_1}$ por uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}_2}$ é uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{L}}$.*

Demonstração: Sejam $\{x_1, \dots, x_{n_1}\}$ uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}_1}$ e $\{y_1, \dots, y_{n_2}\}$ uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}_2}$. Vamos calcular $D_{\mathbb{L}|\mathbb{Q}}(x_1y_1, \dots, x_{n_1}y_{n_2})$. Observamos que se σ é um homomorfismo de \mathbb{L} e se $\sigma_{\mathbb{K}_1}, \sigma_{\mathbb{K}_2}$ denotam a restrição de σ a \mathbb{K}_1 e \mathbb{K}_2 , respectivamente, então a função $\sigma \longrightarrow (\sigma_{\mathbb{K}_1}, \sigma_{\mathbb{K}_2})$ é bijetora, pois $\mathbb{L} = \mathbb{K}_1\mathbb{K}_2$ e $[\mathbb{L}:\mathbb{Q}] = n_1n_2$. Assim, $D_{\mathbb{L}|\mathbb{Q}}(x_1y_1, \dots, x_{n_1}y_{n_2}) = [\det(\sigma_i\tau_j(x_ky_l))]^2$, onde σ_i são os homomorfismos de \mathbb{K}_1 e τ_j são os homomorfismos de \mathbb{K}_2 . O determinante dessa matriz é o produto de Kronecker das matrizes $(\sigma_i(x_k))_{i,k=1}^{n_1}$ e $(\tau_j(y_l))_{j,l=1}^{n_2}$. Assim,

$$[\det(\sigma_i(x_k))]^{2n_2} [\det(\tau_j(y_l))]^{2n_1} = D_{\mathbb{K}_1|\mathbb{Q}}(x_1, \dots, x_{n_1})^{n_2} D_{\mathbb{K}_2|\mathbb{Q}}(y_1, \dots, y_{n_2})^{n_1}.$$

Portanto, $D_{\mathbb{L}|\mathbb{Q}}(x_1y_1, \dots, x_{n_1}y_{n_2}) = D_{\mathbb{K}_1|\mathbb{Q}}(x_1, \dots, x_{n_1})^{n_2} D_{\mathbb{K}_2|\mathbb{Q}}(y_1, \dots, y_{n_2})^{n_1}$. Pela Proposição (3.2.7), temos que $\langle D_{\mathbb{L}|\mathbb{Q}}(x_1y_1, \dots, x_{n_1}y_{n_2}) \rangle = \langle \text{Disc}(\mathbb{L}|\mathbb{Q}) \rangle$. Logo, se $\{z_1, \dots, z_{n_1n_2}\}$ é uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{L}}$, tal que $x_ly_m = \sum_{i=1}^{n_1n_2} a_{ki}z_i$, para $k = lm$, temos que (a_{ki}) é inversível. Logo, $\{x_1y_1, \dots, x_{n_1}y_{n_2}\}$ é uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{L}}$. ■

O próximo teorema obtém o discriminante de qualquer corpo ciclotômico sobre \mathbb{Q} .

Teorema 3.2.3 *Sejam $n \in \mathbb{N}; n > 2$ e $\mathbb{K} = \mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n -ésima primitiva da unidade. Se $n = \prod_{j=1}^r p_j^{a_j}$, onde p_j são primos distintos e $a_j \in \mathbb{N}^*$, então*

$$\text{Disc}(\mathbb{K}|\mathbb{Q}) = \frac{(-1)^{\frac{\varphi(n)r}{2}} n^{\varphi(n)}}{\prod_{j=1}^r p_j^{\frac{\varphi(n)}{p_j-1}}},$$

onde φ é a função de Euler.

Demonstração: Vamos provar por indução sobre r . Para o caso $r = 1$, foi provado na Proposição (2.2.3). Suponhamos que o resultado é válido para $r - 1$, onde $r > 1$. Seja $m = \frac{n}{p_r^{a_r}}$, temos que

$$\text{Disc}(\mathbb{Q}(\zeta_m)|\mathbb{Q}) = \frac{(-1)^{\frac{\varphi(m)(r-1)}{2}} m^{\varphi(m)}}{\prod_{j=1}^{r-1} p_j^{\frac{\varphi(m)}{p_j-1}}} \quad \text{e}$$

$$\text{Disc}(\mathbb{Q}(\zeta_{p_r^{a_r}})|\mathbb{Q}) = \frac{(-1)^{\frac{\varphi(p_r^{a_r})}{2}} (p_r^{a_r})^{\varphi(p_r^{a_r})}}{p_r^{\frac{\varphi(p_r^{a_r})}{p_r-1}}}.$$

Assim, $\text{mdc}(\text{Disc}(\mathbb{Q}(\zeta_m)|\mathbb{Q}), \text{Disc}(\mathbb{Q}(\zeta_{p_r^{a_r}})|\mathbb{Q})) = 1$. Como $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_{p_r^{a_r}})$ temos, pela Proposição (3.2.7), que

$$\text{Disc}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) = (\text{Disc}(\mathbb{Q}(\zeta_m)|\mathbb{Q}))^{\varphi(p_r^{a_r})} (\text{Disc}(\mathbb{Q}(\zeta_{p_r^{a_r}})|\mathbb{Q}))^{\varphi(m)}.$$

Agora,

$$(\text{Disc}(\mathbb{Q}(\zeta_m)|\mathbb{Q}))^{\varphi(p_r^{a_r})} = \frac{(-1)^{\frac{\varphi(m)(r-1)\varphi(p_r^{a_r})}{2}} (m)^{\varphi(m)\varphi(p_r^{a_r})}}{\prod_{j=1}^{r-1} p_j^{\frac{\varphi(m)\varphi(p_r^{a_r})}{p_j-1}}} = \frac{(-1)^{\frac{\varphi(n)(r-1)}{2}} (m)^{\varphi(n)}}{\prod_{j=1}^{r-1} p_j^{\frac{\varphi(n)}{p_j-1}}} \text{ e}$$

$$(\text{Disc}(\mathbb{Q}(\zeta_{p_r^{a_r}})|\mathbb{Q}))^{\varphi(m)} = \frac{(-1)^{\frac{\varphi(p_r^{a_r})\varphi(m)}{2}} (p_r^{a_r})^{\varphi(m)\varphi(p_r^{a_r})}}{p_r^{\frac{\varphi(p_r^{a_r})\varphi(m)}{(p_r-1)}}} = \frac{(-1)^{\frac{\varphi(n)}{2}} (p_r^{a_r})^{\varphi(n)}}{p_r^{\frac{\varphi(n)}{p_r-1}}}.$$

Multiplicando estas igualdades, obtemos

$$\text{Disc}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) = \frac{(-1)^{\frac{\varphi(n)r}{2}} n^{\varphi(n)}}{\prod_{j=1}^r p_j^{\frac{\varphi(n)}{p_j-1}}},$$

o que prova o teorema. ■

Exemplo 3.2.8 *Sejam $n = 20$ e $\mathbb{K} = \mathbb{Q}(\zeta_{20})$ o 20-ésimo corpo ciclotômico. Pelo Teorema (3.2.3), como $\varphi(20) = 8$ e $20 = 2^2 \cdot 5$, segue que*

$$\text{Disc}(\mathbb{Q}(\zeta_{20})|\mathbb{Q}) = \frac{(-1)^{\frac{8 \cdot 2}{2}} 20^8}{2^{\frac{8}{1}} 5^{\frac{8}{4}}} = \frac{2^{16} 5^8}{2^8 5^2} = 2^8 5^6.$$

Exemplo 3.2.9 *Sejam $n = 39$ e $\mathbb{K} = \mathbb{Q}(\zeta_{39})$ o 39-ésimo corpo ciclotômico. Pelo Teorema (3.2.3), como $\varphi(39) = 24$ e $39 = 3 \cdot 13$, segue que*

$$\text{Disc}(\mathbb{Q}(\zeta_{39})|\mathbb{Q}) = \frac{(-1)^{\frac{24 \cdot 2}{2}} 39^{24}}{3^{\frac{24}{2}} 13^{\frac{24}{12}}} = \frac{3^{24} 13^{24}}{3^{12} 13^2} = 3^{12} 13^{22}.$$

Capítulo 4

Ramificação de Ideais

Sejam \mathcal{A} um anel de Dedekind, \mathbb{K} seu corpo de frações, \mathbb{L} uma extensão separável de \mathbb{K} de grau n , $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de \mathbb{L} sobre \mathcal{A} e P um ideal primo de \mathcal{A} . Neste capítulo, apresentamos alguns fatos da decomposição do ideal estendido $P\mathcal{O}_{\mathbb{L}}$ em um produto de ideais primos de $\mathcal{O}_{\mathbb{L}}$. Na Seção 4.1, apresentamos os conceitos de ramificação de um ideal, o Teorema da Igualdade Fundamental e o Teorema de Kummer. Na Seção 4.2, apresentamos a relação entre um ideal primo P de \mathcal{A} que se ramifica em $\mathcal{O}_{\mathbb{L}}$ e o discriminante da extensão $\mathbb{L}|\mathbb{K}$. Na Seção 4.3, apresentamos a relação entre um ideal primo Q de $\mathcal{O}_{\mathbb{L}}$ que se ramifica e o diferente da extensão $\mathbb{L}|\mathbb{K}$. Por fim, na Seção 4.4, apresentamos a ramificação em corpos ciclotômicos, encontrando todos os ideais primos P de \mathbb{Z} que se ramificam em $\mathbb{Z}[\zeta_n]$, todos os ideais primos Q de $\mathbb{Z}[\zeta_n]$ que se ramificam e a fatoração do diferente $\Delta(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ como produto de ideais primos de $\mathbb{Z}[\zeta_n]$.

4.1 Teorema de Kummer

Sejam \mathcal{A} um anel de Dedekind, \mathbb{K} seu corpo de frações, \mathbb{L} uma extensão separável de \mathbb{K} de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de \mathbb{L} sobre \mathcal{A} .

Definição 4.1.1 *Seja B um ideal de \mathcal{A} . Dizemos que o ideal inteiro*

$$B\mathcal{O}_{\mathbb{L}} = \left\{ \sum_{i=1}^n b_i a_i; b_i \in B, a_i \in \mathcal{O}_{\mathbb{L}} \right\}$$

de $\mathcal{O}_{\mathbb{L}}$ é a extensão de B em $\mathcal{O}_{\mathbb{L}}$. Neste caso, chamamos $B\mathcal{O}_{\mathbb{L}}$ de ideal estendido.

Seja P um ideal primo de \mathcal{A} . Como $\mathcal{O}_{\mathbb{L}}$ é um anel de Dedekind segue, pelo Teorema (1.8.2), que o ideal estendido $P\mathcal{O}_{\mathbb{L}}$ de $\mathcal{O}_{\mathbb{L}}$ é expresso de forma única como o produto

$$P\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^g Q_i^{e_i},$$

onde os Q_i 's são ideais primos de $\mathcal{O}_{\mathbb{L}}$ e os e_i 's são inteiros estritamente positivos, para $i = 1, \dots, g$.

Nesta seção, veremos um método para encontrar os ideais primos Q_i que aparecem na fatoração de $P\mathcal{O}_{\mathbb{L}}$ e os valores de e_i , para $i = 1, \dots, g$.

Proposição 4.1.1 *Seja P um ideal primo de \mathcal{A} . Se $P\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^g Q_i^{e_i}$, com Q_i 's ideais primos de $\mathcal{O}_{\mathbb{L}}$ e $e_i \geq 1$, para todo $i = 1, \dots, g$, é a fatoração de $P\mathcal{O}_{\mathbb{L}}$, então $Q_i \cap \mathcal{A} = P$, para $i = 1, \dots, g$. Além disso, os Q_i 's são os únicos ideais primos de $\mathcal{O}_{\mathbb{L}}$ cuja intersecção com \mathcal{A} resulta no ideal primo P .*

Demonstração: Seja Q_i um ideal primo de $\mathcal{O}_{\mathbb{L}}$ que aparece na fatoração de $P\mathcal{O}_{\mathbb{L}}$. Como $\mathcal{A} \subset \mathcal{O}_{\mathbb{L}}$ segue, pela Proposição (1.1.3), que $Q_i \cap \mathcal{A}$ é um ideal primo de \mathcal{A} e também $Q_i \cap \mathcal{A} \subsetneq \mathcal{A}$, pois $1 \notin Q_i$. Agora, como $P \subset P\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^g Q_i^{e_i} \subset Q_i$, para todo i , segue que $P \subset Q_i \cap \mathcal{A} \subsetneq \mathcal{A}$. Como P é maximal, pois \mathcal{A} é um anel de Dedekind, segue que $P = Q_i \cap \mathcal{A}$, para $i = 1, \dots, g$. Para a unicidade, se B é um ideal primo de $\mathcal{O}_{\mathbb{L}}$ tal que $B \cap \mathcal{A} = P$, então, $P \subset B$, o que implica que $P\mathcal{O}_{\mathbb{L}} \subset B\mathcal{O}_{\mathbb{L}} = B$. Assim, $B \supset P\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^g Q_i^{e_i}$. Pelo Lema (1.1.4), temos que $B \supset Q_j$, para algum j . Como $\mathcal{O}_{\mathbb{L}}$ é de Dedekind, segue que Q_j é maximal e, desta forma, $B = Q_j$, pois $B \subsetneq \mathcal{O}_{\mathbb{L}}$. ■

Definição 4.1.2 *Seja B um ideal primo de $\mathcal{O}_{\mathbb{L}}$. Dizemos que B está acima do ideal primo P de \mathcal{A} se $P = \mathcal{A} \cap B$.*

Observação 4.1.1 *Notemos que os ideais primos de $\mathcal{O}_{\mathbb{L}}$ que estão acima de um ideal primo P de \mathcal{A} são exatamente os ideais primos de $\mathcal{O}_{\mathbb{L}}$ que aparecem na fatoração de $P\mathcal{O}_{\mathbb{L}}$.*

Exemplo 4.1.1 *Sejam p um número primo, $\zeta = \zeta_p$ uma raiz p -ésima primitiva da unidade, $\mathcal{A} = \mathbb{Z}$, $\mathbb{K} = \mathbb{Q}$ e $\mathbb{L} = \mathbb{Q}(\zeta_p)$. Temos que $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta_p]$ e que $\langle p \rangle$ é um ideal primo de \mathbb{Z} . Mostremos que $\langle p \rangle \mathbb{Z}[\zeta_p] = p\mathbb{Z}[\zeta_p] = P^{p-1}$, onde P é um ideal primo de $\mathbb{Z}[\zeta_p]$ e $P = \langle 1 - \zeta \rangle$. De fato, primeiro notemos que $1 - \zeta | 1 - \zeta^j$ e $1 - \zeta^j | 1 - \zeta$ para todo $j = 1, \dots, p-1$. Desta forma, geram o mesmo ideal em $\mathbb{Z}[\zeta_p]$. Agora, notemos que como o polinômio ciclotômico $\phi_p(x) = x^{p-1} + \dots + x + 1 = (x - \zeta)(x - \zeta^2) \cdots (x - \zeta^{p-1})$, segue que $p = \phi_p(1) = (1 - \zeta)(1 - \zeta^2) \cdots (1 - \zeta_{p-1})$. Assim,*

$\langle p \rangle = \prod_{j=1}^{p-1} \langle 1 - \zeta^j \rangle$. Agora, como $\langle 1 - \zeta \rangle = \langle 1 - \zeta^j \rangle$, para todo $j = 1, \dots, p-1$, segue que $\langle p \rangle = \langle 1 - \zeta \rangle^{p-1}$. Desta forma, se $P = \langle 1 - \zeta \rangle$, então $p\mathbb{Z}[\zeta_p] = P^{p-1}$. Aplicando a norma temos que $p^{p-1} = N_{\mathbb{L}|\mathbb{K}}(p) = N(P)^{p-1}$, o que implica que $N(P) = p$ e, assim, pela Proposição (1.9.4), temos que P é um ideal primo de $\mathbb{Z}[\zeta_p]$. Logo, a decomposição de $p\mathbb{Z}[\zeta_p]$ em ideais primos de $\mathbb{Z}[\zeta_p]$ é dada por $p\mathbb{Z}[\zeta_p] = P^{p-1}$. Pela Observação (4.1.1), temos que o único ideal primo de $\mathbb{Z}[\zeta_p]$ cuja intersecção com \mathbb{Z} resulta em $\langle p \rangle$ é P .

Observação 4.1.2 Com as notações anteriores, temos \mathcal{A}/P e $\mathcal{O}_{\mathbb{L}}/Q_i$ são corpos, para todo $i = 1, \dots, g$. De fato, basta notar que como \mathcal{A} e $\mathcal{O}_{\mathbb{L}}$ são anéis de Dedekind, segue que P e Q_i são ideais maximais de \mathcal{A} e $\mathcal{O}_{\mathbb{L}}$, respectivamente. Desta forma, temos que \mathcal{A}/P e $\mathcal{O}_{\mathbb{L}}/Q_i$ são corpos, para todo $i = 1, \dots, g$.

Lema 4.1.1 Com as notações anteriores, tem-se que para todo $i = 1, \dots, g$, \mathcal{A}/P pode ser identificado como um subcorpo de $\mathcal{O}_{\mathbb{L}}/Q_i$. Além disso, $\mathcal{O}_{\mathbb{L}}/Q_i$ é um espaço vetorial de dimensão finita sobre \mathcal{A}/P , para $i = 1, \dots, g$.

Demonstração: Considere as aplicações $\mathcal{A} \xrightarrow{i} \mathcal{O}_{\mathbb{L}} \xrightarrow{\pi} \mathcal{O}_{\mathbb{L}}/Q_i$, onde i é a inclusão e π é a projeção. Temos que $\text{Ker}(\pi \circ i) = \{x \in \mathcal{A}; (\pi \circ i)(x) = \bar{0}\} = \{x \in \mathcal{A}; x \in Q_i\} = Q_i \cap \mathcal{A} = P$. Assim, pelo Teorema (1.1.1), temos que $\mathcal{A}/P \simeq \text{Im}(\pi \circ i)$. Portanto, \mathcal{A}/P pode ser identificado como um subcorpo de $\mathcal{O}_{\mathbb{L}}/Q_i$. Agora, sejam as operações:

$$\begin{aligned} \oplus : \mathcal{O}_{\mathbb{L}}/Q_i \times \mathcal{O}_{\mathbb{L}}/Q_i &\longrightarrow \mathcal{O}_{\mathbb{L}}/Q_i \\ (x + Q_i, y + Q_i) &\longmapsto (x + y) + Q_i \\ \otimes : \mathcal{A}/P \times \mathcal{O}_{\mathbb{L}}/Q_i &\longrightarrow \mathcal{O}_{\mathbb{L}}/Q_i \\ (a + P, y + Q_i) &\longmapsto (ay) + Q_i \end{aligned}$$

Com estas operações temos que $\mathcal{O}_{\mathbb{L}}/Q_i$ é um espaço vetorial sobre \mathcal{A}/P , para $i = 1, \dots, g$. Além disso, a dimensão de $\mathcal{O}_{\mathbb{L}}/Q_i$ sobre \mathcal{A}/P é finita. De fato, temos, pela Proposição (1.5.6), que $\mathcal{O}_{\mathbb{L}}$ é um \mathcal{A} -módulo finitamente gerado. Sejam $\{x_1, \dots, x_m\}$ os geradores de $\mathcal{O}_{\mathbb{L}}$ sobre \mathcal{A} . Assim, se $b \in \mathcal{O}_{\mathbb{L}}$ então $b = a_1x_1 + \dots + a_mx_m$; onde $a_i \in \mathcal{A}$, $i = 1, \dots, m$. Desta forma, $\bar{b} = b + Q_i = (a_1x_1 + Q_i) + \dots + (a_mx_m + Q_i) = (a_1 + P)(x_1 + Q_i) + \dots + (a_m + P)(x_m + Q_i)$. Portanto, $\{\bar{x}_1, \dots, \bar{x}_m\}$ gera $\mathcal{O}_{\mathbb{L}}/Q_i$ como um espaço vetorial sobre \mathcal{A}/P , o que implica que $\dim_{\mathcal{A}/P} \mathcal{O}_{\mathbb{L}}/Q_i$ é finita. ■

Definição 4.1.3 O grau $f_i = f(Q_i|P)$ da extensão $\mathcal{O}_{\mathbb{L}}/Q_i$ sobre \mathcal{A}/P , para $i = 1, \dots, g$, é chamado de **grau de inércia de Q_i sobre P** . O expoente $e_i = e(Q_i|P)$, para $i = 1, \dots, g$, é chamado de **índice de ramificação de Q_i sobre P** .

Observação 4.1.3 Notemos que o Lema (4.1.1) garante que f_i é finito para todo $i = 1, \dots, g$.

Definição 4.1.4 Sejam P um ideal primo de \mathcal{A} e $P\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^g Q_i^{e_i}$ a fatoração de $P\mathcal{O}_{\mathbb{L}}$ em um produto de ideais primos de $\mathcal{O}_{\mathbb{L}}$. Dizemos que o ideal P de \mathcal{A} é:

- **totalmente decomposto em \mathbb{L} , (ou em $\mathcal{O}_{\mathbb{L}}$)**, quando $e_i = f_i = 1$, para todo ideal primo Q_i que está acima de P .
- **inerte em \mathbb{L} , (ou em $\mathcal{O}_{\mathbb{L}}$)**, quando $e_i = 1$ e $f_i = n$, para todo ideal primo Q_i que está acima de P .
- **totalmente ramificado em \mathbb{L} , (ou em $\mathcal{O}_{\mathbb{L}}$)**, quando $e_i = n$ e $f_i = 1$, para todo ideal primo Q_i que está acima de P .
- **ramificado em \mathbb{L} , (ou em $\mathcal{O}_{\mathbb{L}}$)**, se existir um ideal primo Q_i de $\mathcal{O}_{\mathbb{L}}$ que está acima de P tal que $e_i > 1$ para algum i .

Definição 4.1.5 Nas condições da Definição (4.1.4), dizemos que um ideal primo Q de $\mathcal{O}_{\mathbb{L}}$ é **ramificado em $\mathcal{O}_{\mathbb{L}}$** se ele está acima de um ideal primo P de \mathcal{A} que se ramifica em $\mathcal{O}_{\mathbb{L}}$ e seu índice de ramificação é $e(Q|P) \geq 2$, ou seja, $P\mathcal{O}_{\mathbb{L}} = \left(\prod_{i=1}^g Q_i^{e_i} \right) Q^{e_Q}$; onde $e_Q \geq 2$.

Observação 4.1.4 Notemos que se um ideal primo Q de $\mathcal{O}_{\mathbb{L}}$ se ramifica, então o ideal primo P de \mathcal{A} tal que $P = Q \cap \mathcal{A}$ se ramifica em $\mathcal{O}_{\mathbb{L}}$. Isto segue do fato de que $P\mathcal{O}_{\mathbb{L}} = \left(\prod_{i=1}^g Q_i^{e_i} \right) Q^{e_Q}$; onde $e_Q \geq 2$.

Exemplo 4.1.2 Nas condições do Exemplo (4.1.1) temos que o ideal primo $\langle p \rangle$ de \mathbb{Z} é ramificado em $\mathbb{Z}[\zeta_p]$. Também, o ideal P de $\mathbb{Z}[\zeta_p]$ é ramificado em $\mathbb{Z}[\zeta_p]$.

Lema 4.1.2 Se P é um ideal primo de \mathcal{A} tal que $P\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^g Q_i^{e_i}$, onde os Q_i 's são ideais primos distintos de $\mathcal{O}_{\mathbb{L}}$, então a sequência de ideais

$$\mathcal{O}_{\mathbb{L}} \supset Q_1 \supset Q_1^2 \supset \dots \supset Q_1^{e_1} \supset Q_1^{e_1} Q_2 \supset \dots \supset Q_1^{e_1} Q_2^{e_2} \supset \dots \supset Q_1^{e_1} \dots Q_g^{e_g} = P\mathcal{O}_{\mathbb{L}}$$

de $\mathcal{O}_{\mathbb{L}}$ é maximal.

Demonstração: Dois elementos consecutivos desta sequência são da forma Q e QQ_i , onde Q é um produto de alguns ideais Q_j , $j = 1, \dots, g$. Se existir um ideal B tal que $QQ_i \subset B \subset Q$

segue, pelo Lema (1.7.1), que B divide QQ_i . Assim, existe um ideal $I \subset \mathcal{O}_L$ tal que $QQ_i = BI$. De modo análogo, Q divide B , ou seja, existe um ideal $J \subset \mathcal{O}_L$ tal que $B = QJ$. Logo, $QQ_i = QJI$, ou seja, $Q_i = JI$. Agora, $Q_i = JI \subset I \subset \mathcal{O}_L$. Como Q_i é maximal, pois \mathcal{O}_L é Dedekind, segue que $Q_i = I$ ou $I = \mathcal{O}_L$, ou seja, $Q_i = I$ ou $Q_i = J$. Se $Q_i = I$, então $B = Q$ e, se $Q_i = J$, então $B = QQ_i$. Portanto, não existe ideal não trivial entre QQ_i e Q . ■

Lema 4.1.3 *Seja P um ideal primo de \mathcal{A} tal que $P\mathcal{O}_L = \prod_{i=1}^g Q_i^{e_i}$, onde Q_i 's são ideais primos distintos de \mathcal{O}_L . Considere a cadeia decrescente de ideais de \mathcal{O}_L*

$$\mathcal{O}_L \supset Q_1 \supset Q_1^2 \supset \cdots \supset Q_1^{e_1} \supset Q_1^{e_1} Q_2 \supset \cdots \supset Q_1^{e_1} Q_2^{e_2} \supset \cdots \supset Q_1^{e_1} \cdots Q_g^{e_g} = P\mathcal{O}_L.$$

Se Q é um ideal desta cadeia diferente de $P\mathcal{O}_L$, então \mathcal{O}_L/QQ_i , Q/QQ_i e \mathcal{O}_L/Q são espaços vetoriais sobre \mathcal{A}/P . Além disso,

$$\dim_{\mathcal{A}/P} \mathcal{O}_L/QQ_i = \dim_{\mathcal{A}/P} Q/QQ_i + \dim_{\mathcal{A}/P} \mathcal{O}_L/Q.$$

Demonstração: Temos que \mathcal{O}_L/QQ_i e \mathcal{O}_L/Q são espaços vetoriais sobre \mathcal{A}/P . Seja $\varphi : \mathcal{O}_L/QQ_i \rightarrow \mathcal{O}_L/Q$ tal que $\varphi(x + QQ_i) = x + Q$. Temos que φ é uma transformação linear sobrejetora. Agora, $\text{Ker}(\varphi) = Q/QQ_i$. De fato, se $\bar{x} = x + QQ_i \in \text{Ker}(\varphi)$, então $\varphi(x + QQ_i) = x + Q = \bar{0}$, o que implica que $x \in Q$. Assim $\bar{x} = x + QQ_i \in Q/QQ_i$. Desta forma, $\text{Ker}(\varphi) \subseteq Q/QQ_i$. Analogamente, se $\bar{x} \in Q/QQ_i$, então $\bar{x} = x + QQ_i$. Daí, $\varphi(\bar{x}) = x + Q = \bar{0}$, pois $x \in Q$. Logo, $Q/QQ_i \subseteq \text{Ker}(\varphi)$. Assim, pelo Teorema do Núcleo e da Imagem, temos que

$$\dim_{\mathcal{A}/P} \mathcal{O}_L/QQ_i = \dim_{\mathcal{A}/P} Q/QQ_i + \dim_{\mathcal{A}/P} \mathcal{O}_L/Q,$$

o que prova o lema. ■

Lema 4.1.4 *Seja P um ideal primo de \mathcal{A} tal que $P\mathcal{O}_L = \prod_{i=1}^g Q_i^{e_i}$, onde Q_i 's são ideais primos distintos de \mathcal{O}_L . Considere a cadeia decrescente de ideais*

$$\mathcal{O}_L \supset Q_1 \supset Q_1^2 \supset \cdots \supset Q_1^{e_1} \supset Q_1^{e_1} Q_2 \supset \cdots \supset Q_1^{e_1} Q_2^{e_2} \supset \cdots \supset Q_1^{e_1} \cdots Q_g^{e_g} = P\mathcal{O}_L.$$

Se Q é um ideal desta cadeia diferente de $P\mathcal{O}_L$, então Q/QQ_i é um espaço vetorial sobre \mathcal{O}_L/Q_i e $\dim_{\mathcal{O}_L/Q_i} Q/QQ_i = 1$, para $i = 1, \dots, g$.

Demonstração: Considere as aplicações:

$$\begin{aligned}
\oplus : Q/QQ_i \times Q/QQ_i &\longrightarrow Q/QQ_i \\
(x + QQ_i, y + QQ_i) &\longmapsto (x + y) + QQ_i \\
\otimes : \mathcal{O}_{\mathbb{L}}/Q_i \times Q/QQ_i &\longrightarrow Q/QQ_i \\
(\alpha + Q_i, y + QQ_i) &\longmapsto (\alpha y) + QQ_i
\end{aligned}$$

Temos que com estas operações Q/QQ_i é um espaço vetorial sobre $\mathcal{O}_{\mathbb{L}}/Q_i$, para $i = 1, \dots, g$. Agora, temos que os únicos subespaços de Q/QQ_i são os triviais. De fato, se existir um subespaço não trivial de Q/QQ_i , então ele é da forma B/QQ_i , onde $QQ_i \subsetneq B \subsetneq Q$, o que contraria o Lema (4.1.2). Assim, segue que $\dim_{\mathcal{O}_{\mathbb{L}}/Q_i} Q/QQ_i = 1$. ■

Teorema 4.1.1 *Com as notações anteriores, tem-se*

$$\sum_{i=1}^g e_i f_i = [\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}} : \mathcal{A}/P].$$

Demonstração: Pelo Lema (4.1.4), temos que Q/QQ_i é um espaço vetorial sobre $\mathcal{O}_{\mathbb{L}}/Q_i$ de dimensão 1 e como $[\mathcal{O}_{\mathbb{L}}/Q_i : \mathcal{A}/P] = f_i$, segue que $[Q/QQ_i : \mathcal{A}/P] = f_i$. Fixado um índice i , temos que existem exatamente e_i quocientes da forma Q/QQ_i , ou seja, existem exatamente e_i espaços vetoriais sobre \mathcal{A}/P de dimensão f_i . Agora, pelo Lema (4.1.3), temos que

$$\begin{aligned}
\dim_{\mathcal{A}/P} \mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}} &= \dim_{\mathcal{A}/P} (Q_1^{e_1} \cdots Q_g^{e_g-1} / Q_1^{e_1} \cdots Q_g^{e_g}) + \dim_{\mathcal{A}/P} (\mathcal{O}_{\mathbb{L}}/Q_1^{e_1} \cdots Q_g^{e_g-1}) \\
&= f_g + \dim_{\mathcal{A}/P} (\mathcal{O}_{\mathbb{L}}/Q_1^{e_1} \cdots Q_g^{e_g-1}) \\
&= f_g + \dim_{\mathcal{A}/P} (Q_1^{e_1} \cdots Q_g^{e_g-2} / Q_1^{e_1} \cdots Q_g^{e_g-1}) + \dim_{\mathcal{A}/P} (\mathcal{O}_{\mathbb{L}}/Q_1^{e_1} \cdots Q_g^{e_g-2}) \\
&= f_g + f_g + \dim_{\mathcal{A}/P} (\mathcal{O}_{\mathbb{L}}/Q_1^{e_1} \cdots Q_g^{e_g-2}) = \dots \\
&= e_g f_g + \dots + e_2 f_2 + (e_1 - 1) f_1 + \dim_{\mathcal{A}/P} \mathcal{O}_{\mathbb{L}}/Q_1 \\
&= \sum_{i=1}^g e_i f_i,
\end{aligned}$$

o que prova o teorema. ■

Lema 4.1.5 *Seja P um ideal primo de \mathcal{A} . Se \mathcal{A} for um anel principal, então*

$$[\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}} : \mathcal{A}/P] = n.$$

Demonstração: Como \mathcal{A} é um domínio principal, pelo Corolário (1.5.6), segue que $\mathcal{O}_{\mathbb{L}}$ é um \mathcal{A} -módulo livre de posto n . Seja $\{x_1, \dots, x_n\}$ uma base de $\mathcal{O}_{\mathbb{L}}$ sobre \mathcal{A} . Mostremos que $\{x_1 + P\mathcal{O}_{\mathbb{L}}, \dots, x_n + P\mathcal{O}_{\mathbb{L}}\}$ é uma base de $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$ sobre \mathcal{A}/P . De fato, primeiro mostremos que $\{x_1 + P\mathcal{O}_{\mathbb{L}}, \dots, x_n + P\mathcal{O}_{\mathbb{L}}\}$ gera $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$ sobre \mathcal{A}/P . Seja $\bar{b} \in \mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$. Temos que

$\bar{b} = b + P\mathcal{O}_{\mathbb{L}} = \sum_{i=1}^n a_i x_i + P\mathcal{O}_{\mathbb{L}}$; $a_i \in \mathcal{A}$, para todo $i = 1, \dots, n$, pois $b \in \mathcal{O}_{\mathbb{L}}$ e $\{x_1, \dots, x_n\}$ é uma base de $\mathcal{O}_{\mathbb{L}}$ sobre \mathcal{A} . Segue então que

$$\bar{b} = (a_1 x_1 + P\mathcal{O}_{\mathbb{L}}) + \dots + (a_n x_n + P\mathcal{O}_{\mathbb{L}}) = (a_1 + P)(x_1 + P\mathcal{O}_{\mathbb{L}}) + \dots + (a_n + P)(x_n + P\mathcal{O}_{\mathbb{L}}).$$

Mostremos agora que $\{x_1 + P\mathcal{O}_{\mathbb{L}}, \dots, x_n + P\mathcal{O}_{\mathbb{L}}\}$ é linearmente independente. Se $\sum_{i=1}^n (a_i + P)(x_i + P\mathcal{O}_{\mathbb{L}}) = 0$, então $\sum_{i=1}^n (a_i x_i + P\mathcal{O}_{\mathbb{L}}) = 0$, o que implica que $\left(\sum_{i=1}^n a_i x_i\right) + P\mathcal{O}_{\mathbb{L}} = 0$.

Desta forma, $\sum_{i=1}^n a_i x_i \in P\mathcal{O}_{\mathbb{L}}$, isto é, $\sum_{i=1}^n a_i x_i = \sum_{j=1}^s b_j p_j$, com $b_j \in \mathcal{O}_{\mathbb{L}}$ e $p_j \in P$, para todo $j = 1, \dots, s$. Como $\{x_1, \dots, x_n\}$ gera $\mathcal{O}_{\mathbb{L}}$ sobre \mathcal{A} , segue que $b_j = \sum_{i=1}^n c_{ij} x_i$; $c_{ij} \in \mathcal{A}$ para $i = 1, \dots, n$, $j = 1, \dots, s$. Assim,

$$\sum_{i=1}^n a_i x_i = \sum_{j=1}^s \left(\sum_{i=1}^n c_{ij} x_i \right) p_j = \sum_{i=1}^n \left(\sum_{j=1}^s c_{ij} p_j \right) x_i,$$

o que implica que $\sum_{i=1}^n \left(a_i - \sum_{j=1}^s c_{ij} p_j \right) x_i = 0$. Como $\{x_1, \dots, x_n\}$ é linearmente independente sobre \mathcal{A} , segue que $a_i = \sum_{j=1}^s c_{ij} p_j \in P$, ou seja, $a_i + P = 0 + P$, para $i = 1, \dots, n$. Logo $\{x_1 + P\mathcal{O}_{\mathbb{L}}, \dots, x_n + P\mathcal{O}_{\mathbb{L}}\}$ é uma base de $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$ sobre \mathcal{A}/P , isto é, $[\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}} : \mathcal{A}/P] = n$. ■

Proposição 4.1.2 *Sejam \mathcal{A} um anel de Dedekind, P um ideal primo de \mathcal{A} tal que $P\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^g Q_i^{e_i}$, onde os Q_i 's são ideais primos de $\mathcal{O}_{\mathbb{L}}$ e $f_i = [\mathcal{O}_{\mathbb{L}}/Q_i : \mathcal{A}/P]$. Nestas condições, tem-se que $[\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}} : \mathcal{A}/P] = n$.*

Demonstração: Sendo \mathcal{A} um anel de Dedekind e P é um ideal primo não nulo de \mathcal{A} , temos que se $S = \mathcal{A} - P$ então, pela Proposição (1.10.5), segue que $S^{-1}\mathcal{A}$ é um anel principal e pela Proposição (1.10.4), segue que $S^{-1}\mathcal{O}_{\mathbb{L}}$ é o anel dos inteiros de \mathbb{L} sobre $S^{-1}\mathcal{A}$. Logo, $S^{-1}\mathcal{O}_{\mathbb{L}}$ é um $S^{-1}\mathcal{A}$ -módulo livre de posto n . Daí, pelo Lema (4.1.5), tem-se que $[S^{-1}\mathcal{O}_{\mathbb{L}}/PS^{-1}\mathcal{O}_{\mathbb{L}} : S^{-1}\mathcal{A}/PS^{-1}\mathcal{A}] = n$. Considerando a fatoração do ideal $PS^{-1}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^g (S^{-1}\mathcal{O}_{\mathbb{L}}Q_i)^{e_i}$ e como $Q_i \cap \mathcal{A} = P$, $Q_i \cap S = \emptyset$ e $S^{-1}\mathcal{O}_{\mathbb{L}}Q_i$ são ideais primos não nulos de $S^{-1}\mathcal{O}_{\mathbb{L}}$ segue, pelo Teorema (4.1.1), que

$$[S^{-1}\mathcal{O}_{\mathbb{L}}/PS^{-1}\mathcal{O}_{\mathbb{L}} : S^{-1}\mathcal{A}/PS^{-1}\mathcal{A}] = \sum_{i=1}^g e_i [S^{-1}\mathcal{O}_{\mathbb{L}}/S^{-1}\mathcal{O}_{\mathbb{L}}Q_i : S^{-1}\mathcal{A}/PS^{-1}\mathcal{A}].$$

Agora, pelo Teorema (1.10.2), temos que $S^{-1}\mathcal{A}/PS^{-1}\mathcal{A} \simeq \mathcal{A}/P$ e $S^{-1}\mathcal{O}_{\mathbb{L}}/S^{-1}\mathcal{O}_{\mathbb{L}}Q_i \simeq \mathcal{O}_{\mathbb{L}}/Q_i$. Portanto,

$$n = [S^{-1}\mathcal{O}_{\mathbb{L}}/PS^{-1}\mathcal{O}_{\mathbb{L}} : S^{-1}\mathcal{A}/PS^{-1}\mathcal{A}] = \sum_{i=1}^g e_i f_i = [\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}} : \mathcal{A}/P],$$

onde a última igualdade segue do Teorema (4.1.1). \blacksquare

Teorema 4.1.2 (Igualdade Fundamental) *Sejam \mathcal{A} um anel de Dedekind, \mathbb{K} seu corpo de frações, \mathbb{L} uma extensão separável de \mathbb{K} de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de \mathbb{L} sobre \mathcal{A} . Se P é um ideal primo de \mathcal{A} tal que $P\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^g Q_i^{e_i}$, onde os Q_i 's são ideais primos de $\mathcal{O}_{\mathbb{L}}$ e $f_i = [\mathcal{O}_{\mathbb{L}}/Q_i : \mathcal{A}/P]$, então*

$$\sum_{i=1}^g e_i f_i = [\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}} : \mathcal{A}/P] = n.$$

Demonstração: A primeira igualdade segue do Teorema (4.1.1) e a segunda segue da Proposição (4.1.2). \blacksquare

Proposição 4.1.3 *Sejam \mathcal{A} um anel de Dedekind, \mathbb{K} seu corpo de frações, \mathbb{L} uma extensão separável de \mathbb{K} de grau n , \mathbb{N} uma extensão separável de \mathbb{L} de grau m , $\mathcal{O}_{\mathbb{L}}$ e $\mathcal{O}_{\mathbb{N}}$ os anéis de inteiros de \mathbb{L} e \mathbb{N} , respectivamente. Se I é um ideal primo de $\mathcal{O}_{\mathbb{N}}$ tal que $I \cap \mathcal{O}_{\mathbb{L}} = Q$ e $Q \cap \mathcal{A} = P$, então*

$$e(I|Q)e(Q|P) = e(I|P) \quad e$$

$$f(I|Q)f(Q|P) = f(I|P).$$

Demonstração: Temos, por definição, que

$$f(I|Q) = [\mathcal{O}_{\mathbb{N}}/I : \mathcal{O}_{\mathbb{L}}/Q] \quad e \quad f(Q|P) = [\mathcal{O}_{\mathbb{L}}/Q : \mathcal{A}/P].$$

Assim, temos, pela multiplicidade dos graus, que

$$f(I|P) = [\mathcal{O}_{\mathbb{N}}/I : \mathcal{A}/P] = [\mathcal{O}_{\mathbb{N}}/I : \mathcal{O}_{\mathbb{L}}/Q][\mathcal{O}_{\mathbb{L}}/Q : \mathcal{A}/P] = f(I|Q)f(Q|P).$$

Vamos mostrar a outra igualdade. Como $Q \cap \mathcal{A} = P$, segue que $P\mathcal{O}_{\mathbb{L}} = Q^{e(Q|P)}J$, onde J é um ideal de $\mathcal{O}_{\mathbb{L}}$ e Q não divide J . Analogamente, como $I \cap \mathcal{O}_{\mathbb{L}} = Q$, segue que $Q\mathcal{O}_{\mathbb{N}} = I^{e(I|Q)}R$, onde R é um ideal de $\mathcal{O}_{\mathbb{N}}$ e I não divide R . Assim, temos que $P\mathcal{O}_{\mathbb{N}} = (P\mathcal{O}_{\mathbb{L}})\mathcal{O}_{\mathbb{N}} = (Q^{e(Q|P)}J)\mathcal{O}_{\mathbb{N}} = (Q\mathcal{O}_{\mathbb{N}})^{e(Q|P)}(J\mathcal{O}_{\mathbb{N}}) = (I^{e(I|Q)}R)^{e(Q|P)}(J\mathcal{O}_{\mathbb{N}}) = I^{e(I|Q)e(Q|P)}R^{e(Q|P)}(J\mathcal{O}_{\mathbb{N}})$. Além

disso, I não divide $J\mathcal{O}_{\mathbb{N}}$, pois, caso contrário, teríamos que $J\mathcal{O}_{\mathbb{N}} \subset I$ e, assim, $J \subset J\mathcal{O}_{\mathbb{N}} \subset I$. Agora, como $J \subset \mathcal{O}_{\mathbb{L}}$, segue que $J \subset I \cap \mathcal{O}_{\mathbb{L}} = Q$, o que implica que Q divide J e isto é um absurdo. Desta forma, temos que I não divide $J\mathcal{O}_{\mathbb{N}}$ e I não divide R , portanto, $e(I|Q)e(Q|P)$ é o maior índice com o qual I divide $P\mathcal{O}_{\mathbb{N}}$. Assim,

$$e(I|P) = e(I|Q)e(Q|P),$$

o que prova a proposição. ■

Proposição 4.1.4 *Com as notações anteriores, tem-se que $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}} \simeq \prod_{i=1}^g \mathcal{O}_{\mathbb{L}}/Q_i^{e_i}$.*

Demonstração: Temos que Q_i é o único ideal maximal de $\mathcal{O}_{\mathbb{L}}$ que contém $Q_i^{e_i}$, para $i = 1, \dots, g$, pois se existir um outro ideal maximal M tal que $M \supset Q_i^{e_i}$ temos, pelo Lema (1.1.4), que $M \supset Q_i$. Como Q_i é maximal, segue que $M = Q_i$. Agora, vamos mostrar que $Q_i^{e_i} + Q_j^{e_j} = \mathcal{O}_{\mathbb{L}}$, para $i \neq j$. Suponhamos que $Q_i^{e_i} + Q_j^{e_j} \subsetneq \mathcal{O}_{\mathbb{L}}$. Assim, existe um ideal maximal M de $\mathcal{O}_{\mathbb{L}}$, tal que $Q_i^{e_i} + Q_j^{e_j} \subset M \subset \mathcal{O}_{\mathbb{L}}$. Como $Q_i^{e_i} \subset Q_i^{e_i} + Q_j^{e_j}$, segue que $Q_i^{e_i} \subset M$. Logo, $Q_i = M$. De modo análogo, como $Q_j^{e_j} \subset Q_i^{e_i} + Q_j^{e_j}$, segue que $Q_j^{e_j} \subset M$, assim $Q_j = M$. Assim, $Q_i = Q_j$, o que é um absurdo. Logo, $Q_i^{e_i} + Q_j^{e_j} = \mathcal{O}_{\mathbb{L}}$. Assim, pelo Lema (1.1.2), temos que $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}} \simeq \prod_{i=1}^g \mathcal{O}_{\mathbb{L}}/Q_i^{e_i}$. ■

Agora iremos provar o Teorema de Kummer. Este teorema, sob certas situações, nos auxilia a encontrar explicitamente a decomposição de um ideal primo estendido em um produto de ideais primos.

Definição 4.1.6 *Sejam \mathcal{A} um anel e $f(x) = \sum_{i=1}^n a_i x^i \in \mathcal{A}[x]$. Denotamos por $\bar{f}(x)$ o polinômio $\sum_{i=1}^n (a_i + P)x^i \in (\mathcal{A}/P)[x]$, onde P é um ideal primo não nulo de \mathcal{A} .*

Proposição 4.1.5 *Sejam \mathcal{A} um anel de Dedekind, \mathbb{K} seu corpo de frações, \mathbb{L} uma extensão separável de \mathbb{K} de grau n , $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de \mathbb{L} sobre \mathcal{A} tal que $\mathcal{O}_{\mathbb{L}} = \mathcal{A}[\beta]$, para algum $\beta \in \mathbb{L}$ e P um ideal primo não nulo de \mathcal{A} . Se $f(x) = \min_{\mathbb{K}} \beta$ e f_1, \dots, f_r são polinômios mônicos em $\mathcal{A}[x]$, tal que a fatoração de \bar{f} em polinômios irredutíveis distintos em $(\mathcal{A}/P)[x]$ seja dada por*

$$\bar{f} = \bar{f}_1^{e_1} \cdots \bar{f}_r^{e_r},$$

então ideais primos, dois a dois distintos, Q_1, \dots, Q_r de \mathcal{O}_L , que estão acima de P e satisfazem

$$\mathcal{O}_L/Q_j \simeq (\mathcal{A}/P)[\bar{\beta}_j],$$

onde $\bar{\beta}_j$ é uma raiz de \bar{f}_j . Além disso, $f(Q_j|P) = \text{grau}(f_j)$, para $j = 1, \dots, r$.

Demonstração: Para todo $j = 1, \dots, r$, seja $\bar{\beta}_j$ uma raiz de \bar{f}_j , em alguma extensão de A/P . Como \bar{f}_j é irredutível em $(\mathcal{A}/P)[x]$, segue que \bar{f}_j é o polinômio minimal de $\bar{\beta}_j$ sobre A/P . Além disso, $\bar{f}_i(\bar{\beta}_j) \neq 0$, para todo $i \neq j$, pois caso contrário, $\bar{f}_j | \bar{f}_i$, o que é um absurdo visto que \bar{f}_j, \bar{f}_i são irredutíveis. Agora, temos que o homomorfismo sobrejetor

$$\lambda_j : \mathcal{A}[x] \longrightarrow (\mathcal{A}/P)[\bar{\beta}_j]$$

$$h(x) \longmapsto \bar{h}(\bar{\beta}_j)$$

induz o homomorfismo sobrejetor

$$\bar{\lambda}_j : \mathcal{A}[x]/\langle f(x) \rangle \longrightarrow (\mathcal{A}/P)[\bar{\beta}_j],$$

uma vez que $\text{Ker}(\lambda_j) \supset \langle f(x) \rangle$. Por outro lado, o homomorfismo sobrejetor

$$\lambda : \mathcal{A}[x] \longrightarrow \mathcal{A}[\beta]$$

$$h(x) \longmapsto h(\beta)$$

tem como núcleo o ideal principal $\langle f(x) \rangle$. Portanto, λ induz um isomorfismo

$$\bar{\lambda} : \mathcal{A}[x]/\langle f(x) \rangle \longrightarrow \mathcal{A}[\beta]$$

$$h(x) + \langle f(x) \rangle \longmapsto h(\beta).$$

Resulta, então, que

$$\mu_j = \bar{\lambda}_j \circ (\bar{\lambda})^{-1} : \mathcal{A}[\beta] \longrightarrow (\mathcal{A}/P)[\bar{\beta}_j]$$

$$g(\beta) \longmapsto \bar{g}(\bar{\beta}_j)$$

é um homomorfismo sobrejetor. Como $(\mathcal{A}/P)[\bar{\beta}_j]$ é um corpo, segue que o núcleo de μ_j é um ideal maximal Q_j de $\mathcal{O}_{\mathbb{L}} = \mathcal{A}[\beta]$. Além disso, μ_j induz um isomorfismo

$$\bar{\mu}_j : \mathcal{A}[\beta]/Q_j \longrightarrow (\mathcal{A}/P)[\bar{\beta}_j]$$

$$g(\beta) + Q_j \longmapsto \bar{g}(\bar{\beta}_j).$$

Mostremos que Q_j está acima de P , para todo $j = 1, \dots, r$. Temos que $P \subset Q_j$, pois se $p \in P$ então $\mu_j(p) = \bar{p} = \bar{0}$. Logo, $P \subset Q_j \cap \mathcal{A} \neq \mathcal{A}$, pois Q_j é um ideal maximal de $\mathcal{O}_{\mathbb{L}}$. Como P é primo e \mathcal{A} é um domínio de Dedekind segue que P é maximal e, assim, $P = Q_j \cap \mathcal{A}$. Portanto, Q_j está acima de P , para todo $j = 1, \dots, r$. Mostremos que $Q_j \neq Q_i$, para todo $i \neq j$. Fixado j , temos que $\mu_j(f_j(\beta)) = \bar{f}_j(\bar{\beta}_j) = \bar{0}$, o que implica que $f_j(\beta) \in \text{Ker}(\mu_j) = Q_j$. Agora, $\mu_i(f_j(\beta)) = \bar{f}_j(\bar{\beta}_i) \neq \bar{0}$ pois $\bar{\beta}_i$ não é raiz de \bar{f}_j . Logo, $f_j(\beta) \notin \text{Ker}(\mu_i) = Q_i$, para todo $i \neq j$. Portanto, $Q_i \neq Q_j$, se $i \neq j$. Logo, Q_1, \dots, Q_r são dois a dois distintos. Finalmente, como $\bar{\mu}_j$ é um \mathcal{A}/P -isomorfismo de $\mathcal{A}[\beta]/Q_j$ sobre $(\mathcal{A}/P)[\bar{\beta}_j]$, segue que

$$f(Q_j|P) = [\mathcal{A}[\beta]/Q_j : \mathcal{A}/P] = [(\mathcal{A}/P)[\bar{\beta}_j] : \mathcal{A}/P] = \text{grau}(f_j),$$

para todo $j = 1, \dots, r$. ■

Teorema 4.1.3 (Teorema de Kummer) *Nas condições da Proposição (4.1.5), tem-se que se $\bar{f} = \bar{f}_1^{e_1} \cdots \bar{f}_r^{e_r}$ é a fatoração de \bar{f} em polinômios irredutíveis em $\mathcal{A}/P[x]$, então:*

$$\begin{aligned} P\mathcal{O}_{\mathbb{L}} &= Q_1^{e_1} \cdots Q_r^{e_r}, \text{ onde} \\ Q_j &= P\mathcal{O}_{\mathbb{L}} + f_j(\beta)\mathcal{O}_{\mathbb{L}}, \text{ para } j = 1, \dots, r, \\ e(Q_j|P) &= e_j, \text{ para } j = 1, \dots, r \text{ e} \\ f(Q_j|P) &= \text{grau } f_j, \text{ para } j = 1, \dots, r. \end{aligned}$$

Demonstração: Pela demonstração da Proposição (4.1.5), consideremos $Q_j = \text{Ker}(\mu_j)$, para $j = 1, \dots, r$, onde

$$\mu_j : \mathcal{A}[\beta] \longrightarrow (\mathcal{A}/P)[\bar{\beta}_j]$$

$$g(\beta) \longmapsto \bar{g}(\bar{\beta}_j),$$

com $\bar{\beta}_j$ uma raiz de $\bar{f}_j(x)$. Mostremos que $Q_j = P\mathcal{O}_{\mathbb{L}} + f_j(\beta)\mathcal{O}_{\mathbb{L}}$. Temos que, $P\mathcal{O}_{\mathbb{L}} + f_j(\beta)\mathcal{O}_{\mathbb{L}} \subset Q_j$, para $j = 1, \dots, r$, pois se $x \in P\mathcal{O}_{\mathbb{L}} + f_j(\beta)\mathcal{O}_{\mathbb{L}}$, então $x = \sum_{i=1}^s p_i y_i + f_j(\beta)w$, onde $p_i \in P$,

$y_i \in \mathcal{O}_L$ e $w \in \mathcal{O}_L$, para todo $i = 1, \dots, s$. Assim, $\mu_j(x) = \sum_{i=1}^s \bar{p}_i \bar{y}_i + \bar{f}_j(\bar{\beta}_j) \bar{w} = \bar{0}$, o que implica que $x \in \text{Ker}(\mu_j) = Q_j$. Por outro lado, $Q_j \subseteq P\mathcal{O}_L + f_j(\beta)\mathcal{O}_L$. De fato, se $\alpha \in Q_j$, então $\alpha = g(\beta)$ para algum $g(x) \in \mathcal{A}[x]$. Como $\bar{g}(\bar{\beta}_j) = \mu_j(g(\beta)) = 0$ e \bar{f}_j é o polinômio minimal de $\bar{\beta}_j$ sobre \mathcal{A}/P , segue que existe $h \in \mathcal{A}[x]$ tal que $\bar{g}(x) = \bar{f}_j(x)\bar{h}(x)$. Desta forma, $g(x) - f_j(x)h(x) \in P[x]$ e $\alpha = (g(\beta) - f_j(\beta)h(\beta)) + f_j(\beta)h(\beta) = (g - f_jh)(\beta) + f_j(\beta)h(\beta) \in P\mathcal{O}_L + f_j(\beta)\mathcal{O}_L$. Assim

$$Q_j = P\mathcal{O}_L + f_j(\beta)\mathcal{O}_L, \text{ para } j = 1, \dots, r.$$

Mostremos agora que Q_1, \dots, Q_r são os únicos ideais primos de \mathcal{O}_L que estão acima de P . Temos que $Q_1^{e_1} \dots Q_r^{e_r} \subseteq P\mathcal{O}_L$. De fato, uma vez que $(U + B)(U + B') \subseteq U + BB'$ para quaisquer ideais U, B, B' de \mathcal{O}_L , temos que $Q_1^{e_1} \dots Q_r^{e_r} \subseteq P\mathcal{O}_L + f_1(\beta)^{e_1} \dots f_r(\beta)^{e_r} \mathcal{O}_L$. Agora, como $\bar{f}(x) = \bar{f}_1(x)^{e_1} \dots \bar{f}_r(x)^{e_r}$, segue que $\bar{f}(x) - \bar{f}_1(x)^{e_1} \dots \bar{f}_r(x)^{e_r} = \bar{0}$. Desta forma, $f(x) - f_1(x)^{e_1} \dots f_r(x)^{e_r} \in P[x]$ e como $f(\beta) = 0$, então $f(\beta) - f_1(\beta)^{e_1} \dots f_r(\beta)^{e_r} = f_1(\beta)^{e_1} \dots f_r(\beta)^{e_r} \in P\mathcal{O}_L$. Assim, temos que $Q_1^{e_1} \dots Q_r^{e_r} \subseteq P\mathcal{O}_L$. Notemos que não existe um outro ideal primo M de \mathcal{O}_L que divide $P\mathcal{O}_L$. Assim, Q_1, \dots, Q_r são os únicos ideais primos de \mathcal{O}_L que estão acima de P , o que implica que $P\mathcal{O}_L = \prod_{j=1}^r Q_j^{e(Q_j|P)}$. Notemos que $e(Q_j|P) \leq e_j$, para todo $j = 1, \dots, r$. Pelo Teorema da Igualdade Fundamental (4.1.2), temos que $n = \sum_{j=1}^r e(Q_j|P)f(Q_j|P) = \sum_{j=1}^r e(Q_j|P) \text{ grau}(f_j) \leq \sum_{j=1}^r e_j \text{ grau}(f_j) = \text{grau } f = n$. Logo, $e(Q_j|P) = e_j$, para $j = 1, \dots, r$. ■

Exemplo 4.1.3 *Sejam $\mathcal{A} = \mathbb{Z}$, $\mathbb{K} = \mathbb{Q}$ e $\mathbb{L} = \mathbb{Q}(\sqrt{7})$. Temos que o anel de inteiros de \mathbb{L} sobre \mathcal{A} é $\mathcal{O}_L = \mathbb{Z}[\sqrt{7}]$, pois $7 \equiv 3 \pmod{4}$. Seja $P = \langle 3 \rangle$ um ideal primo de \mathbb{Z} . Temos que $\text{min}_{\mathbb{Q}} \sqrt{7} = x^2 - 7$. Agora,*

$$\bar{f}(x) = x^2 - \bar{7} = x^2 - \bar{1} = (\bar{1} + x)(\bar{2} + x) \pmod{\frac{\mathbb{Z}}{3\mathbb{Z}}[x]}.$$

Assim, pelo Teorema de Kummer (4.1.3), temos que

$$3\mathbb{Z}[\sqrt{7}] = PQ, \text{ onde } P = \langle 3, \sqrt{7} + 1 \rangle \text{ e } Q = \langle 3, \sqrt{7} + 2 \rangle.$$

Observação 4.1.5 *Um caso particular em que o Teorema de Kummer é utilizado é quando \mathbb{L} é um corpo de números. Neste caso, temos que $\mathcal{A} = \mathbb{Z}$ é um anel de Dedekind, $\mathbb{K} = \mathbb{Q}$ é o corpo de frações de \mathbb{Z} e \mathbb{L} é um extensão separável de \mathbb{K} . Se $\mathcal{O}_L = \mathbb{Z}[\beta]$, para algum $\beta \in \mathbb{L}$, podemos utilizar o Teorema.*

Exemplo 4.1.4 Sejam ζ_{24} uma raiz 24-ésima primitiva da unidade e $\mathbb{Q}(\zeta_{24})$ o 24-ésimo corpo ciclotômico. Temos que $\min_{\mathbb{Q}}\zeta_{24} = \phi_{24}(x) = x^8 - x^4 + 1$. Agora,

$$\bar{\phi}_{24}(x) = (x^2 + x + \bar{1})^4 \left(\text{mod } \frac{\mathbb{Z}}{2\mathbb{Z}}[x] \right) e$$

$$\bar{\phi}_{24}(x) = (x^2 + x + \bar{2})^2(x^2 + \bar{2}x + \bar{2})^2 \left(\text{mod } \frac{\mathbb{Z}}{3\mathbb{Z}}[x] \right).$$

Assim, pelo Teorema de Kummer (4.1.3), temos que

$$2\mathbb{Z}[\zeta_{24}] = Q^4, \text{ onde } Q = \langle 2, 1 + \zeta_{24} + \zeta_{24}^2 \rangle e$$

$$3\mathbb{Z}[\zeta_{24}] = S^2R^2, \text{ onde } S = \langle 3, 2 + \zeta_{24} + \zeta_{24}^2 \rangle e R = \langle 3, 2 + 2\zeta_{24} + \zeta_{24}^2 \rangle.$$

Exemplo 4.1.5 Sejam p um número primo, ζ_p uma raiz p -ésima primitiva da unidade e $\mathbb{Q}(\zeta_p)$ o p -ésimo corpo ciclotômico. Temos que $\min_{\mathbb{Q}}\zeta_p = \phi_p(x) = x^{p-1} + \dots + x + 1$. Agora,

$$\bar{\phi}_p(x) = (x - \bar{1})^{p-1} \left(\text{mod } \frac{\mathbb{Z}}{p\mathbb{Z}}[x] \right).$$

Assim, pelo Teorema de Kummer (4.1.3), temos que

$$p\mathbb{Z}[\zeta_p] = P^{p-1}, \text{ onde } P = \langle p, \zeta_p - 1 \rangle.$$

No que segue, sejam \mathcal{A} um domínio de Dedekind, \mathbb{K} seu corpo de frações, \mathbb{L} uma extensão de Galois de \mathbb{K} de grau n , $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de \mathbb{L} sobre \mathcal{A} e $G = Gal(\mathbb{L}|\mathbb{K})$ o grupo de Galois de \mathbb{L} sobre \mathbb{K} . Veremos que em extensões de Galois, dado um ideal primo P de \mathcal{A} , o ideal estendido $P\mathcal{O}_{\mathbb{L}}$ apresenta certas particularidades na sua decomposição como produto de primos.

Proposição 4.1.6 Se P é um ideal primo de \mathcal{A} e Q é um ideal primo de $\mathcal{O}_{\mathbb{L}}$ tal que $Q \cap \mathcal{A} = P$, então para todo $\sigma \in G$ temos que $\sigma(Q) \cap \mathcal{A} = P$.

Demonstração: Temos que $P \subseteq \sigma(Q) \cap \mathcal{A}$. De fato, como $Q \cap \mathcal{A} = P$, segue que $P = \sigma(P) = \sigma(Q \cap \mathcal{A}) \subseteq \sigma(Q) \cap \sigma(\mathcal{A}) = \sigma(Q) \cap \mathcal{A}$, pois σ fixa \mathcal{A} e P . Agora, como Q é um ideal primo de $\mathcal{O}_{\mathbb{L}}$, segue que $\sigma(Q)$ também o é. Pela Proposição (1.1.3), temos que $\sigma(Q) \cap \mathcal{A}$ é um ideal primo de \mathcal{A} . Como \mathcal{A} é um anel de Dedekind e $P \subset \sigma(Q) \cap \mathcal{A}$, segue que $P = \sigma(Q) \cap \mathcal{A}$, pois P é maximal e $\sigma(Q) \cap \mathcal{A} \neq \mathcal{A}$. ■

Observação 4.1.6 Pela Proposição (4.1.6), temos que se um ideal primo Q de $\mathcal{O}_{\mathbb{L}}$ está acima de um ideal primo P de \mathcal{A} então, para todo $\sigma \in G$, temos que $\sigma(Q)$ está acima de P , ou seja, se $P\mathcal{O}_{\mathbb{L}} = \left(\prod_{i=1}^g Q_i^{e_i} \right) Q^{e_Q}$, então $\sigma(Q) = Q$ ou $\sigma(Q) = Q_i$, para algum $i = 1, \dots, g$ e para todo $\sigma \in G$.

Definição 4.1.7 Sejam I, J ideais primos de $\mathcal{O}_{\mathbb{L}}$. Dizemos que I e J são **ideais primos conjugados** de $\mathcal{O}_{\mathbb{L}}$ se existe $\sigma \in G$ tal que $\sigma(I) = J$.

Proposição 4.1.7 Sejam \mathcal{A} um anel de Dedekind, \mathbb{K} seu corpo de frações e $\mathbb{L}|\mathbb{K}$ uma extensão de Galois. Se P é um ideal primo de \mathcal{A} , então os ideais primos Q_i de $\mathcal{O}_{\mathbb{L}}$ que estão acima de P são dois a dois conjugados, têm o mesmo grau de inércia f e têm o mesmo índice de ramificação e . Portanto,

$$P\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^g Q_i^e \quad e \quad n = efg.$$

Demonstração: Suponhamos, por absurdo, que existem ideais primos Q e Q' de $\mathcal{O}_{\mathbb{L}}$, acima de P tal que $\sigma(Q) \neq Q'$ para todo $\sigma \in G$. Em particular, $Q \neq Q'$. Como Q' é um ideal maximal de $\mathcal{O}_{\mathbb{L}}$, segue que $\sigma(Q')$ também o é. Assim, como Q e $\sigma(Q')$ são ideais maximais de $\mathcal{O}_{\mathbb{L}}$, segue que $Q \not\subset \sigma(Q')$, para todo $\sigma \in G$. Pelo Lema (1.1.3), existe um elemento $\alpha \in Q - \bigcup_{\sigma \in G} \sigma(Q')$.

Sendo α inteiro sobre \mathcal{A} , pois $\alpha \in Q \subset \mathcal{O}_{\mathbb{L}}$, temos que $N_{\mathbb{L}|\mathbb{K}}(\alpha) \in \mathcal{A}$. Agora, $\prod_{\sigma \in G} \sigma(\alpha) = N_{\mathbb{L}|\mathbb{K}}(\alpha)$ é um elemento de Q , pois existe $\sigma \in G$ tal que $\sigma(\alpha) = \alpha \in Q$ e assim $\prod_{\sigma \in G} \sigma(\alpha) = N_{\mathbb{L}|\mathbb{K}}(\alpha) \in Q$.

Portanto $N_{\mathbb{L}|\mathbb{K}}(\alpha) \in Q \cap \mathcal{A} = P$. Por outro lado, $\sigma(\alpha)$ não está em Q' , para todo $\sigma \in G$, pois caso contrário, teríamos que $\sigma^{-1}(\sigma(\alpha)) = \alpha \in \sigma^{-1}(Q')$, contrariando a hipótese feita sobre α .

Desta forma, $N_{\mathbb{L}|\mathbb{K}}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) \notin Q'$, pois Q' é um ideal primo e assim $P \not\subset Q' \cap \mathcal{A}$, o que é um absurdo. Agora, como um automorfismo preserva todas as relações algébricas, segue que preserva o índice de ramificação e o grau de inércia. Logo, $e_i = e$ e $f_i = f$, para todo i . Pelo

Teorema da Igualdade Fundamental (4.1.2), segue que $n = \sum_{i=1}^g e_i f_i = efg$. ■

Observação 4.1.7 Notemos que em extensões de Galois um ideal primo Q de $\mathcal{O}_{\mathbb{L}}$ se ramifica se, e somente se, Q está acima de um ideal primo P de \mathcal{A} que se ramifica em $\mathcal{O}_{\mathbb{L}}$. De fato, se Q se ramifica em $\mathcal{O}_{\mathbb{L}}$, então existe um ideal primo P de \mathcal{A} tal que $P\mathcal{O}_{\mathbb{L}} = \left(\prod_{i=1}^g Q_i^{e_i} \right) Q^{e_Q}$, onde $e_Q \geq 2$. Logo, P se ramifica. Agora, se P se ramifica em $\mathcal{O}_{\mathbb{L}}$, como $P\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^g Q_i^e$, segue que $e > 1$. Logo, todos os ideais que estão acima de P se ramificam em $\mathcal{O}_{\mathbb{L}}$.

Exemplo 4.1.6 *Sejam ζ_{20} uma raiz 20-ésima primitiva da unidade e $\mathbb{Q}(\zeta_{20})$ o 20-ésimo corpo ciclotômico. Temos que $\min_{\mathbb{Q}} \zeta_{20} = \phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1$. Agora,*

$$\bar{\phi}_{20}(x) = (x^4 + x^3 + x^2 + x + \bar{1})^2 \pmod{\frac{\mathbb{Z}}{2\mathbb{Z}}[x]} \text{ e}$$

$$\bar{\phi}_{20}(x) = (x + \bar{2})^4(x + \bar{3})^4 \pmod{\frac{\mathbb{Z}}{5\mathbb{Z}}[x]}.$$

Assim, pelo Teorema de Kummer (4.1.3), temos que

$$2\mathbb{Z}[\zeta_{20}] = Q^2, \text{ onde } Q = \langle 2, 1 + \zeta_{20} + \zeta_{20}^2 + \zeta_{20}^3 + \zeta_{20}^4 \rangle \text{ e}$$

$$5\mathbb{Z}[\zeta_{20}] = S^4 R^4, \text{ onde } S = \langle 5, 2 + \zeta_{20} \rangle \text{ e } R = \langle 5, 3 + \zeta_{20} \rangle.$$

Notemos que $\mathbb{Q}(\zeta_{20})|\mathbb{Q}$ é uma extensão de Galois e, como foi mostrado na Proposição (4.1.7), temos que

$$5\mathbb{Z}[\zeta_{20}] = (SR)^4.$$

Neste caso, temos que $e = 4$ e como $efg = n$, segue que $f(R|5) = f(S|5) = \frac{n}{eg} = \frac{\varphi(20)}{4 \cdot 2} = 1$.

Definição 4.1.8 *Seja P um ideal primo de \mathcal{A} . Para cada ideal primo Q de $\mathcal{O}_{\mathbb{L}}$ satisfazendo $Q \cap \mathcal{A} = P$, o conjunto*

$$D_{\mathbb{L}}(Q|P) = \{\sigma \in G; \sigma(Q) = Q\}$$

*é um subgrupo de $G = \text{Gal}(\mathbb{L}|\mathbb{K})$, chamado de **grupo de decomposição** de Q com relação ao ideal P .*

Observação 4.1.8 *Se \mathbb{L} é uma extensão abeliana de \mathbb{K} , os grupos $D_{\mathbb{L}}(Q_i|P)$, para $i = 1, \dots, g$, onde os Q_i 's são os ideais primos de $\mathcal{O}_{\mathbb{L}}$ acima de P , são todos iguais, dependendo somente do ideal P de \mathcal{A} . Neste caso, denotaremos tais grupos simplesmente por $D_{\mathbb{L}}(P)$. Desta forma, se g denota o número de ideais acima de P , então*

$$\text{card}(D_{\mathbb{L}}(P)) = \frac{n}{g} = ef.$$

4.2 Ramificação e Discriminante

Para esta seção, sejam \mathcal{A} um anel de Dedekind, \mathbb{K} seu corpo de frações, \mathbb{L} uma extensão finita de \mathbb{K} de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de \mathbb{L} sobre \mathcal{A} . Veremos os ideais primos de \mathcal{A} que se ramificam em $\mathcal{O}_{\mathbb{L}}$. Mostraremos que um ideal primo P de \mathcal{A} se ramifica em $\mathcal{O}_{\mathbb{L}}$ se, e somente

se P divide o ideal $D_{\mathbb{L}|\mathbb{K}}$. Desta forma, veremos que existe apenas um número finito de ideais primos de \mathcal{A} que se ramificam em $\mathcal{O}_{\mathbb{L}}$.

Observação 4.2.1 *Seja P um ideal primo de \mathcal{A} . Como \mathcal{A} é um anel de Dedekind, segue que $\mathcal{O}_{\mathbb{L}}$ é um anel noetheriano. Pela Proposição (1.2.3), temos que $\mathcal{O}_{\mathbb{L}}$ é noetheriano se, e somente se, $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$ é um anel noetheriano.*

Lema 4.2.1 *Tem-se que $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$ é um anel reduzido se, e somente se, $D_{(\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}})|(\mathcal{A}/P)} \neq \{0\}$.*

Demonstração: Como \mathcal{A} é um anel de Dedekind, pela Observação (4.2.1), segue que $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$ é um anel noetheriano. Suponha que $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$ é reduzido. Pelo Corolário (1.2.4), temos que $\langle \bar{0} \rangle = \bigcap_{i=1}^g R_i$, onde os R_i 's são ideais primos distintos de $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$. Para todo $i = 1, \dots, g$, como R_i é um ideal primo de $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$, segue que $(\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}})/R_i$ é um domínio. Além disso, $(\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}})/R_i$ é uma extensão finita e inteira de \mathcal{A}/P . Como \mathcal{A}/P é um corpo, pela Proposição (1.5.2), segue que $(\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}})/R_i$ é um corpo. Portanto, R_i é maximal, para todo $i = 1, \dots, g$. Desta forma, $R_i + R_j = \mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$, para todo $i \neq j$. Pelo Lema (1.1.2), temos que

$$\prod_{i=1}^g (\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}})/R_i \simeq (\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}})/\prod_{i=1}^g R_i = (\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}})/\langle \bar{0} \rangle = (\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}).$$

Assim, pelo Lema (1.6.2), temos que $D_{(\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}})|(\mathcal{A}/P)} = \prod_{i=1}^g D_{(\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}})/R_i|\mathcal{A}/P}$. Como $(\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}})/R_i$ e \mathcal{A}/P são corpos, pela Proposição (1.6.2), segue que $D_{((\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}})/R_i)|(\mathcal{A}/P)} \neq \{0\}$. Logo, $D_{(\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}})|(\mathcal{A}/P)} \neq \{0\}$. Reciprocamente, suponhamos que $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$ não é reduzido. Sejam $S = \mathcal{A} - P$, $\mathcal{A}' = S^{-1}\mathcal{A}$, $P' = PA'$ e $\mathcal{O}'_{\mathbb{L}} = S^{-1}\mathcal{O}_{\mathbb{L}}$. Temos que $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}} \simeq \mathcal{O}'_{\mathbb{L}}/P'\mathcal{O}'_{\mathbb{L}}$ e $\mathcal{A}/P \simeq \mathcal{A}'/P'$. Assim, temos que $\mathcal{O}'_{\mathbb{L}}/P'\mathcal{O}'_{\mathbb{L}}$ não é reduzido. Logo, existe $\bar{x} \in \mathcal{O}'_{\mathbb{L}}/P'\mathcal{O}'_{\mathbb{L}}$; $\bar{x} \neq \bar{0}$, \bar{x} nilpotente. Seja $\{\bar{x}_1, \dots, \bar{x}_n\}$ uma base de $\mathcal{O}'_{\mathbb{L}}/P'\mathcal{O}'_{\mathbb{L}}$ sobre \mathcal{A}'/P' com $\bar{x} = \bar{x}_1$. Temos que $\bar{x}\bar{x}_j$ é nilpotente, para todo $j = 1, \dots, n$. Logo, se definirmos $\sigma_{\bar{x}\bar{x}_j} : \mathcal{O}'_{\mathbb{L}}/P'\mathcal{O}'_{\mathbb{L}} \rightarrow \mathcal{O}'_{\mathbb{L}}/P'\mathcal{O}'_{\mathbb{L}}$, por $\sigma_{\bar{x}\bar{x}_j}(\bar{a}) = \bar{a}\bar{x}\bar{x}_j$, para $\bar{a} \in \mathcal{O}'_{\mathbb{L}}/P'\mathcal{O}'_{\mathbb{L}}$, temos que $\sigma_{\bar{x}\bar{x}_j}$ possui os autovalores todos nulos e, portanto, $Tr_{(\mathcal{O}'_{\mathbb{L}}/P'\mathcal{O}'_{\mathbb{L}})|(\mathcal{A}'/P')}(\bar{x}\bar{x}_j) = 0$. Logo, a matriz traço $(Tr_{(\mathcal{O}'_{\mathbb{L}}/P'\mathcal{O}'_{\mathbb{L}})|(\mathcal{A}'/P')}(\bar{x}\bar{x}_j))$ tem a primeira linha nula, o que implica que $D_{(\mathcal{O}'_{\mathbb{L}}/P'\mathcal{O}'_{\mathbb{L}})|(\mathcal{A}'/P')}(\bar{x}_1, \dots, \bar{x}_n) = \{0\}$ e, assim, $D_{(\mathcal{O}'_{\mathbb{L}}/P'\mathcal{O}'_{\mathbb{L}})|(\mathcal{A}'/P')} = \{0\}$, o que é um absurdo. Portanto, $D_{(\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}})|(\mathcal{A}/P)} \neq \{0\}$. ■

Teorema 4.2.1 *Um ideal primo P de \mathcal{A} se ramifica em $\mathcal{O}_{\mathbb{L}}$ se, e somente se, $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$ não é reduzido.*

Demonstração: Suponhamos que P se ramifica em $\mathcal{O}_{\mathbb{L}}$. Seja $P\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^g Q_i^{e_i}$, onde Q_i 's são ideais primos de $\mathcal{O}_{\mathbb{L}}$ e $e_i \geq 1$, para todo $i = 1, \dots, g$. Como P se ramifica, segue que existe $k \in \{1, \dots, g\}$ tal que $e_k > 1$. Temos, pela Proposição (4.1.4), que

$$\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{L}}/\prod_{i=1}^g Q_i^{e_i} \simeq \prod_{i=1}^g \mathcal{O}_{\mathbb{L}}/Q_i^{e_i}.$$

Mostremos que existe um elemento $\bar{x} = (x_1 + Q_1^{e_1}, \dots, x_g + Q_g^{e_g}) \in \prod_{i=1}^g \mathcal{O}_{\mathbb{L}}/Q_i^{e_i}$ tal que $\bar{x} \neq \bar{0}$ e \bar{x} é nilpotente. Como $e_k > 1$, segue temos que $Q_k^{e_k} \subsetneq Q_k$. Logo, existe $\alpha_k \in Q_k - Q_k^{e_k}$. Seja $\bar{x} = (0 + Q_1^{e_1}, \dots, 0 + Q_{k-1}^{e_{k-1}}, \alpha_k + Q_k^{e_k}, 0 + Q_{k+1}^{e_{k+1}}, \dots, 0 + Q_g^{e_g}) \neq \bar{0}$. Tomando $r = e_k$, temos que $\bar{x}^r = (0 + Q_1^{e_1}, \dots, 0 + Q_{k-1}^{e_{k-1}}, \alpha_k^{e_k} + Q_k^{e_k}, 0 + Q_{k+1}^{e_{k+1}}, \dots, 0 + Q_g^{e_g}) = \bar{0}$, pois $\alpha_k^{e_k} \in Q_k^{e_k}$. Logo, existe um elemento não nulo nilpotente em $\prod_{i=1}^g \mathcal{O}_{\mathbb{L}}/Q_i^{e_i}$ e como $\prod_{i=1}^g \mathcal{O}_{\mathbb{L}}/Q_i^{e_i} \simeq \mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$, segue que $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$ não é reduzido. Reciprocamente, suponha que $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$ não é reduzido. Sendo $P\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^g Q_i^{e_i}$, onde Q_i 's são ideais primos de $\mathcal{O}_{\mathbb{L}}$ e $e_i \geq 1$, para todo i , temos, pela Proposição (4.1.4), que $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}} \simeq \prod_{i=1}^g \mathcal{O}_{\mathbb{L}}/Q_i^{e_i}$. Do fato de $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$ não ser reduzido resulta que $\prod_{i=1}^g \mathcal{O}_{\mathbb{L}}/Q_i^{e_i}$ não é reduzido. Logo, existe $\bar{x} = (x_1 + Q_1^{e_1}, \dots, x_g + Q_g^{e_g}) \in \prod_{i=1}^g \mathcal{O}_{\mathbb{L}}/Q_i^{e_i}$ tal que $\bar{x} \neq \bar{0}$ e $\bar{x}^n = \bar{0}$, para algum $n \in \mathbb{N}^*$. Como $\bar{x} \neq \bar{0}$, segue que existe $k \in \{1, \dots, g\}$ tal que $x_k \notin Q_k^{e_k}$. Se $e_k = 1$, segue que $x_k \notin Q_k$. Agora $\bar{x}^n = (x_1^n + Q_1^{e_1}, \dots, x_g^n + Q_g^{e_g}) = \bar{0}$, o que implica que $x_k^n \in Q_k^{e_k}$. Como $e_k = 1$, então $x_k^n \in Q_k$. Sendo Q_k um ideal primo, temos que $x_k \in Q_k$, o que é um absurdo. Logo, $e_k > 1$. Portanto, P se ramifica em $\mathcal{O}_{\mathbb{L}}$. ■

Corolário 4.2.1 *Com as hipóteses do Teorema (4.2.1), P se ramifica em $\mathcal{O}_{\mathbb{L}}$ se, e somente se*

$$D_{(\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}})|(A/P)} = \{0\}.$$

Demonstração: Temos, pelo Teorema (4.2.1), que P se ramifica em $\mathcal{O}_{\mathbb{L}}$ se, e somente se, $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$ não é reduzido e, pelo Lema (4.2.1), temos que $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}$ não é reduzido se, e somente se, $D_{(\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}})|(A/P)} = \{0\}$. ■

Lema 4.2.2 *Sejam \mathcal{A}, \mathcal{B} anéis tal que \mathcal{A} é um subanel de \mathcal{B} , \mathcal{B} é um \mathcal{A} -módulo livre com base $\{x_1, \dots, x_n\}$ e P é um ideal primo de \mathcal{A} . Se $\bar{x} = x + P\mathcal{B} \in \mathcal{B}/P\mathcal{B}$, então $\{\bar{x}_1, \dots, \bar{x}_n\}$ é uma*

base de $\mathcal{B}/P\mathcal{B}$ sobre \mathcal{A}/P e

$$D_{(\mathcal{B}/P\mathcal{B})|(\mathcal{A}/P)}(\overline{x_1}, \dots, \overline{x_n}) = \overline{D_{\mathcal{B}|\mathcal{A}}(x_1, \dots, x_n)}.$$

Demonstração: Temos que $\{\overline{x_1}, \dots, \overline{x_n}\}$ é uma base de $\mathcal{B}/P\mathcal{B}$ sobre \mathcal{A}/P . Sejam $x \in \mathcal{B}$ e $\sigma_x : \mathcal{B} \rightarrow \mathcal{B}$ tal que $\sigma_x(a) = ax$, para todo $a \in \mathcal{B}$. Temos que

$$\begin{cases} \sigma_x(x_1) = xx_1 = a_{11}x_1 + \dots + a_{n1}x_n \\ \vdots \\ \sigma_x(x_n) = xx_n = a_{1n}x_1 + \dots + a_{nn}x_n. \end{cases}$$

Logo, $Tr_{\mathcal{B}|\mathcal{A}}(x) = \sum_{i=1}^n a_{ii}$. Agora, seja $\overline{\sigma_x} : \mathcal{B}/P\mathcal{B} \rightarrow \mathcal{B}/P\mathcal{B}$ tal que $\overline{\sigma_x}(\overline{a}) = \overline{ax}$, para todo $\overline{a} \in \mathcal{B}/P\mathcal{B}$. Temos que

$$\begin{cases} \overline{\sigma_x}(\overline{x_1}) = \overline{xx_1} = xx_1 + P\mathcal{B} = \overline{a_{11}}\overline{x_1} + \dots + \overline{a_{n1}}\overline{x_n} \\ \vdots \\ \overline{\sigma_x}(\overline{x_n}) = \overline{xx_n} = xx_n + P\mathcal{B} = \overline{a_{1n}}\overline{x_1} + \dots + \overline{a_{nn}}\overline{x_n}. \end{cases}$$

Logo, $Tr_{(\mathcal{B}/P\mathcal{B})|(\mathcal{A}/P)}(\overline{x}) = \sum_{i=1}^n \overline{a_{ii}}$. Assim, $Tr_{(\mathcal{B}/P\mathcal{B})|(\mathcal{A}/P)}(\overline{x}) = \overline{Tr_{\mathcal{B}|\mathcal{A}}(x)}$. Tomando $x_{ij} = x_i x_j$, temos que $Tr_{(\mathcal{B}/P\mathcal{B})|(\mathcal{A}/P)}(\overline{x_i x_j}) = \overline{Tr_{\mathcal{B}|\mathcal{A}}(x_i x_j)}$, para todo i, j . Logo,

$$D_{(\mathcal{B}/P\mathcal{B})|(\mathcal{A}/P)}(\overline{x_1}, \dots, \overline{x_n}) = \overline{D_{\mathcal{B}|\mathcal{A}}(x_1, \dots, x_n)},$$

o que prova o lema. ■

Teorema 4.2.2 *Um ideal primo P de \mathcal{A} se ramifica em $\mathcal{O}_{\mathbb{L}}$ se, e somente se, $D_{\mathbb{L}|\mathbb{K}} \subset P$.*

Demonstração: Sejam P um ideal primo de \mathcal{A} , $S = \mathcal{A} - P$, $\mathcal{A}' = S^{-1}\mathcal{A}$, $\mathcal{O}'_{\mathbb{L}} = S^{-1}\mathcal{O}_{\mathbb{L}}$ e $P' = \mathcal{A}'P$. Pela Proposição (1.10.5), temos que \mathcal{A}' é um anel principal e, assim, segue que $\mathcal{O}'_{\mathbb{L}}$ é um \mathcal{A}' -módulo livre de posto n . Seja $\{e_1, \dots, e_n\}$ uma base de $\mathcal{O}'_{\mathbb{L}}$ sobre \mathcal{A}' . Suponha que P se ramifica em $\mathcal{O}_{\mathbb{L}}$. Pelo Corolário (4.2.1), temos que como P se ramifica em $\mathcal{O}_{\mathbb{L}}$ segue que $D_{(\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}})|(\mathcal{A}/P)} = \{0\}$. Agora, temos que $\mathcal{A}/P \simeq \mathcal{A}'/P'$ e $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}} \simeq \mathcal{O}'_{\mathbb{L}}/P'\mathcal{O}'_{\mathbb{L}}$. Desta forma, $D_{(\mathcal{O}'_{\mathbb{L}}/P'\mathcal{O}'_{\mathbb{L}})|(\mathcal{A}'/P')} = \{0\}$. Agora, como $\{e_1, \dots, e_n\}$ é uma base de $\mathcal{O}'_{\mathbb{L}}$ sobre \mathcal{A}' , segue que $\{\overline{e_1}, \dots, \overline{e_n}\}$ é uma base de $\mathcal{O}'_{\mathbb{L}}/P'\mathcal{O}'_{\mathbb{L}}$ sobre \mathcal{A}'/P' . Logo, $D_{(\mathcal{O}'_{\mathbb{L}}/P'\mathcal{O}'_{\mathbb{L}})|(\mathcal{A}'/P')}$ é um ideal de \mathcal{A}'/P' gerado por $D_{(\mathcal{O}'_{\mathbb{L}}/P'\mathcal{O}'_{\mathbb{L}})|(\mathcal{A}'/P')}(\overline{e_1}, \dots, \overline{e_n})$ e, assim, $\overline{0} = D_{(\mathcal{O}'_{\mathbb{L}}/P'\mathcal{O}'_{\mathbb{L}})|(\mathcal{A}'/P')}(\overline{e_1}, \dots, \overline{e_n}) =$

$\overline{D_{\mathcal{O}'_{\mathbb{L}}|\mathcal{A}'}(e_1, \dots, e_n)} \in \mathcal{A}'/P'$ e, portanto, $D_{\mathcal{O}'_{\mathbb{L}}|\mathcal{A}'}(e_1, \dots, e_n) \in P'$. Agora, se $\{x_1, \dots, x_n\}$ é uma base de \mathbb{L} sobre \mathbb{K} contida em $\mathcal{O}_{\mathbb{L}}$, então $x_j \in \mathcal{O}'_{\mathbb{L}}$, para todo $j = 1, \dots, n$. Logo, $x_j = \sum_{i=1}^n a_{ij}e_i$, com $a_{ij} \in \mathcal{A}'$, $j = 1, \dots, n$. Desta forma, $D_{\mathcal{O}_{\mathbb{L}}|\mathcal{A}}(x_1, \dots, x_n) \in \mathcal{A}$ e $D_{\mathcal{O}'_{\mathbb{L}}|\mathcal{A}'}(x_1, \dots, x_n) = \det(a_{ij})^2 D_{\mathcal{O}'_{\mathbb{L}}|\mathcal{A}'}(e_1, \dots, e_n) \in \mathcal{A}'P' \subset P'$. Assim, $D(x_1, \dots, x_n) \in \mathcal{A} \cap P' = P$. Portanto, $D_{\mathbb{L}|\mathbb{K}} = \langle D_{\mathbb{L}|\mathbb{K}}(x_1, \dots, x_n) \rangle \subset P$. Reciprocamente, se $D_{\mathbb{L}|\mathbb{K}} \subset P$ e se $\{e_1, \dots, e_n\}$ é uma base de $\mathcal{O}'_{\mathbb{L}}$ sobre \mathcal{A}' , então para $i = 1, \dots, n$, temos que $e_i = \frac{y_i}{s_i}$, com $y_i \in \mathcal{O}_{\mathbb{L}}$ e $s_i \in S$. Assim,

$$\begin{aligned} D_{\mathbb{L}|\mathbb{K}}(e_1, \dots, e_n) &= \det(\text{Tr}_{\mathbb{L}|\mathbb{K}}(e_i e_j)) = \det\left(\text{Tr}_{\mathbb{L}|\mathbb{K}}\left(\frac{y_i y_j}{s_i s_j}\right)\right) \\ &= \frac{1}{s^{2n}} \det(\text{Tr}_{\mathbb{L}|\mathbb{K}}(y_i y_j)) = s^{-2n} D_{\mathbb{L}|\mathbb{K}}(y_1, \dots, y_n) \in \mathcal{A}' D_{\mathbb{L}|\mathbb{K}} \subseteq \mathcal{A}' P = P', \end{aligned}$$

ou seja, $D_{\mathbb{L}|\mathbb{K}}(e_1, \dots, e_n) \in P'$. Assim, $\overline{D_{\mathbb{L}|\mathbb{K}}(e_1, \dots, e_n)} = \bar{0}$ em \mathcal{A}'/P' e portanto, $D_{(\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}})|(\mathcal{A}/P)} = \{0\}$. Pelo Corolário (4.2.1), segue que P ramifica. ■

Exemplo 4.2.1 *Sejam ζ_9 uma raiz 9-ésima primitiva da unidade e $\mathbb{Q}(\zeta_9)$ o 9-ésimo corpo ciclotômico. Temos que $\langle \text{Disc}(\mathbb{Q}(\zeta_9)|\mathbb{Q}) \rangle = \langle 3^9 \rangle$. Logo, o único ideal primo de \mathbb{Z} que se ramifica em $\mathbb{Z}[\zeta_9]$ é o ideal $P = \langle 3 \rangle$, pois é o único ideal primo que divide o ideal gerado pelo discriminante.*

Exemplo 4.2.2 *Sejam ζ_{13} uma raiz 13-ésima primitiva da unidade e $\mathbb{Q}(\zeta_{13})$ o 13-ésimo corpo ciclotômico. Temos que $\langle \text{Disc}(\mathbb{Q}(\zeta_{13})|\mathbb{Q}) \rangle = \langle 13^{13-2} \rangle$. Logo, o único ideal primo de \mathbb{Z} que se ramifica em $\mathbb{Z}[\zeta_{13}]$ é o ideal $P = \langle 13 \rangle$, pois é o único ideal primo que divide o ideal gerado pelo discriminante.*

Corolário 4.2.2 *Com as hipóteses do Teorema (4.2.2), tem-se que existe somente um número finito de ideais primos de \mathcal{A} que ramificam em $\mathcal{O}_{\mathbb{L}}$.*

Demonstração: Temos que $D_{\mathbb{L}|\mathbb{K}} = \prod_{i=1}^g P_i^{e_i}$, onde P_i 's são ideais primos de \mathcal{A} . Pelo Teorema (4.2.2), temos que um ideal primo P de \mathcal{A} se ramifica se, e somente se, $D_{\mathbb{L}|\mathbb{K}} \subset P$. Agora, $D_{\mathbb{L}|\mathbb{K}} \subset P$ implica que $\prod_{i=1}^g P_i^{e_i} \subset P$. Como P é primo, segue que $P_i \subset P$ para algum $i = 1, \dots, g$. Como P_i é maximal, pois \mathcal{A} é Dedekind, segue que $P_i = P$, para algum $i = 1, \dots, g$. Assim, se ramificam em $\mathcal{O}_{\mathbb{L}}$ apenas os ideais primos P_1, \dots, P_g . ■

4.3 Ramificação e Diferente

Nesta seção apresentamos um resultado que relaciona os conceitos de diferente e ramificação. Para isto, sejam \mathcal{A} um domínio de Dedekind, \mathbb{K} seu corpo de frações, \mathbb{L} uma extensão separável

de \mathbb{K} de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros de \mathbb{L} sobre \mathcal{A} . Mostraremos que os ideais primos de $\mathcal{O}_{\mathbb{L}}$ que se ramificam são exatamente os ideais primos de $\mathcal{O}_{\mathbb{L}}$ que aparecem na fatoração do diferente.

Seja P um ideal primo não nulo de \mathcal{A} . Pelo Teorema (1.8.2), temos que $P\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^g Q_i^{e_i}$, onde os Q_i 's são ideais primos de $\mathcal{O}_{\mathbb{L}}$. Sejam

$$\psi : A \longrightarrow A/P, \quad \psi_0 : \mathcal{O}_{\mathbb{L}} \longrightarrow \mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}}, \quad \psi_i : \mathcal{O}_{\mathbb{L}} \longrightarrow \mathcal{O}_{\mathbb{L}}/Q_i,$$

os homomorfismos canônicos de anéis, para todo $i = 1, \dots, g$.

Seja $\pi_i : \mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}} \longrightarrow \mathcal{O}_{\mathbb{L}}/Q_i^{e_i}$ a i -ésima projeção induzida do isomorfismo natural $\mathcal{O}_{\mathbb{L}}/P\mathcal{O}_{\mathbb{L}} \simeq \prod_{i=1}^g \mathcal{O}_{\mathbb{L}}/Q_i^{e_i}$. Assim, se $y \in \mathcal{O}_{\mathbb{L}}$ então

$$\psi_0(y) = y + P\mathcal{O}_{\mathbb{L}} \text{ e } \pi_i(\psi_0(y)) = y + Q_i^{e_i}.$$

Essas funções são naturalmente estendidas para os polinômios, pela ação dos coeficientes.

Sejam $S = A - P$, $A' = S^{-1}A$, $\mathcal{O}'_{\mathbb{L}} = S^{-1}\mathcal{O}_{\mathbb{L}}$ e $P' = A'P$.

Omitimos a demonstração do próximo lema por ser muito longa.

Lema 4.3.1 ([5], pag. 190) *Se $x \in \mathcal{O}_{\mathbb{L}}$, então*

$$\psi(\text{Tr}_{\mathbb{L}|\mathbb{K}}(x)) = \sum_{j=1}^g e_j [\text{Tr}_{\mathcal{O}_{\mathbb{L}}/Q_i|A/P}(\psi_j(x))] \quad e$$

$$\psi(N_{\mathbb{L}|\mathbb{K}}(x)) = \prod_{j=1}^g [N_{\mathcal{O}_{\mathbb{L}}/Q_i|A/P}(\psi_j(x))]^{e_j}.$$

■

Observação 4.3.1 *Como $\Delta(\mathbb{L}|\mathbb{K})$ é um ideal de $\mathcal{O}_{\mathbb{L}}$ e $\mathcal{O}_{\mathbb{L}}$ é um domínio de Dedekind segue, pelo Teorema (1.8.2), que $\Delta(\mathbb{L}|\mathbb{K})$ pode ser escrito de modo único como*

$$\Delta(\mathbb{L}|\mathbb{K}) = \prod_{i=1}^r Q_i^{s_i},$$

onde Q_i 's são ideais primos de $\mathcal{O}_{\mathbb{L}}$ e $s_i > 0$ são inteiros.

Proposição 4.3.1 *Seja $\Delta(\mathbb{L}|\mathbb{K}) = \prod_{i=1}^r Q_i^{s_i}$, onde Q_i 's são ideais primos de $\mathcal{O}_{\mathbb{L}}$ e $s_i \geq 0$ são*

inteiros. Para todo $i = 1, \dots, r$, seja $P_i = Q_i \cap \mathcal{A}$. Se $P_i \mathcal{O}_{\mathbb{L}} = \left(\prod_{j=1}^k R_j^{a_j} \right) Q_i^{e_i}$ é a fatoração de $P_i \mathcal{O}_{\mathbb{L}}$ em um produto de ideais primos de $\mathcal{O}_{\mathbb{L}}$, então $s_i \geq e_i - 1$, para $i = 1, \dots, n$.

Demonstração: Sejam $Q_\lambda \in \{Q_1, \dots, Q_r\}$ e P_λ o ideal primo de \mathcal{A} tal que $Q_\lambda \cap \mathcal{A} = P_\lambda$. Como Q_λ está acima de P_λ , segue que

$$P_\lambda \mathcal{O}_{\mathbb{L}} = \left(\prod_{j=1}^k R_j^{a_j} \right) Q_\lambda^{e_\lambda},$$

onde R_j 's são ideais primos de $\mathcal{O}_{\mathbb{L}}$ e a_j 's são inteiros positivos. Sejam $S = \mathcal{A} - P_\lambda$, $\mathcal{A}' = S^{-1}\mathcal{A}$ e $\mathcal{O}'_{\mathbb{L}} = S^{-1}\mathcal{O}_{\mathbb{L}}$. Pelo Corolário (1.10.2), temos que $P_\lambda \mathcal{O}'_{\mathbb{L}} = \left(\prod_{j=1}^k \mathcal{O}'_{\mathbb{L}} R_j^{a_j} \right) \mathcal{O}'_{\mathbb{L}} Q_\lambda^{e_\lambda}$. Pela Proposição (3.2.4), temos que

$$\Delta_{P_\lambda}(\mathbb{L}|\mathbb{K}) = \mathcal{O}'_{\mathbb{L}} \Delta(\mathbb{L}|\mathbb{K}) = \prod_{i=1}^r \mathcal{O}'_{\mathbb{L}} Q_i^{s_i}.$$

Assim, temos que

$$\Delta_{P_\lambda}(\mathbb{L}|\mathbb{K})^{-1} = \prod_{i=1}^r \mathcal{O}'_{\mathbb{L}} Q_i^{-s_i}.$$

Mostremos que $s_\lambda \geq e_\lambda - 1$. Para isto, seja $x \in \left(\prod_{j=1}^k \mathcal{O}'_{\mathbb{L}} R_j^{1-a_j} \right) \mathcal{O}'_{\mathbb{L}} Q_\lambda^{1-e_\lambda}$. Vamos mostrar

que $x \in \Delta_{P_\lambda}(\mathbb{L}|\mathbb{K})^{-1} = \prod_{i=1}^r \mathcal{O}'_{\mathbb{L}} Q_i^{-s_i}$ e, assim, $\left(\prod_{j=1}^k \mathcal{O}'_{\mathbb{L}} R_j^{1-a_j} \right) \mathcal{O}'_{\mathbb{L}} Q_\lambda^{1-e_\lambda} \subseteq \prod_{i=1}^r \mathcal{O}'_{\mathbb{L}} Q_i^{-s_i}$, o que

implica que $1 - e_\lambda \geq -s_\lambda$ e, portanto, $s_\lambda \geq e_\lambda - 1$. Seja então $x \in \left(\prod_{j=1}^k \mathcal{O}'_{\mathbb{L}} R_j^{1-a_j} \right) \mathcal{O}'_{\mathbb{L}} Q_\lambda^{1-e_\lambda}$.

Como $P_\lambda' = \mathcal{A}' P_\lambda$ é um ideal principal de \mathcal{A}' , segue que existe $t \in \mathbb{K}$ tal que $P_\lambda' = \mathcal{A}' t$. Como $\mathcal{O}'_{\mathbb{L}} t = \mathcal{O}'_{\mathbb{L}} P_\lambda = \left(\prod_{j=1}^k \mathcal{O}'_{\mathbb{L}} R_j^{a_j} \right) \mathcal{O}'_{\mathbb{L}} Q_\lambda^{e_\lambda}$, segue que $xt \in \left(\prod_{j=1}^k \mathcal{O}'_{\mathbb{L}} R_j \right) \mathcal{O}'_{\mathbb{L}} Q_\lambda \subseteq \left(\bigcap_{j=1}^k \mathcal{O}'_{\mathbb{L}} R_j \right) \cap \mathcal{O}'_{\mathbb{L}} Q_\lambda$.

Desta forma, temos que $Tr_{\mathbb{L}|\mathbb{K}}(xt) \in \mathcal{A}' P_\lambda$. De fato, seja \mathbb{M} a menor extensão de Galois de \mathbb{K} contendo \mathbb{L} e $\mathcal{O}_{\mathbb{M}}$ seu anel de inteiros. Temos que $xt \in S^{-1} \mathcal{O}_{\mathbb{M}} \bar{Q}$ para todo ideal primo \bar{Q} de $\mathcal{O}_{\mathbb{M}}$ tal que $\bar{Q} \cap \mathcal{A} = P_\lambda$. O mesmo acontece para todos os conjugados de

xt em \mathbb{M} e, assim, $Tr_{\mathbb{M}|\mathbb{K}}(xt) = [\mathbb{M} : \mathbb{L}] Tr_{\mathbb{L}|\mathbb{K}}(xt) \in \left(\bigcap_{\bar{Q}} S^{-1} \mathcal{O}_{\mathbb{M}} \bar{Q} \right) \cap \mathcal{A}' = \mathcal{A}' P_\lambda$. Assim,

$Tr_{\mathbb{L}|\mathbb{K}}(xt) = t Tr_{\mathbb{L}|\mathbb{K}}(x) \in \mathcal{A}' P_\lambda = \mathcal{A}' t$. Portanto, $Tr_{\mathbb{L}|\mathbb{K}}(x) \in \mathcal{A}'$. Agora, se $y \in \mathcal{O}'_{\mathbb{L}}$, então

$xy \in \left(\prod_{i=1}^k \mathcal{O}'_{\mathbb{L}} R_i^{1-a_i} \right) \mathcal{O}'_{\mathbb{L}} Q_\lambda^{1-e_\lambda}$ e $Tr_{\mathbb{L}|\mathbb{K}}(xy) \in \mathcal{A}'$. Assim, $x \in \Delta_{P_\lambda}(\mathbb{L}|\mathbb{K})^{-1}$, como queríamos. ■

Teorema 4.3.1 *Seja $\Delta(\mathbb{L}|\mathbb{K}) = \prod_{i=1}^r Q_i^{s_i}$, onde Q_i 's são ideais primos de $\mathcal{O}_{\mathbb{L}}$ e $s_i \geq 0$, para todo $i = 1, \dots, n$. Fixado i , seja $P_i = Q_i \cap \mathcal{A}$. Se $P_i \mathcal{O}_{\mathbb{L}} = \left(\prod_{j=1}^k R_j^{a_j} \right) Q_i^{e_i}$, então $s_i = e_i - 1$ se, e somente se, a característica de $\mathcal{O}_{\mathbb{L}}/Q_i$ não divide o índice de ramificação e_i .*

Demonstração: Para simplificar a notação, faremos a demonstração para $i = 1$. Para os demais índices o processo é análogo. Sejam $P_1 = Q_1 \cap \mathcal{A}$, $S = \mathcal{A} - P_1$, $\mathcal{A}' = S^{-1}\mathcal{A}$, $P_1' = \mathcal{A}'P_1$ e $\mathcal{O}'_{\mathbb{L}} = S^{-1}\mathcal{O}_{\mathbb{L}}$. Suponha que a característica de $\mathcal{O}_{\mathbb{L}}/Q_1 \simeq \mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}Q_1$ divide o índice de ramificação e_1 . Seja

$$I = \mathcal{O}'_{\mathbb{L}}Q_1^{-e_1} \left(\prod_{j=1}^k \mathcal{O}'_{\mathbb{L}}R_j^{1-a_j} \right).$$

Se mostrarmos que $I \subseteq \Delta_{P_1}(\mathbb{L}|\mathbb{K})^{-1}$, teremos que $s_1 \geq e_1$, o que é um absurdo. Como \mathcal{A}' é principal, segue que $P_1 = t\mathcal{A}'$, onde $t \in \mathbb{K}$. Pela demonstração da Proposição (4.3.1), temos que $t \in \left(\prod_{j=1}^k \mathcal{O}'_{\mathbb{L}}R_j^{a_j} \right) \mathcal{O}'_{\mathbb{L}}Q_1^{e_1}$. Assim, dado $x \in I$, temos que $xt \in \prod_{j=1}^k \mathcal{O}'_{\mathbb{L}}R_j$. Logo,

$xt \in \bigcap_{j=1}^k \mathcal{O}'_{\mathbb{L}}R_j$. Pelo Lema (4.3.1), se $\psi : \mathcal{A}' \rightarrow \mathcal{A}'/P_1'$, $\psi_j : \mathcal{O}'_{\mathbb{L}} \rightarrow \mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}R_j$, $j = 1, \dots, k$ e $\psi_{k+1} : \mathcal{O}'_{\mathbb{L}} \rightarrow \mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}Q_1$ são os homomorfismos canônicos, então $\psi(\text{Tr}_{\mathbb{L}|\mathbb{K}}(xt)) = \sum_{j=1}^k a_j \text{Tr}_{(\mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}R_j)|(\mathcal{A}'/P_1')}(\psi_j(xt)) + e_1 \text{Tr}_{(\mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}Q_1)|(\mathcal{A}'/P_1')}(\psi_{k+1}(xt))$. Como $xt \in \mathcal{O}'_{\mathbb{L}}R_j$, para todo $j = 1, \dots, k$, segue que $\psi_j(xt) = \bar{0}$, para todo $j = 1, \dots, k$. Logo, $\psi(\text{Tr}_{\mathbb{L}|\mathbb{K}}(xt)) = e_1 \text{Tr}_{(\mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}Q_1)|(\mathcal{A}'/P_1')}(\psi_{k+1}(xt))$. Agora, como a característica de $\mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}Q_1$ divide e_1 , segue que $\psi(\text{Tr}_{\mathbb{L}|\mathbb{K}}(xt)) = 0$ e, assim, $\text{Tr}_{\mathbb{L}|\mathbb{K}}(xt) = t\text{Tr}_{\mathbb{L}|\mathbb{K}}(x) \in P_1' = \mathcal{A}'t$, ou seja, $\text{Tr}_{\mathbb{L}|\mathbb{K}}(x) \in \mathcal{A}'$. Dado $y \in \mathcal{O}'_{\mathbb{L}}$, temos que $xy \in I$ e $\text{Tr}_{\mathbb{L}|\mathbb{K}}(xy) \in \mathcal{A}'$, o que implica que $x \in \Delta_{P_1}(\mathbb{L}|\mathbb{K})^{-1}$, como queríamos. Reciprocamente, suponhamos que a característica de $\mathcal{O}_{\mathbb{L}}/Q_1 \simeq \mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}Q_1$ não divide o índice de ramificação e_1 . Seja $x \in \mathcal{O}'_{\mathbb{L}}$ um elemento tal que a imagem $\psi_{k+1}(x) \in \mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}Q_1$ tem o traço não nulo. Temos que existe $y \in \mathcal{O}'_{\mathbb{L}}$, tal que $y - x \in \mathcal{O}'_{\mathbb{L}}Q_1$ e $y \in \mathcal{O}'_{\mathbb{L}}R_j^{a_j}$, para $j = 1, 2, \dots, k$. Assim,

$$\psi(\text{Tr}_{\mathbb{L}|\mathbb{K}}(y)) = \sum_{j=1}^k a_j \text{Tr}_{(\mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}R_j)|(\mathcal{A}'/P_1')}(\psi_j(y)) + e_1 \text{Tr}_{(\mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}Q_1)|(\mathcal{A}'/P_1')}(\psi_{k+1}(x)) \neq 0,$$

pois e_1 não é múltiplo da característica de $\mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}Q_1$. Assim, $\text{Tr}_{\mathbb{L}|\mathbb{K}}(y) \notin P_1' = \mathcal{A}'t$. Logo $\text{Tr}_{\mathbb{L}|\mathbb{K}}\left(\frac{y}{t}\right) = \frac{1}{t}\text{Tr}_{\mathbb{L}|\mathbb{K}}(y) \notin \mathcal{A}'$. Isto mostra que $\frac{y}{t} \notin \Delta_{P_1}(\mathbb{L}|\mathbb{K})^{-1}$. Como $\mathcal{O}'_{\mathbb{L}}t = \mathcal{O}'_{\mathbb{L}}P_1$ e $y \in \mathcal{O}'_{\mathbb{L}}R_i^{a_i}$, para $i = 1, 2, \dots, k$, segue que $\frac{y}{t} \in \mathcal{O}'_{\mathbb{L}}Q_1^{-e_1} \not\subseteq \Delta_{P_1}(\mathbb{L}|\mathbb{K})^{-1}$ e assim não é verdade que

$-e_1 \geq -s_1$. Logo $e_1 > s_1 \geq e_1 - 1$ e portanto, $s_1 = e_1 - 1$. ■

Teorema 4.3.2 *Um ideal primo Q de $\mathcal{O}_{\mathbb{L}}$ se ramifica em $\mathcal{O}_{\mathbb{L}}$ se, e somente se, Q divide o diferente $\Delta(\mathbb{L}|\mathbb{K})$.*

Demonstração: Suponha que o ideal primo Q se ramifica em $\mathcal{O}_{\mathbb{L}}$. Temos que existe um ideal primo P de \mathcal{A} tal que $P\mathcal{O}_{\mathbb{L}} = \left(\prod_{i=1}^g R_i^{e_i} \right) Q^{e_Q}$, com $s_Q \geq 2$. Assim, pela Proposição (4.3.1), temos que $s_Q \geq e_Q - 1 \geq 1$. Logo, Q divide o diferente $\Delta(\mathbb{L}|\mathbb{K})$. Reciprocamente, suponha que Q não se ramifica em $\mathcal{O}_{\mathbb{L}}$. Assim, existe P um ideal primo de \mathcal{A} tal que $P\mathcal{O}_{\mathbb{L}} = \left(\prod_{i=1}^g R_i^{e_i} \right) Q$. Logo, $e_Q = 1$. Como a característica de $\mathcal{O}_{\mathbb{L}}/Q$ não divide o índice de ramificação e_Q temos, pelo Teorema (4.3.1), que $s_Q = e_Q - 1 = 0$. Logo, Q não divide o diferente, o que contradiz a hipótese. ■

Exemplo 4.3.1 *Sejam ζ_9 uma raiz 9-ésima primitiva da unidade e $\mathbb{Q}(\zeta_9)$ o 9-ésimo corpo ciclotômico. Como $\mathbb{Q}(\zeta_9)|\mathbb{Q}$ é uma extensão de Galois, temos que um ideal primo Q de $\mathbb{Z}[\zeta_9]$ se ramifica em $\mathbb{Z}[\zeta_9]$ se, e somente se, ele está acima de um ideal primo P de \mathbb{Z} que se ramifica em $\mathbb{Z}[\zeta_9]$. Pelo Exemplo (4.2.1), temos que o único ideal primo de \mathbb{Z} que se ramifica em $\mathbb{Z}[\zeta_9]$ é o ideal $P = \langle 3 \rangle$. Como $\phi_9(x) = x^6 + x^3 + 1 = \min_{\mathbb{Q}} \zeta_9$, segue que*

$$\bar{\phi}_9(x) = (\bar{2} + x)^6 \pmod{\frac{\mathbb{Z}}{3\mathbb{Z}}[x]}.$$

Assim, pelo Teorema de Kummer, temos que

$$3\mathbb{Z}[\zeta_9] = Q^6, \text{ com } Q = \langle 3, 2 + \zeta_9 \rangle.$$

Dessa forma, o único ideal primo de $\mathbb{Z}[\zeta_9]$ que se ramifica é o ideal Q . Agora, pelo Teorema (4.3.2), temos que o único ideal primo de $\mathbb{Z}[\zeta_9]$ que aparece na fatoração do diferente $\Delta(\mathbb{Q}(\zeta_9)|\mathbb{Q})$ é o ideal Q . Como $3^6 = |N_{\mathbb{L}|\mathbb{K}}(3)| = N(3\mathbb{Z}[\zeta_9]) = N(Q)^6$, segue que $N_{\mathbb{L}|\mathbb{K}}(Q) = 3$. Pelo Teorema (3.2.1), temos que $N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathbb{L}|\mathbb{K})) = |\text{Disc}(\mathbb{L}|\mathbb{K})| = 3^9$. Assim, temos que

$$\Delta(\mathbb{L}|\mathbb{K}) = Q^9.$$

4.4 Ramificação em Corpos Ciclotômicos

Sejam $\zeta_n = e^{\frac{2\pi i}{n}}$ uma raiz n -ésima primitiva da unidade e $\mathbb{Q}(\zeta_n)$ o n -ésimo corpo ciclotômico. Nesta seção estudaremos quais ideais primos P de \mathbb{Z} se ramificam em $\mathbb{Z}[\zeta_n]$ e quais ideais

primos Q de $\mathbb{Z}[\zeta_n]$ se ramificam em $\mathbb{Z}[\zeta_n]$. Com isto, será possível obter a fatoração do diferente $\Delta(\mathbb{Q}(\zeta_n)|\mathbb{Q})$. Além disso, dado um ideal primo Q de $\mathbb{Z}[\zeta_n]$ que divide $\Delta(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ veremos uma condição suficiente para que $\bar{Q} \neq Q$, onde $\bar{}$ denota a conjugação complexa.

Proposição 4.4.1 *Se $n \in \mathbb{N}^*$ é tal que $n \neq 2m$, para algum $m \in \mathbb{Z}$, m ímpar, então os únicos ideais primos de \mathbb{Z} que se ramificam em $\mathbb{Z}[\zeta_n]$ são da forma $P = \langle p \rangle$, onde p é primo e p divide n .*

Demonstração: Consideremos a extensão $\mathbb{Q}(\zeta_n)|\mathbb{Q}$. Sabemos que os ideais primos de \mathbb{Z} são da forma $P = \langle p \rangle$, onde p é um número primo. Pelo Teorema (3.2.3), temos que

$$D_{\mathbb{Q}(\zeta_n)|\mathbb{Q}} = \langle Disc(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \rangle = \left\langle \frac{n^{\varphi(n)}}{\prod_{i=1}^g p_i^{\frac{\varphi(n)}{p_i-1}}} \right\rangle,$$

onde $n = \prod_{i=1}^g p_i^{e_i}$, e φ é a função de Euler. Agora, temos que

$$\frac{n^{\varphi(n)}}{\prod_{i=1}^g p_i^{\frac{\varphi(n)}{p_i-1}}} = \frac{p_1^{e_1 \varphi(n)} \cdots p_g^{e_g \varphi(n)}}{p_1^{\frac{\varphi(n)}{p_1-1}} \cdots p_g^{\frac{\varphi(n)}{p_g-1}}}.$$

Seja

$$a_i = e_i \varphi(n) - \frac{\varphi(n)}{p_i - 1} = \frac{e_i(p_i - 1)\varphi(n) - \varphi(n)}{p_i - 1} = \frac{[e_i(p_i - 1) - 1]\varphi(n)}{p_i - 1}.$$

Como $\varphi(p_i^{e_i}) = (p_i - 1)p_i^{e_i-1}$ e $n \neq 2m$; m ímpar, segue que $a_i \geq 1$, para todo $i = 1, \dots, g$. Logo,

$$\langle Disc(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \rangle = \langle p_1^{a_1} \cdots p_g^{a_g} \rangle = \langle p_1 \rangle^{a_1} \cdots \langle p_g \rangle^{a_g}, \text{ com } a_i \geq 1, \text{ para todo } i = 1, \dots, g.$$

Assim, os únicos ideais primos que dividem $\langle Disc(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \rangle$ são $\langle p_i \rangle$, para $i = 1, \dots, g$. Pelo Teorema (4.2.2), são os únicos ideais primos de \mathbb{Z} que se ramificam em $\mathbb{Z}[\zeta_n]$. ■

Exemplo 4.4.1 *Sejam $n = 48$ e ζ_n uma raiz n -ésima primitiva da unidade. Temos que $48 = 2^4 \cdot 3$ e, assim, pela Proposição (4.4.1), temos que os únicos ideais primos de \mathbb{Z} que se ramificam em $\mathbb{Z}[\zeta_n]$ são $P_1 = \langle 2 \rangle$ e $P_2 = \langle 3 \rangle$.*

Observação 4.4.1 *Os ideais primos P de \mathbb{Z} são da forma $P = \langle p \rangle$, p primo. Deste modo,*

diremos simplesmente que p se ramifica em $\mathbb{Z}[\zeta_n]$ quando nos referirmos ao fato de o ideal primo P se ramificar em $\mathbb{Z}[\zeta_n]$.

Proposição 4.4.2 *Se ζ_n é uma raiz n -ésima primitiva da unidade com $n \neq 2m$; m ímpar, então os únicos ideais primos de $\mathbb{Z}[\zeta_n]$ que se ramificam em $\mathbb{Z}[\zeta_n]$ são os ideais que aparecem na fatoração de $p\mathbb{Z}[\zeta_n]$ para todo primo p tal que $p|n$.*

Demonstração: Como $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ é uma extensão de Galois, segue que um ideal primo Q de $\mathbb{Z}[\zeta_n]$ se ramifica em $\mathbb{Z}[\zeta_n]$ se, e somente se, Q está acima de um ideal primo P de \mathbb{Z} que se ramifica em $\mathbb{Z}[\zeta_n]$. Pela Proposição (4.4.1), temos que os ideais primos de \mathbb{Z} que se ramificam em $\mathbb{Z}[\zeta_n]$ são os ideais gerados por p tal que p é primo e $p|n$. Assim, se ramificam em $\mathbb{Z}[\zeta_n]$ os ideais primos que aparecem na fatoração de $p\mathbb{Z}[\zeta_n]$ tal que p é primo e $p|n$. ■

Corolário 4.4.1 *Se ζ_n é uma raiz n -ésima primitiva da unidade tal que $n \neq 2m$, com m ímpar, então os ideais primos de $\mathbb{Z}[\zeta_n]$ que aparecem na fatoração do diferente $\Delta(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ são exatamente os ideais primos de $\mathbb{Z}[\zeta_n]$ que estão acima dos ideais primos p de \mathbb{Z} tal que p é primo e $p|n$.*

Demonstração: Seja $\Delta(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ o diferente de $\mathbb{Q}(\zeta_n)$ sobre \mathbb{Q} . Pelo Teorema (4.3.2), temos que um ideal primo de $\mathbb{Z}[\zeta_n]$ se ramifica se, e somente se, ele aparece na fatoração do diferente. Pela Proposição (4.4.2), temos que se ramificam em $\mathbb{Z}[\zeta_n]$ os ideais primos que estão acima dos ideais p tal que p é primo e $p|n$. Portanto, são estes os ideais que aparecem na fatoração do diferente. ■

Observação 4.4.2 *Sejam ζ_n uma raiz n -ésima primitiva da unidade, $\mathbb{Q}(\zeta_n)$ o n -ésimo corpo ciclotômico e $p \in \mathbb{Z}$ um número primo. Como $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ é uma extensão de Galois segue, pela Proposição (4.1.7), que se $P = \langle p \rangle$, então*

$$p\mathbb{Z}[\zeta_n] = P\mathbb{Z}[\zeta_n] = \prod_{i=1}^g Q_i^e,$$

onde os Q_i 's são ideais primos de $\mathbb{Z}[\zeta_n]$, e é um inteiro positivo e $f(Q_i|P) = f$, para todo $i = 1, \dots, g$. Agora, pela Observação (4.1.8), como $\mathbb{Q}(\zeta_n)$ é uma extensão abeliana de \mathbb{Q} , segue que os grupos $D_{\mathbb{Q}(\zeta_n)}(Q_i|P)$, para $i = 1, \dots, g$, são todos iguais e iremos denotá-los por $D_{\mathbb{Q}(\zeta_n)}(p)$. Seja $\bar{\sigma}$ a conjugação complexa. Se $\bar{\sigma} \notin D_{\mathbb{Q}(\zeta_n)}(p)$, então $\bar{\sigma}(Q_i) \neq Q_i$, $\forall i = 1, \dots, g$. Mas, como $\bar{\sigma}(Q_i)$, $\forall i = 1, \dots, g$, é um ideal primo de $\mathbb{Z}[\zeta_n]$ que aparece na fatoração de $p\mathbb{Z}[\zeta_n]$, segue que para cada $i = 1, \dots, g$, existe um único índice $k \in \{1, \dots, g\}$, $k \neq i$, tal que

$\bar{\sigma}(Q_i) = \overline{Q_i} = Q_k$. Notemos também que $\overline{Q_k} = Q_i$. Sem perda de generalidade, podemos supor que $\overline{Q_g} = Q_1, \overline{Q_{g-1}} = Q_2, \dots$. Desta forma, reordenando os ideais de maneira conveniente, temos que se $\bar{\sigma} \notin D_{\mathbb{Q}(\zeta_n)}(p)$, então

$$p\mathbb{Z}[\zeta_n] = (Q_1 Q_2 \cdots Q_{g/2} \overline{Q_1} \overline{Q_2} \cdots \overline{Q_{g/2}})^e.$$

Pelo Teorema da Igualdade Fundamental (4.1.2), temos que $gef = \varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$. Desta forma, $g = \frac{\varphi(n)}{ef}$ é o número de ideais primos distintos que aparecem na fatoração de $p\mathbb{Z}[\zeta_n]$.

No que segue, iremos estudar quando $\bar{\sigma} \in D_{\mathbb{Q}(\zeta_n)}(p)$ para todo primo p tal que $p|n$.

Observação 4.4.3 Notemos que se $p \nmid n$, então p não se ramifica em $\mathbb{Z}[\zeta_n]$. Desta forma, $e = 1$ e $g = \frac{\varphi(n)}{f}$.

Observação 4.4.4 Seja p um número primo tal que $p|n$. Podemos escrever $n = p^k t$; $k \geq 1$ e $p \nmid t$. Como $p \nmid t$, segue que p não se ramifica em $\mathbb{Z}[\zeta_t]$, isto é, $p\mathbb{Z}[\zeta_t] = P_1 P_2 \cdots P_r$, onde os P_i 's são ideais primos distintos de $\mathbb{Z}[\zeta_t]$ e possuem o mesmo grau de inercia f .

Proposição 4.4.3 Sejam ζ_n uma raiz n -ésima primitiva da unidade e $n = p^k t$; $k \geq 1$, $p \nmid t$, p primo. Se $p\mathbb{Z}[\zeta_t] = P_1 P_2 \cdots P_r$; $P_i \neq P_j$ se $i \neq j$, é a decomposição de p em ideais primos de $\mathbb{Z}[\zeta_t]$, então

$$p\mathbb{Z}[\zeta_n] = (Q_1 Q_2 \cdots Q_r)^{\varphi(p^k)},$$

onde Q_1, \dots, Q_r são ideais primos de $\mathbb{Z}[\zeta_n]$ acima de P_1, \dots, P_r , respectivamente e $f(Q_i|P) = f(P_i|P)$, para todo $i = 1, \dots, r$.

Demonstração: Temos que $p\mathbb{Z}[\zeta_{p^k}] = R^{\varphi(p^k)}$, onde $R = (1 - \zeta_{p^k})\mathbb{Z}[\zeta_{p^k}]$ é um ideal primo de $\mathbb{Z}[\zeta_{p^k}]$. Já $p\mathbb{Z}[\zeta_t] = P_1 P_2 \cdots P_r$, onde os P_i 's são ideais primos distintos de $\mathbb{Z}[\zeta_t]$, com grau de inercia f . Fixemos Q_1, \dots, Q_r ideais primos de $\mathbb{Z}[\zeta_n]$ acima de P_1, \dots, P_r , respectivamente. Temos que Q_i está acima de p para todo i , pois $Q_i \cap \mathbb{Z} = Q_i \cap (\mathbb{Z}[\zeta_t] \cap \mathbb{Z}) = (Q_i \cap \mathbb{Z}[\zeta_t]) \cap \mathbb{Z} = P_i \cap \mathbb{Z} = p\mathbb{Z}$. Desta forma, segue que Q_i está acima de R , para todo $i = 1, \dots, r$. De fato, temos que $Q_i \cap \mathbb{Z}[\zeta_{p^k}]$ é um ideal primo de $\mathbb{Z}[\zeta_{p^k}]$ e como Q_i está acima de p , segue que $Q_i \cap \mathbb{Z}[\zeta_{p^k}] = R$, pois R é o único ideal primo de $\mathbb{Z}[\zeta_{p^k}]$ acima de p . Logo, $p\mathbb{Z}[\zeta_n] = (Q_1 \cdots Q_r Q_{r+1} \cdots Q_s)^{\bar{e}}$, onde Q_i 's são ideais primos de $\mathbb{Z}[\zeta_n]$, com grau de inercia \bar{f} . Pelo Teorema da Igualdade Fundamental (4.1.2), temos que $s\bar{e}\bar{f} = \varphi(n)$. Agora, temos que

$$\bar{e} = e(Q_i|p) = e(Q_i|R)e(R|p) = e(Q_i|R)\varphi(p^k) \quad e$$

$$\bar{f} = f(Q_i|p) = f(Q_i|P_i)f(P_i|p) = f(Q_i|P_i)f.$$

Assim, $\varphi(n) = s\bar{e}\bar{f} = se(Q_i|R)\varphi(p^k)f(Q_i|P_i)f \geq r\varphi(p^k)f = \varphi(p^k)\varphi(t) = \varphi(n)$, pois $r = \frac{\varphi(t)}{f}$. Logo, $se(Q_i|R)\varphi(p^k)f(Q_i|P_i)f = r\varphi(p^k)f$, o que implica que, $se(Q_i|R)f(Q_i|P_i) = r$, com $s \geq r$ e $e(Q_i|R) \geq 1$, $f(Q_i|P_i) \geq 1$. Portanto, $r = s$, $e(Q_i|R) = f(Q_i|P_i) = 1$. Desta forma, $\bar{e} = \varphi(p^k)$ e $\bar{f} = f$, o que implica que $p\mathbb{Z}[\zeta_n] = (Q_1 \cdots Q_r)^{\varphi(p^k)}$ e $f = f(Q_i|p) = f(P_i|p)$. ■

O próximo teorema segue sem demonstração por apresentar demonstração longa.

Teorema 4.4.1 ([6], pag. 76) *Se $\zeta_n = e^{\frac{2\pi i}{n}}$ e p um número primo tal que $n = p^k t$; $p \nmid t$ e $k \geq 0$, então $p\mathbb{Z}[\zeta_n] = (Q_1 \cdots Q_r)^e$, onde os Q_i 's são ideais primos de $\mathbb{Z}[\zeta_n]$, $e = \varphi(p^k)$ e $f = O_t(p)$ (ordem de p em \mathbb{Z}_t^*).* ■

Corolário 4.4.2 *Se $p \nmid n$, então existem $r = \frac{\varphi(n)}{f}$ ideais primos distintos de $\mathbb{Z}[\zeta_n]$ acima de p , onde $f = O_n(p)$ (ordem de p em $\mathbb{Z}[\zeta_n]^*$)*

Demonstração: Basta notar que se p não divide n , então $e = 1$. Logo, $r = \frac{\varphi(n)}{f}$, com $f = O_n(p)$ (ordem de p em $\mathbb{Z}[\zeta_n]^*$). ■

Exemplo 4.4.2 *Sejam $n = 18$ e $p = 5$. Temos que $p \nmid n$, assim pelo Corolário (4.4.2), existem $r = \frac{\varphi(18)}{f}$ ideais primos distintos de $\mathbb{Z}[\zeta_{18}]$ acima de 5, onde $f = O_{18}(5) = 6$. Logo, $r = \frac{\varphi(18)}{6} = \frac{6}{6} = 1$. Desta forma, existe um único ideal primo Q de $\mathbb{Z}[\zeta_{18}]$ tal que $5\mathbb{Z}[\zeta_{18}] = Q$. Segue que $5\mathbb{Z}[\zeta_{18}]$ é um ideal primo de $\mathbb{Z}[\zeta_{18}]$.*

Estamos interessados em saber se a conjugação complexa $\bar{\sigma} \in D_{\mathbb{Q}(\zeta_n)}(p)$, para todo n e todo p primo tal que p divide n . O próximo resultado de [12] nos dá uma condição necessária e suficiente para que a conjugação complexa pertença a $D_{\mathbb{Q}(\zeta_n)}(q)$ quando $n = pq$, com p, q primos distintos. No que segue, generalizamos este resultado para todo n e mostramos com um contra-exemplo, no final da seção, que no caso geral a condição é apenas suficiente e não necessária.

Corolário 4.4.3 ([12], pag. 69) *Se $n = pq$, com p, q primos distintos, então $\bar{\sigma} \in D_{\mathbb{Q}(\zeta_{pq})}(q)$ se, e somente se, $O_p(q) \equiv 0 \pmod{2}$.* ■

Proposição 4.4.4 *Sejam $n = p^k t$; $k \geq 1$, $p \nmid t$, p primo, $\mathbb{L} = \mathbb{Q}(\zeta_n)$, $\mathbb{K} = \mathbb{Q}(\zeta_t)$ e $\bar{\sigma}$ a conjugação complexa. Se $\bar{\sigma} \in D_{\mathbb{L}}(p)$, então $\bar{\sigma} \in D_{\mathbb{K}}(p)$.*

Demonstração: Como $p \nmid t$, segue que p não se ramifica em $\mathbb{Z}[\zeta_t]$. Desta forma, $p\mathbb{Z}[\zeta_t] = P_1 P_2 \cdots P_r$, onde os P_i 's são ideais primos distintos de $\mathbb{Z}[\zeta_t]$. Pela Proposição (4.4.3), temos que $p\mathbb{Z}[\zeta_n] = (Q_1 \cdots Q_r)^{\varphi(p^k)}$, onde os Q_i 's são ideais primos distintos de $\mathbb{Z}[\zeta_n]$ e Q_i está acima de P_i , para todo $i = 1, \dots, r$. Se $\bar{\sigma} \in D_{\mathbb{L}}(p)$, então $\bar{\sigma}(Q_i) = Q_i$, para todo $i = 1, \dots, r$. Agora, temos que $\bar{\sigma}(P_i) = \bar{\sigma}(Q_i \cap \mathbb{Z}[\zeta_t]) \subset \bar{\sigma}(Q_i) \cap \bar{\sigma}(\mathbb{Z}[\zeta_t]) = Q_i \cap \mathbb{Z}[\zeta_t] = P_i$, para todo $i = 1, \dots, r$. Como $\bar{\sigma}(P_i)$ e P_i são ideais primos de $\mathbb{Z}[\zeta_t]$ e $\mathbb{Z}[\zeta_t]$ é um anel de Dedekind, segue que $\bar{\sigma}(P_i) = P_i$, para todo $i = 1, \dots, r$, o que implica que $\bar{\sigma} \in D_{\mathbb{K}}(p)$. ■

Proposição 4.4.5 *Com as notações da Proposição (4.4.4), se $\bar{\sigma} \in D_{\mathbb{K}}(p)$, então $O_t(p) \equiv 0 \pmod{2}$.*

Demonstração: Como $p \nmid t$, pelo Corolário (4.4.2), segue que existem $r = \frac{\varphi(t)}{O_t(p)}$ ideais primos distintos de $\mathbb{Z}[\zeta_t]$ acima de p . Mas, pela Observação (4.1.8), temos que $\text{card}(D_{\mathbb{K}}(p)) = \frac{\varphi(t)}{r} = O_t(p)$. Assim, se $\bar{\sigma} \in D_{\mathbb{K}}(p)$, então $O(\bar{\sigma}) = 2$ divide $\text{card}(D_{\mathbb{K}}(p)) = O_t(p)$. Desta forma, segue que $O_t(p) \equiv 0 \pmod{2}$. ■

Corolário 4.4.4 *Nas condições anteriores, se $O_t(p) \equiv 1 \pmod{2}$, então $\bar{\sigma} \notin D_{\mathbb{L}}(p)$.*

Demonstração: Notemos que se $\bar{\sigma} \in D_{\mathbb{L}}(p)$, pela Proposição (4.4.4), segue que $\bar{\sigma} \in D_{\mathbb{K}}(p)$ e, pela Proposição (4.4.5), que $O_t(p) \equiv 0 \pmod{2}$. Logo, se $O_t(p) \equiv 1 \pmod{2}$, então $\bar{\sigma} \notin D_{\mathbb{L}}(p)$. ■

Exemplo 4.4.3 *Sejam $n = 20$ e $\mathbb{L} = \mathbb{Q}(\zeta_{20})$. Temos que $20 = 2^2 5$. Agora, $O_{2^2}(5) = 1 \equiv 1 \pmod{2}$, o que implica que $\bar{\sigma} \notin D_{\mathbb{L}}(5)$. Pelo Exemplo (4.1.6), temos que $5\mathbb{Z}[\zeta_{20}] = (SR)^4$. Desta forma, como $\bar{\sigma} \notin D_{\mathbb{L}}(5)$, segue que $\bar{S} = R$ e, assim,*

$$5\mathbb{Z}[\zeta_{20}] = (\bar{S}S)^4.$$

Observação 4.4.5 *Notemos que $O_t(p) \equiv 0 \pmod{2}$ não implica que $\bar{\sigma} \in D_{\mathbb{L}}(p)$. O próximo exemplo mostra isso.*

Exemplo 4.4.4 *Sejam $\mathbb{L} = \mathbb{Q}(\zeta_{24})$ e $\zeta = \zeta_{24}$. Temos que $\phi_{24}(x) = x^8 - x^4 + 1 = \min_{\mathbb{Q}} \zeta_{24}$ e, assim,*

$$\bar{\phi}_{24}(x) = (\bar{2} + x + x^2)^2 (\bar{2} + \bar{2}x + x^2)^2 \pmod{\frac{\mathbb{Z}}{3\mathbb{Z}}[x]}.$$

Desta forma, pelo Teorema de Kummer (4.1.3), temos que

$$3\mathbb{Z}[\zeta_{24}] = S^2 R^2, \text{ onde } S = \langle 3, 2 + \zeta + \zeta^2 \rangle \text{ e } R = \langle 3, 2 + 2\zeta + \zeta^2 \rangle.$$

Agora, temos que $O_8(3) = 2 \equiv 0 \pmod{2}$ e, no entanto, $\bar{\sigma} \notin D_{\mathbb{L}}(3)$. De fato, mostremos que $\bar{S} = R$. Seja $x = 3(a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4 + a_5\zeta^5 + a_6\zeta^6 + a_7\zeta^7) + (2 + \zeta + \zeta^2)(b_0 + b_1\zeta + b_2\zeta^2 + b_3\zeta^3 + b_4\zeta^4 + b_5\zeta^5 + b_6\zeta^6 + b_7\zeta^7) \in S$, onde $a_i, b_i \in \mathbb{Z}$, para todo $i = 0, 1, \dots, 7$. Temos que $\bar{x} = (3a_0 + 3a_4 + 2b_0 + b_2 + b_3 + 2b_4) + (3a_3 + b_1 + b_2 + 2b_3)\zeta + (3a_2 + b_0 + b_1 + 2b_2)\zeta^2 + (3a_1 + b_0 + 2b_1 - b_7)\zeta^3 + (-3a_4 - b_2 - b_3 - 2b_4 - b_6 - b_7)\zeta^4 + (-3a_3 - 3a_7 - b_1 - b_2 - 2b_3 - b_5 - b_6 - 2b_7)\zeta^5 + (-3a_2 - 3a_6 - b_0 - b_1 - 2b_2 - b_4 - b_5 - 2b_6)\zeta^6 + (-3a_1 - 3a_5 - b_0 - 2b_1 - b_3 - b_4 - 2b_5)\zeta^7$. Assim, se $\bar{x} \in R = \langle 3, 2 + 2\zeta + \zeta^2 \rangle$, então $\bar{x} = 3(d_0 + d_1\zeta + d_2\zeta^2 + d_3\zeta^3 + d_4\zeta^4 + d_5\zeta^5 + d_6\zeta^6 + d_7\zeta^7) + (2 + 2\zeta + \zeta^2)(f_0 + f_1\zeta + f_2\zeta^2 + f_3\zeta^3 + f_4\zeta^4 + f_5\zeta^5 + f_6\zeta^6 + f_7\zeta^7)$, para inteiros d_i, f_i , com $i = 0, 1, \dots, 7$. Fazendo as contas, temos que se tomarmos $d_0 = 0$, $d_1 = a_3 - b_1 + 11b_2 + 6b_3$, $d_2 = a_2 - b_0 - b_1 + 6b_2$, $d_3 = a_1 - b_0 + b_7$, $d_4 = a_0 + b_6 + b_7$, $d_5 = -a_3 - a_7 + b_1 + b_2 + b_5 + b_6$, $d_6 = 2a_0 - a_2 + 2a_4 - a_6 + b_0 + b_1 + b_4 + b_5$, $d_7 = 2a_0 - a_1 + 2a_4 - a_5 + b_0 + b_4$, $f_0 = 0$, $f_1 = 2b_1 - 16b_2 - 8b_3$, $f_2 = 2b_0 + 8b_2 + 8b_3$, $f_3 = -4b_3 - 2b_7$, $f_4 = -4b_2 - 2b_6$, $f_5 = -2b_1 + 2b_2 + b_3 - 2b_5$, $f_6 = -3a_0 - 3a_4 - 2b_0 - b_2 - b_3 - 2b_4 - 4 + 3d_0$ e $f_7 = 0$ temos que $\bar{x} \in R$. Logo, $\bar{S} \subset R$. Como \bar{S} e R são ideais maximais, segue que $\bar{S} = R$. Portanto, $\bar{\sigma} \notin D_{\mathbb{L}}(3)$.

Capítulo 5

Reticulados no \mathbb{R}^n

Neste capítulo, veremos o conceito de reticulados no \mathbb{R}^n . Este conceito surgiu a partir do problema de como cobrir o espaço \mathbb{R}^n com esferas de mesmo raio, de forma que quaisquer duas esferas se toquem em apenas um ponto e ocupem a maior parte do espaço possível. Na Seção 5.1, apresentamos a definição de reticulados no \mathbb{R}^n , alguns exemplos, alguns parâmetros e algumas de suas principais propriedades. Na Seção 5.2, apresentamos os conceitos de empacotamento esférico e empacotamento reticulado.

5.1 Definição

Nesta seção, apresentamos a definição de reticulados no \mathbb{R}^n e alguns de seus parâmetros, como matriz de Gram, determinante do reticulado, diversidade e distância produto mínima.

Definição 5.1.1 *Seja $\beta = \{v_1, \dots, v_m\}$ um conjunto de vetores do \mathbb{R}^n linearmente independentes sobre \mathbb{R} , com $m \leq n$. Chamamos de **reticulado de dimensão m** ao subconjunto do \mathbb{R}^n da forma*

$$\mathcal{H}_\beta = \left\{ x \in \mathbb{R}^n \text{ tal que } x = \sum_{i=1}^m a_i v_i \text{ com } a_i \in \mathbb{Z} \right\}.$$

*O conjunto β é chamado de **base** de \mathcal{H}_β .*

Observação 5.1.1 *Notemos que um reticulado \mathcal{H}_β no \mathbb{R}^n é um subespaço vetorial do \mathbb{R}^n . Desta forma, \mathcal{H}_β é um subgrupo aditivo do $(\mathbb{R}^n, +)$. Em particular, a soma ou a diferença de quaisquer dois vetores do reticulado é ainda um vetor do reticulado.*

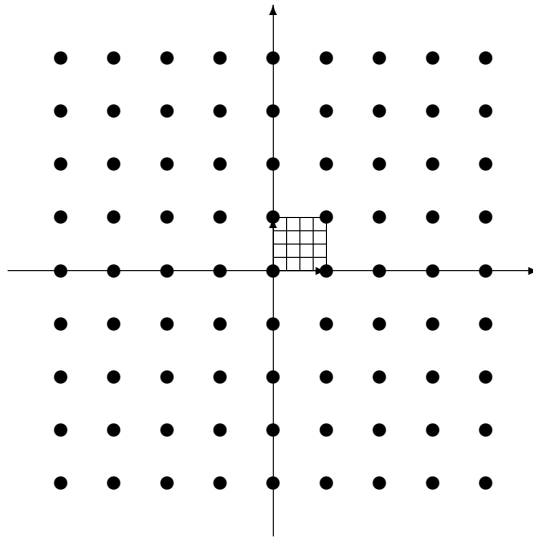
Observação 5.1.2 *Notemos também que \mathcal{H}_β é um conjunto de pontos discretos, ou seja, para qualquer conjunto compacto \mathcal{K} do \mathbb{R}^n , temos que $\mathcal{H}_\beta \cap \mathcal{K}$ é finito.*

Definição 5.1.2 Seja $\mathcal{H}_\beta \subset \mathbb{R}^n$ um reticulado com base $\beta = \{v_1, \dots, v_m\}$, $m \leq n$. O conjunto

$$\mathcal{P}_\beta = \left\{ x \in \mathbb{R}^n : x = \sum_{i=1}^m \lambda_i v_i, 0 \leq \lambda_i < 1 \right\},$$

é chamado de **região fundamental** ou **domínio fundamental** de \mathcal{H}_β com relação a base $\beta = \{v_1, \dots, v_m\}$.

Exemplo 5.1.1 Consideremos $\beta = \{(1, 0), (0, 1)\}$. O reticulado \mathcal{H}_β gerado por β é dado por $\mathcal{H}_\beta = \{a(1, 0) + b(0, 1); a, b \in \mathbb{Z}\} = \{(a, b); a, b \in \mathbb{Z}\} = \mathbb{Z}^2$. A figura a seguir mostra o reticulado e sua região fundamental.



No que segue, consideraremos apenas o caso em que $m = n$, ou seja, estudaremos reticulados n -dimensionais no \mathbb{R}^n .

Existem muitas bases diferentes que podem definir um mesmo reticulado. A proposição seguinte nos dá uma condição necessária e suficiente para que um conjunto de vetores linearmente independentes seja uma base de um dado reticulado.

Proposição 5.1.1 Sejam \mathcal{H}_β um reticulado com base $\beta = \{v_1, \dots, v_n\}$ e $\{e_1, \dots, e_n\}$ um conjunto de vetores de \mathcal{H}_β linearmente independentes tal que $e_i = \sum_{j=1}^n a_{ij} v_j$, com $a_{ij} \in \mathbb{Z}$. Tem-se que $\{e_1, \dots, e_n\}$ é uma base de \mathcal{H}_β se, e somente se, $\det(A) = \pm 1$, onde $A = (a_{ij})_{i,j=1}^n$.

Demonstração: Sejam $\beta = \{v_1, \dots, v_n\}$ uma base de \mathcal{H}_β e $\{e_1, \dots, e_n\}$ um conjunto de vetores de \mathcal{H}_β linearmente independentes tal que

$$\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}.$$

Temos que $\{e_1, \dots, e_n\}$ é uma base de \mathcal{H}_β se, e somente se, $A = (a_{ij})_{i,j=1}^n$ é a matriz mudança de base, o que é equivalente a $\det(A) = \pm 1$. ■

Observação 5.1.3 *Seja um reticulado \mathcal{H}_β no \mathbb{R}^n . Uma vez que \mathcal{H}_β pode ser definido por mais de uma base, passaremos a denotá-lo por Λ ao invés de \mathcal{H}_β .*

Definição 5.1.3 *Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado e $\beta = \{v_1, \dots, v_n\}$ uma base de Λ . Se $v_i = (v_{i1}, \dots, v_{in})$, para $i = 1, \dots, n$, chamamos de **matriz geradora** do reticulado Λ a matriz*

$$M = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \cdots & v_{nn} \end{pmatrix}.$$

A matriz $G = MM^t$, onde t denota a transposta, é chamada de **matriz de Gram** do reticulado.

Com as mesmas hipóteses da Definição (5.1.3), temos que o reticulado Λ pode ser descrito por

$$\Lambda = \{\lambda M \text{ tal que } \lambda \in \mathbb{Z}^n\}.$$

Observação 5.1.4 *Note que da mesma forma que mais de uma base pode determinar o mesmo reticulado Λ também mais de uma matriz geradora pode determiná-lo. No entanto, o módulo do determinante de qualquer matriz geradora de Λ é sempre o mesmo. De fato, sejam $\{f_1, \dots, f_n\}$ e $\{v_1, \dots, v_n\}$ duas bases do reticulado Λ , tal que $f_i = (f_{i1}, \dots, f_{in})$ e $v_i = (v_{i1}, \dots, v_{in})$, para todo i . Temos que se $f_i = \sum_{j=1}^n a_{ij}v_j$, com $a_{ij} \in \mathbb{Z}$, então*

$$|\det(f_{ij})_{i,j=1}^n| = |\det(a_{ij})_{i,j=1}^n| |\det(v_{ij})_{i,j=1}^n| = |\det(v_{ij})_{i,j=1}^n|,$$

pois $|\det(a_{ij})| = 1$.

Definição 5.1.4 Seja $\Lambda \subset \mathbb{R}^n$ um reticulado, $\beta = \{v_1, \dots, v_n\}$ uma base de Λ e \mathcal{P}_Λ sua região fundamental. Se $v_i = (v_{i1}, \dots, v_{in})$, para $i = 1, \dots, n$, definimos o **volume da região fundamental** \mathcal{P}_Λ como o módulo do determinante da matriz geradora M , isto é,

$$\text{vol}(\mathcal{P}_\Lambda) = \left| \det \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \cdots & v_{nn} \end{pmatrix} \right|.$$

Notemos, pela Observação (5.1.4), que o volume da região fundamental está bem definido, pois independe da base do reticulado considerada.

Observação 5.1.5 Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado e M, N duas matrizes geradoras de Λ . Seja $G_1 = MM^t$ e $G_2 = NN^t$ matrizes de Gram de Λ . Temos que existe uma matriz inversível A tal que $M = AN$. Logo, $G_1 = ANN^tA^t$. Desta forma, $\det(G_1) = \det(ANN^tA^t) = (\det(A))^2 \det(NN^t) = (\det(A))^2 \det(G_2)$. Como A é inversível, temos que $\det(A) = \pm 1$. Assim, $\det(G_1) = \det(G_2)$. Portanto, o determinante da matriz de Gram independe da matriz geradora utilizada.

Definição 5.1.5 Consideremos as mesmas hipóteses da Definição (5.1.3). O **determinante do reticulado** Λ é definido por

$$\det(\Lambda) = \det(G),$$

onde G é uma matriz de Gram do reticulado Λ .

Exemplo 5.1.2 Sejam $\beta = \{(3, -2, 4), (1, 0, 2), (0, 0, -1)\}$ um conjunto linearmente independente e Λ o reticulado gerado por β . Uma matriz geradora de Λ é dada por

$$M = \begin{pmatrix} 3 & -2 & 4 \\ 1 & 0 & 2 \\ 0 & 0 & -1 \end{pmatrix}.$$

Sua matriz de Gram é

$$G = MM^t = \begin{pmatrix} 3 & -2 & 4 \\ 1 & 0 & 2 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 3 & 1 & 0 \\ -2 & 0 & 0 \\ 4 & 2 & -1 \end{pmatrix} = \begin{pmatrix} 29 & 11 & -4 \\ 11 & 5 & -2 \\ -4 & -2 & 1 \end{pmatrix}.$$

Assim, $\det(\Lambda) = \det(G) = 4$.

Observação 5.1.6 Como a matriz de Gram é dada por $G = MM^t$, onde M é a matriz que contém os vetores v_1, \dots, v_n em suas linhas, segue que cada ij -ésima entrada de G é dada pelo produto interno $\langle v_i, v_j \rangle = v_i \cdot v_j^t$.

Definição 5.1.6 Um reticulado Λ é chamado de **reticulado inteiro** se sua matriz de Gram tem todas as entradas em \mathbb{Z} .

No que segue, seja Λ um reticulado n -dimensional definido por uma matriz geradora M .

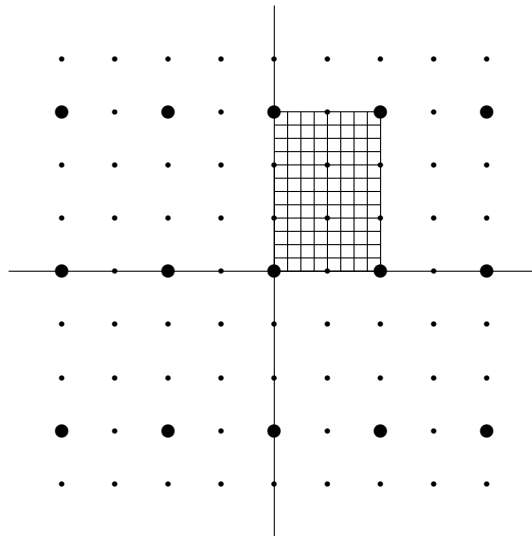
Definição 5.1.7 Seja B uma matriz inteira $n \times n$. Um **sub-reticulado** de Λ é um reticulado dado por

$$\Lambda' = \{\lambda BM, \text{ tal que } \lambda \in \mathbb{Z}^n\}.$$

Exemplo 5.1.3 Seja $\bar{\beta} = \{(2, 0), (0, 3)\}$. O reticulado Λ , gerado por $\bar{\beta}$ é dado por

$$\Lambda = \{a(2, 0) + b(0, 3); a, b \in \mathbb{Z}\} = \{(2a, 3b); a, b \in \mathbb{Z}\}.$$

A figura a seguir mostra o reticulado e sua região fundamental.



Notemos que o reticulado Λ é um subreticulado do reticulado \mathbb{Z}^2 do Exemplo (5.1.1). De fato, $\Lambda = \{\lambda BM; \lambda \in \mathbb{Z}^n\}$, onde $M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ é uma matriz geradora de \mathbb{Z}^2 e $B = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$.

Definição 5.1.8 Dado um reticulado Λ , dizemos que Λ' é uma **versão escalar** de Λ se Λ' é obtido multiplicando todos os vetores de Λ por uma constante $c \in \mathbb{R}$, isto é, $\Lambda' = c\Lambda$. Quando $c \in \mathbb{Z}$, temos que Λ' é um subreticulado de Λ .

Definição 5.1.9 Dados dois vetores $x, y \in \mathbb{R}^n$, definimos a **diversidade**, ou a *distância de Hamming*, de x e y como

$$\text{div}(x, y) = \#\{i, x_i \neq y_i, i = 1, \dots, n\}.$$

Definição 5.1.10 Dado um subconjunto $S \subseteq \mathbb{R}^n$, a **diversidade**, ou a *distância mínima de Hamming*, de S é definida por

$$\text{div}(S) = \min\{\text{div}(x, y) \mid x \neq y, x, y \in S\}.$$

Todo reticulado Λ é um subconjunto do \mathbb{R}^n . Desta forma, podemos estender as Definições (5.1.9) e (5.1.10) para reticulados. Como reticulados têm estrutura de grupo, isto é, a soma de quaisquer dois pontos de Λ está em Λ , podemos reformular a definição de distância de Hamming entre dois vetores.

Definição 5.1.11 Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado e $x = (x_1, \dots, x_n) \in \Lambda$.

- A **diversidade** de x é definida como o número de x_i 's não nulos.
- A **diversidade** de Λ é definida como $\text{div}(\Lambda) = \min\{\text{div}(x); x \in \Lambda, x \neq 0\}$.

Exemplo 5.1.4 Consideremos o reticulado $\Lambda = \{\lambda M; \lambda \in \mathbb{Z}^n\}$, onde

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

Temos que $\Lambda = \{a_1(1, 0, 0, 0) + a_2(0, 1, 0, 0) + a_3(0, 0, 1, 0) + a_4(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}); a_i \in \mathbb{Z}\}$. Agora, $\text{div}(\Lambda) = \min\{\text{div}(x); x \in \Lambda, x \neq 0\} = 1$. Este reticulado é conhecido como D_4 .

Definição 5.1.12 Sejam Λ um reticulado em \mathbb{R}^n com diversidade $l \leq n$ e $x = (x_1, \dots, x_n) \in \Lambda$. Definimos:

- A **distância l -produto** de x por $d_p^l(x) = \prod_{x_i \neq 0} |x_i|$.
- A **distância l -produto mínima** de Λ por $d_{p,min}^l(\Lambda) = \min\{d_p^l(x) \mid x \neq 0, x \in \Lambda\}$.

Definição 5.1.13 *Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado com diversidade n e $x = (x_1, \dots, x_n) \in \Lambda$.*

- A **distância produto** de x é definida como $d_p(x) = \prod_{i=1}^n |x_i|$.
- A **distância produto mínima** de Λ é definida como $d_{p,min}(\Lambda) = \min\{d_p(x) \mid x \in \Lambda, x \neq 0\}$.

Exemplo 5.1.5 *Nas mesmas condições do Exemplo (5.1.4), temos que $(2, 3, 0, 0) \in \Lambda$. Assim, $d_p^1(2, 3, 0, 0) = 2 \cdot 3 = 6$.*

5.2 Empacotamento Reticulado

Nesta seção veremos o conceito de empacotamento esférico e algumas propriedades de empacotamento reticulado.

Definição 5.2.1 • *Um **empacotamento esférico**, ou simplesmente um empacotamento no \mathbb{R}^n , é uma distribuição de esferas de mesmo raio no \mathbb{R}^n de forma que a interseção de quaisquer duas esferas tenha no máximo um ponto. Pode-se descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio.*

- Um **empacotamento reticulado** é um empacotamento em que o conjunto dos centros das esferas formam um reticulado Λ no \mathbb{R}^n .

Exemplo 5.2.1 *Considere $\Lambda = \mathbb{Z}^2$ um reticulado. Se traçarmos esferas de raio $r = \frac{1}{2}$ centralizadas em cada ponto de Λ , teremos um empacotamento reticulado.*

Observação 5.2.1 *Estudar empacotamentos reticulados equivale ao estudo de reticulados. Estamos interessados nos empacotamentos associados a um reticulado Λ em que as esferas tenham raio máximo. Para a determinação deste raio, observe que fixado $k > 0$, a interseção do conjunto compacto $\{x \in \mathbb{R}^n; |x| \leq k\}$ com o reticulado Λ é um conjunto finito, visto que Λ é um conjunto discreto. Assim, segue que o número $\Lambda_{min} = \min\{|\lambda|; \lambda \in \Lambda, \lambda \neq 0\}$ está bem definido.*

Definição 5.2.2 *Sejam Λ um reticulado e $\Lambda_{min} = \min\{|\lambda|; \lambda \in \Lambda, \lambda \neq 0\}$. O número $(\Lambda_{min})^2$ é chamado de **norma mínima do reticulado**.*

Observação 5.2.2 Observamos que $\rho = \frac{\Lambda_{min}}{2}$ é o maior raio para o qual é possível distribuir esferas centradas nos pontos de Λ e obter um empacotamento.

Definição 5.2.3 Seja $\mathcal{B}(\rho)$ a esfera com centro na origem e raio ρ . A **densidade de empacotamento** de Λ é definida por

$$\Delta(\Lambda) = \frac{\text{volume da região coberta por uma esfera}}{\text{volume da região fundamental}} = \frac{\text{Vol}(\mathcal{B}(\rho))}{\text{Vol}(\mathcal{P}_\Lambda)} = \frac{\text{Vol}(\mathcal{B}(1))\rho^n}{\text{Vol}(\mathcal{P}_\Lambda)}.$$

Definição 5.2.4 Definimos a **densidade de centro** do reticulado Λ por

$$\delta(\Lambda) = \frac{\rho^n}{\text{Vol}(\mathcal{P}_\Lambda)}.$$

Exemplo 5.2.2 Sejam $\beta = \{(1, 0, 0), (0, 2, 0), (1, 0, 3)\}$ e Λ o reticulado gerado por β . Temos que

$$\Lambda = \{a(1, 0, 0) + b(0, 2, 0) + c(1, 0, 3); a, b, c \in \mathbb{Z}\} = \{(a + c, 2b, 3c); a, b, c \in \mathbb{Z}\}.$$

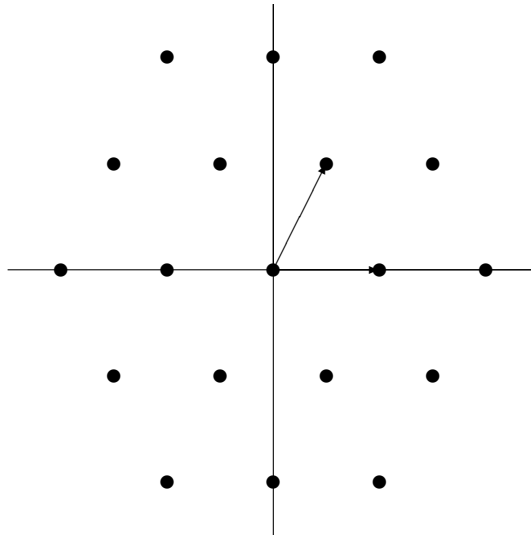
Assim, $\Lambda_{min} = \min\{|\lambda|; \lambda \in \Lambda, \lambda \neq 0\} = 1$, o que implica que $\rho = \frac{\Lambda_{min}}{2} = 1/2$ é o maior raio para o qual é possível obter um empacotamento. Também,

$$\text{Vol}(\mathcal{P}_\Lambda) = \left| \det \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 1 & 0 & 3 \end{pmatrix} \right| = 6,$$

$$\Delta(\Lambda) = \frac{\text{Vol}(\mathcal{B}(1))\rho^3}{\text{Vol}(\mathcal{P}_\Lambda)} = \frac{(\frac{4}{3})\pi(\frac{1}{2^3})}{6} = \frac{\pi}{36} \simeq 0,0873 \quad e$$

$$\delta(\Lambda) = \frac{(\frac{1}{2^3})}{6} = \frac{1}{48} \simeq 0,020833.$$

Exemplo 5.2.3 Sejam $\beta = \{(1, 0), (1/2, \sqrt{3}/2)\}$ e Λ o reticulado gerado por β . Temos que $\Lambda = \{a(1, 0) + b(1/2, \sqrt{3}/2); a, b \in \mathbb{Z}\}$. A figura a seguir mostra o reticulado Λ .



Temos que $\Lambda_{min} = \min\{|\lambda|; \lambda \in \Lambda, \lambda \neq 0\} = 1$. Assim, $\rho = \frac{\Lambda_{min}}{2} = 1/2$ é o maior raio para o qual é possível obter um empacotamento. Também,

$$Vol(\mathcal{P}_\Lambda) = \left| \det \begin{pmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{pmatrix} \right| = \sqrt{3}/2,$$

$$\Delta(\Lambda) = \frac{Vol(\mathcal{B}(1))\rho^2}{Vol(\mathcal{P}_\Lambda)} = \frac{(\frac{1}{4})\pi}{\frac{\sqrt{3}}{2}} = \frac{\pi}{\sqrt{12}} \simeq 0,9069 \text{ e}$$

$$\delta(\Lambda) = \frac{(\frac{1}{2})^2}{\frac{\sqrt{3}}{2}} = \frac{1}{\sqrt{12}} = 0,2886751.$$

O reticulado deste exemplo é conhecido como A_2 ou reticulado hexagonal. Em [13] vemos que este é o reticulado com maior densidade de centro no \mathbb{R}^2 .

Capítulo 6

Reticulados Algébricos

Seja \mathbb{K} um corpo de números de grau n . Neste capítulo apresentamos um método para a geração de reticulados no \mathbb{R}^n . O método consiste na aplicação de determinados homomorfismos a certos \mathbb{Z} -módulos livres de posto n contidos em \mathbb{K} . Os reticulados gerados por este método são conhecidos como reticulados algébricos.

A vantagem de obter reticulados por este método é que podemos identificar os pontos do reticulado no \mathbb{R}^n com os elementos de \mathbb{K} . Desta forma, podemos utilizar algumas propriedades do corpo \mathbb{K} no estudo de tais reticulados.

Sendo \mathbb{K} um corpo de números de grau n temos, pelo Teorema (1.3.3), que existem exatamente n homomorfismos distintos $\sigma_j : \mathbb{K} \rightarrow \mathbb{C}$, $j = 1, \dots, n$. Se $\bar{\sigma} : \mathbb{C} \rightarrow \mathbb{C}$ é a conjugação complexa, então para todo $j = 1, \dots, n$, temos que $\bar{\sigma} \circ \sigma_j = \sigma_k$, para algum $1 \leq k \leq n$, e que $\bar{\sigma} \circ \sigma_j = \sigma_j$ se, e somente se, $\sigma_j(\mathbb{K}) \subset \mathbb{R}$. Desta forma, temos que os homomorfismos imaginários aparecem aos pares, isto é, se σ_j é imaginário, existe k tal que $\bar{\sigma} \circ \sigma_j = \sigma_k$.

Assim, usando r_1 para denotar o número de homomorfismos reais e r_2 o número de pares de homomorfismos imaginários, podemos reordenar os homomorfismos $\sigma_1, \dots, \sigma_n$ de modo que $\sigma_1, \dots, \sigma_{r_1}$ sejam os homomorfismos reais e que $\sigma_{r_1+1}, \dots, \sigma_{r_1+2r_2}$ sejam os homomorfismos imaginários com $\sigma_{r_1+r_2+i} = \bar{\sigma} \circ \sigma_{r_1+i}$, para $i = 1, \dots, r_2$. Notemos que $n = r_1 + 2r_2$.

Na Seção 6.1, apresentamos o homomorfismo de Minkowski, na Seção 6.2, o homomorfismo Torcido e na Seção 6.3 a Perturbação de Imersão Canônica.

6.1 Homomorfismo de Minkowski

Uma das aplicações do homomorfismo que iremos definir nesta seção é a geração de reticulados no \mathbb{R}^n .

Definição 6.1.1 *Seja \mathbb{K} um corpo de números de grau n . Consideremos o homomorfismo injetivo de anéis*

$$\sigma_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{R}^n$$

$$x \longmapsto (\sigma_1(x), \dots, \sigma_{r_1}(x), \Re(\sigma_{r_1+1}(x)), \Im(\sigma_{r_1+1}(x)), \dots, \Re(\sigma_{r_1+r_2}(x)), \Im(\sigma_{r_1+r_2}(x))),$$

onde \Re representa a parte real e \Im representa a parte imaginária, respectivamente, do número complexo. Tal homomorfismo é chamado de **homomorfismo canônico** ou **homomorfismo de Minkowski** de \mathbb{K} em \mathbb{R}^n .

Exemplo 6.1.1 *Sejam $\zeta = \zeta_5$ uma raiz 5-ésima primitiva da unidade e $\mathbb{K} = \mathbb{Q}(\zeta_5)$ o 5-ésimo corpo ciclotômico. Temos que os \mathbb{Q} -homomorfismos de \mathbb{K} em \mathbb{C} são dados por $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$, onde $\sigma_i(\zeta) = \zeta^i$, para $i = 1, \dots, 4$. Agora, $\sigma_i(\mathbb{K}) \not\subseteq \mathbb{R}$, para todo $i = 1, 2, 3, 4$. De fato, basta notar que $\sigma_i(\zeta) \notin \mathbb{R}$, para todo $i = 1, 2, 3, 4$. Neste caso, temos que \mathbb{K} é totalmente imaginário, assim $r_1 = 0$ e $r_2 = 2$. Notemos que $\bar{\sigma} \circ \sigma_1 = \sigma_4$ e $\bar{\sigma} \circ \sigma_2 = \sigma_3$. Reorganizando os homomorfismos de maneira conveniente, temos que O homomorfismo de Minkowski é dado por*

$$\sigma_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{R}^4$$

$$x \longmapsto (\Re(\sigma_1(x)), \Im(\sigma_1(x)), \Re(\sigma_2(x)), \Im(\sigma_2(x))).$$

Exemplo 6.1.2 *Seja $\mathbb{L} = \mathbb{Q}(\zeta_7)$ o 7-ésimo corpo ciclotômico e $\mathbb{K} = \mathbb{Q}(\zeta + \zeta^{-1})$ seu subcorpo real maximal. Temos que os \mathbb{Q} -homomorfismos de \mathbb{K} em \mathbb{C} são dados por $\{\sigma_1, \sigma_2, \sigma_3\}$, onde $\sigma_j(\zeta_7 + \zeta_7^{-1}) = \zeta_7^j + \zeta_7^{-j}$, para $j = 1, 2, 3$. Neste caso, temos que \mathbb{K} é totalmente real, pois $\sigma_j(\mathbb{K}) \subset \mathbb{R}$, para todo $j = 1, 2, 3$. O homomorfismo de Minkowski é dado por*

$$\sigma_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{R}^3$$

$$x \longmapsto (\sigma_1(x), \sigma_2(x), \sigma_3(x)).$$

A próxima proposição mostra como o homomorfismo de Minkowski gera reticulados no \mathbb{R}^n .

Proposição 6.1.1 ([3], pag. 56) *Sejam \mathbb{K} um corpo de números de grau n e $\sigma_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{R}^n$ o homomorfismo de Minkowski. Se $M \subseteq \mathbb{K}$ é um \mathbb{Z} -módulo livre de posto n e se $\{x_j\}_{1 \leq j \leq n}$ é uma \mathbb{Z} -base de M , então $\sigma_{\mathbb{K}}(M)$ é um reticulado no \mathbb{R}^n com base $\{\sigma_{\mathbb{K}}(x_1), \dots, \sigma_{\mathbb{K}}(x_n)\}$ e volume*

$$\text{Vol}(\sigma_{\mathbb{K}}(M)) = 2^{-r_2} \left| \det(\sigma_j(x_k))_{j,k=1}^n \right|,$$

onde r_2 é o número de pares de homomorfismos imaginários. ■

Se $\{x_1, \dots, x_n\}$ é uma \mathbb{Z} -base de $M \subset \mathbb{K}$, então a matriz geradora do reticulado $\sigma_{\mathbb{K}}(M) = \left\{ \sum_{i=1}^n a_i \sigma_{\mathbb{K}}(x_i); a_i \in \mathbb{Z} \right\}$ é dada por

$$\begin{pmatrix} \sigma_1(x_1) & \dots & \sigma_{r_1}(x_1) & \Re(\sigma_{r_1+1}(x_1)) & \Im(\sigma_{r_1+1}(x_1)) & \dots & \Re(\sigma_{r_1+r_2}(x_1)) & \Im(\sigma_{r_1+r_2}(x_1)) \\ \sigma_1(x_2) & \dots & \sigma_{r_1}(x_2) & \Re(\sigma_{r_1+1}(x_2)) & \Im(\sigma_{r_1+1}(x_2)) & \dots & \Re(\sigma_{r_1+r_2}(x_2)) & \Im(\sigma_{r_1+r_2}(x_2)) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(x_n) & \dots & \sigma_{r_1}(x_n) & \Re(\sigma_{r_1+1}(x_n)) & \Im(\sigma_{r_1+1}(x_n)) & \dots & \Re(\sigma_{r_1+r_2}(x_n)) & \Im(\sigma_{r_1+r_2}(x_n)) \end{pmatrix}.$$

Exemplo 6.1.3 Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{15})$ e $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{15}]$ o seu anel de inteiros, pois $15 \equiv 3, \pmod{4}$. Seja $I = 3\mathcal{O}_{\mathbb{K}}$ um ideal de $\mathcal{O}_{\mathbb{K}}$. Temos que I é um \mathbb{Z} -módulo livre com base $\{3, 3\sqrt{15}\}$. Pela Proposição (6.1.1), temos que $\sigma_{\mathbb{K}}(I)$ é um reticulado no \mathbb{R}^2 com base $\{\sigma_{\mathbb{K}}(3), \sigma_{\mathbb{K}}(3\sqrt{15})\}$. Como os \mathbb{Q} -homomorfismos de \mathbb{K} em \mathbb{C} são dados por $\{\sigma_1, \sigma_2\}$, onde $\sigma_1(\sqrt{15}) = \sqrt{15}$ e $\sigma_2(\sqrt{15}) = -\sqrt{15}$, segue que \mathbb{K} é totalmente real, o que implica que $r_2 = 0$. Assim, $\sigma_{\mathbb{K}}(3) = (\sigma_1(3), \sigma_2(3)) = (3, 3)$ e $\sigma_{\mathbb{K}}(3\sqrt{15}) = (\sigma_1(3\sqrt{15}), \sigma_2(3\sqrt{15})) = (3\sqrt{15}, -3\sqrt{15})$. Desta forma, a matriz geradora do reticulado $\sigma_{\mathbb{K}}(I)$ é dada por

$$G = \begin{pmatrix} 3 & 3 \\ 3\sqrt{15} & -3\sqrt{15} \end{pmatrix}.$$

Ainda, pela Proposição (6.1.1), temos que

$$\text{Vol}(\sigma_{\mathbb{K}}(I)) = \left| \det \begin{pmatrix} \sigma_1(3) & \sigma_1(3\sqrt{15}) \\ \sigma_2(3) & \sigma_2(3\sqrt{15}) \end{pmatrix} \right| = \left| \det \begin{pmatrix} 3 & 3\sqrt{15} \\ 3 & -3\sqrt{15} \end{pmatrix} \right| = 18\sqrt{15}.$$

Proposição 6.1.2 Se \mathbb{K} é um corpo de números de grau n , $\text{Disc}(\mathbb{K}|\mathbb{Q})$ o discriminante de \mathbb{K} sobre \mathbb{Q} , $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de \mathbb{K} e I um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ e $\sigma_{\mathbb{K}}(I)$ são reticulados, com respectivos volumes,

$$\text{Vol}(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 2^{-r_2} |\text{Disc}(\mathbb{K}|\mathbb{Q})|^{\frac{1}{2}} e$$

$$\text{Vol}(\sigma_{\mathbb{K}}(I)) = 2^{-r_2} |\text{Disc}(\mathbb{K}|\mathbb{Q})|^{\frac{1}{2}} N(I),$$

onde r_2 é o número de pares de homomorfismos imaginários.

Demonstração: Pelo Corolário (1.5.7), temos que I e $\mathcal{O}_{\mathbb{K}}$ são \mathbb{Z} -módulos livres de posto n . Assim, pela Proposição (6.1.1), temos que $\sigma_{\mathbb{K}}(I)$ e $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ são reticulados no \mathbb{R}^n . Além disso, temos que:

- $Vol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 2^{-r_2} |\det(\sigma_i(x_k))|$, onde $\{x_1, \dots, x_n\}$ é uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}}$. Pela Proposição (1.6.2), temos que $Disc(\mathbb{K}|\mathbb{Q}) = \det(\sigma_i(x_k))^2$ e, assim, $|Disc(\mathbb{K}|\mathbb{Q})|^{\frac{1}{2}} = |\det(\sigma_i(x_k))|$ e, portanto,

$$Vol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 2^{-r_2} |Disc(\mathbb{K}|\mathbb{Q})|^{\frac{1}{2}}.$$

- Seja $\{w_1, \dots, w_n\}$ uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}}$. Pelo Teorema (1.2.1), temos que existem inteiros não nulos e_1, \dots, e_n tal que $\{e_1 w_1, \dots, e_n w_n\}$ é uma \mathbb{Z} -base de I , pois I é um \mathbb{Z} -módulo livre de posto n . Assim,

$$Vol(\sigma_{\mathbb{K}}(I)) = 2^{-r_2} |\det(\sigma_i(e_j w_j))| = 2^{-r_2} |e_1 \cdots e_n| |\det(\sigma_i(w_j))|.$$

Pela Proposição (1.9.5), temos que $|e_1 \cdots e_n| = N(I)$. Como $|\det(\sigma_i(w_j))| = |Disc(\mathbb{K}|\mathbb{Q})|^{\frac{1}{2}}$, segue que

$$Vol(\sigma_{\mathbb{K}}(I)) = 2^{-r_2} |Disc(\mathbb{K}|\mathbb{Q})|^{\frac{1}{2}} N(I),$$

o que prova a proposição. ■

Exemplo 6.1.4 *Sejam $\mathbb{K} = \mathbb{Q}(\zeta_8)$, onde $\zeta_8 = e^{\frac{2\pi i}{8}}$ e $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_8]$ seu anel de inteiros com \mathbb{Z} -base $\{1, \zeta_8, \zeta_8^2, \zeta_8^3\}$. Seja $I = 5\mathbb{Z}[\zeta_8]$ um ideal de $\mathbb{Z}[\zeta_8]$. Temos, pela Proposição (6.1.2), que $\sigma_{\mathbb{K}}(I)$ é um reticulado. Além disso, temos que*

$$Vol(\sigma_{\mathbb{K}}(I)) = 2^{-r_2} |Disc(\mathbb{K}|\mathbb{Q})|^{\frac{1}{2}} N(I).$$

Agora, como \mathbb{K} é totalmente complexo, segue que $r_2 = 2$. Pelo Teorema (3.2.3), temos que $|Disc(\mathbb{Q}(\zeta_8)|\mathbb{Q})| = 2^8$ e como I é um ideal principal, pela Proposição (1.9.1), temos que $N(I) = |N_{\mathbb{K}|\mathbb{Q}}(5)| = 5^4$. Assim, $Vol(\sigma_{\mathbb{K}}(I)) = 2^{-2} 2^{8/2} 5^4 = 2^{4-2} 5^4 = 2^2 5^4 = 2500$.

Dado um corpo de números \mathbb{K} de grau n , vamos estudar agora qual a relação entre as matrizes geradoras dos reticulados $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ e $\sigma_{\mathbb{K}}(I)$, onde $\mathcal{O}_{\mathbb{K}}$ é o anel de inteiros de \mathbb{K} sobre \mathbb{Z} e I é um ideal de $\mathcal{O}_{\mathbb{K}}$.

Pelo Corolário (1.5.7), temos que $\mathcal{O}_{\mathbb{K}}$ e I são \mathbb{Z} -módulos livres de posto n . Sejam $\{w_1, \dots, w_n\}$ uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}}$ e $\{\gamma_1, \dots, \gamma_n\}$ uma \mathbb{Z} -base de I . Como $I \subset \mathcal{O}_{\mathbb{K}}$, temos que para todo i , γ_i pode ser expresso como uma combinação linear de w_1, \dots, w_n . Suponha então que $\gamma_i =$

$\sum_{j=1}^n t_{ij}w_j$, onde $t_{ij} \in \mathbb{Z}$, para todo i, j . Seja T a matriz dada por $T = (t_{ij})_{i,j=1}^n$. Temos que $(\gamma_i)_{i=1}^n = T(w_i)_{i=1}^n$.

Proposição 6.1.3 *Nas condições anteriores, a matriz geradora G_I do reticulado $\sigma_{\mathbb{K}}(I)$ pode ser obtida através da matriz geradora G do reticulado $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ por $G_I = TG$.*

Demonstração: Seja $\gamma_i = \sum_{j=1}^n t_{ij}w_j$. Para todo $k = 1, \dots, r_1$, temos que $\sigma_{\mathbb{K}}(\gamma_i) = \sum_{j=1}^n t_{ij}\sigma_{\mathbb{K}}(w_j)$.

Além disso, para todo $k = r_1 + 1, \dots, r_1 + r_2$, $\Re(\sigma_{\mathbb{K}}(\gamma_i)) = \sum_{j=1}^n t_{ij}\Re(\sigma_{\mathbb{K}}(w_j))$ e $\Im(\sigma_{\mathbb{K}}(\gamma_i)) = \sum_{j=1}^n t_{ij}\Im(\sigma_{\mathbb{K}}(w_j))$. Logo, segue que $G_I = TG$. ■

6.2 Homomorfismo Torcido

Nesta seção apresentamos um outro homomorfismo que também serve para gerar reticulados no \mathbb{R}^n . Este homomorfismo é obtido por uma perturbação do homomorfismo canônico.

Definição 6.2.1 *Sejam \mathbb{K} um corpo de números de grau n e $\alpha \in \mathbb{K}$ tal que $\alpha_i = \sigma_i(\alpha) \in \mathbb{R}$ e $\alpha_i > 0$, para todo $i = 1, \dots, n$. Considere o homomorfismo injetivo $\sigma_{\alpha} : \mathbb{K} \rightarrow \mathbb{R}^n$ tal que*

$$\sigma_{\alpha}(x) = (\sqrt{\alpha_1}\sigma_1(x), \dots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x)), \\ \sqrt{2\alpha_{r_1+1}}\Im(\sigma_{r_1+1}(x)), \dots, \sqrt{2\alpha_{r_1+r_2}}\Re(\sigma_{r_1+r_2}(x)), \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x))),$$

onde \Re e \Im representam a parte real e imaginária, respectivamente, de um número complexo. Tal homomorfismo é definido como **homomorfismo torcido**.

Exemplo 6.2.1 *Sejam $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2})$ um corpo de números de grau 3, $\alpha = 3 \in \mathbb{K}$ e $\{\sigma_1, \sigma_2, \sigma_3\}$ os \mathbb{Q} -homomorfismos de \mathbb{K} em \mathbb{C} , dados por $\sigma_i(\sqrt[3]{2}) = \sqrt[3]{2}w^{i-1}$, $i = 1, 2, 3$, onde $w = e^{\frac{2\pi i}{3}}$. Temos que $\sigma_{\alpha} : \mathbb{K} \rightarrow \mathbb{R}^n$, definido por $\sigma_{\alpha}(x) = (\sqrt{\sigma_1(\alpha)}\sigma_1(x), \sqrt{2\sigma_2(\alpha)}\Re(\sigma_2(x)), \sqrt{2\sigma_2(\alpha)}\Im(\sigma_2(x)))$ é um homomorfismo torcido.*

Proposição 6.2.1 *Se $L \subseteq \mathbb{K}$ é um \mathbb{Z} -módulo livre de posto n com \mathbb{Z} -base $\{w_1, \dots, w_n\}$, então a imagem $\sigma_{\alpha}(L)$ em \mathbb{R}^n é um reticulado com base $\{\sigma_{\alpha}(w_1), \dots, \sigma_{\alpha}(w_n)\}$.*

Demonstração: Análoga a Proposição (6.1.1). ■

Se $\{w_1, \dots, w_n\}$ é uma \mathbb{Z} -base de L , então o reticulado $\sigma_\alpha(L)$ tem matriz geradora M dada por

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(w_1) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(w_1) & \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(w_1)) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(w_1)) \\ \sqrt{\alpha_1}\sigma_1(w_2) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(w_2) & \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(w_2)) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(w_2)) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \sqrt{\alpha_1}\sigma_1(w_n) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(w_n) & \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(w_n)) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(w_n)) \end{pmatrix}.$$

Assim, podemos descrever $\sigma_\alpha(L)$ como

$$\sigma_\alpha(L) = \{\lambda M, \lambda \in \mathbb{Z}^n\}.$$

Capítulo 7

Reticulados Ideais

Neste capítulo apresentamos o conceito de reticulados ideais e suas principais propriedades. Através deste conceito podemos estudar algumas propriedades de certos reticulados no \mathbb{R}^n . Veremos relações para calcular o determinante de um reticulado ideal e que envolvem sua paridade.

7.1 Definição e Propriedades

Sejam \mathbb{K} um corpo de números de grau n tal que \mathbb{K} é totalmente real ou um CM-corpo, $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de \mathbb{K} sobre \mathbb{Z} , $\alpha \in \mathbb{K}$ tal que $\alpha_i = \sigma_i(\alpha) > 0$, para todo $i = 1, \dots, n$ e $\sigma_{\alpha} : \mathbb{K} \rightarrow \mathbb{R}^n$ o homomorfismo torcido.

Se tomarmos $L \subset \mathbb{K}$ um \mathbb{Z} -módulo livre com \mathbb{Z} -base $\{w_1, \dots, w_n\}$ vimos que $\sigma_{\alpha}(L)$ é um reticulado no \mathbb{R}^n com matriz geradora

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(w_1) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(w_1) & \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(w_1)) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(w_1)) \\ \sqrt{\alpha_1}\sigma_1(w_2) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(w_2) & \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(w_2)) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(w_2)) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \sqrt{\alpha_1}\sigma_1(w_n) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(w_n) & \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(w_n)) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(w_n)) \end{pmatrix}.$$

Nestas condições, como \mathbb{K} é totalmente real ou um CM-corpo, temos que a conjugação complexa comuta com σ_i , para todo $i = 1, \dots, n$. Desta forma, a matriz de Gram $G = MM^t$ é dada por $G = (g_{ij})_{i,j=1}^n$, onde

$$g_{ij} = \sum_{k=1}^{r_1} \sqrt{\alpha_k}\sigma_k(w_i)\sqrt{\alpha_k}\sigma_k(w_j) + \sum_{k=1}^{r_2} \sqrt{2\alpha_{r_1+k}}\Re(\sigma_{r_1+k}(w_i))\sqrt{2\alpha_{r_1+k}}\Re(\sigma_{r_1+k}(w_j))$$

$$\begin{aligned}
& + \sum_{k=1}^{r_2} \sqrt{2\alpha_{r_1+k}} \Im(\sigma_{r_1+k}(w_i)) \sqrt{2\alpha_{r_1+k}} \Im(\sigma_{r_1+k}(w_j)) \\
& = \sum_{k=1}^{r_1} \alpha_k \sigma_k(w_i) \sigma_k(w_j) + \sum_{k=1}^{r_2} 2\alpha_{r_1+k} \Re(\sigma_{r_1+k}(w_i) \sigma_{r_1+k}(w_j)) \\
& = \sum_{k=1}^{r_1} \alpha_k \sigma_k(w_i w_j) + \sum_{k=1}^{r_2} \alpha_{r_1+k} 2\Re(\sigma_{r_1+k}(w_i \bar{w}_j)) \\
& = \sum_{k=1}^{r_1} \alpha_k \sigma_k(w_i w_j) + \sum_{k=1}^{r_2} \alpha_{r_1+k} \sigma_{r_1+k}(w_i \bar{w}_j) + \sum_{k=1}^{r_2} \alpha_{r_1+k} \overline{\sigma_{r_1+k}(w_i \bar{w}_j)} \\
& = \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha w_i \bar{w}_j).
\end{aligned}$$

Motivados pelo estudo de reticulados cuja matriz de Gram apresenta todas as suas entradas da forma $g_{ij} = \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha w_i \bar{w}_j)$, passaremos ao estudo de reticulados ideais.

Definição 7.1.1 *Seja \mathbb{K} um corpo de números.*

- Uma **involução** $\phi : \mathbb{K} \longrightarrow \mathbb{K}$ é uma aplicação aditiva e multiplicativa tal que ϕ^2 é a aplicação identidade.
- O conjunto $\mathbb{F} = \{x \in \mathbb{K} \mid \phi(x) = x\}$ é um corpo chamado **corpo fixo da involução**.

Lema 7.1.1 *Se $\phi : \mathbb{K} \longrightarrow \mathbb{K}$ é uma involução, então $\phi \in \text{Gal}(\mathbb{K}|\mathbb{Q})$, onde $\text{Gal}(\mathbb{K}|\mathbb{Q})$ denota o grupo de Galois de \mathbb{K} sobre \mathbb{Q} .*

Demonstração: Por definição, temos que ϕ é um homomorfismo e que ϕ fixa \mathbb{Q} . Mostremos que ϕ é injetora. De fato, sejam $a, b \in \mathbb{K}$ tal que $\phi(a) = \phi(b)$. Aplicando ϕ na igualdade, obtemos que $\phi(\phi(a)) = \phi(\phi(b))$ e, desta forma, como $\phi^2 = id$, segue que $a = b$. Falta mostrar que ϕ é sobrejetora. Para isto, seja $y \in \mathbb{K}$. Temos que $\phi^2(y) = y$. Assim, tomando $x = \phi(y)$, temos que $\phi(x) = \phi(\phi(y)) = \phi^2(y) = y$. Desta forma, temos que ϕ é um isomorfismo que fixa \mathbb{Q} . Logo, $\phi \in \text{Gal}(\mathbb{K}|\mathbb{Q})$. ■

Proposição 7.1.1 *Com as notações da Definição (7.1.1), temos que $[\mathbb{K} : \mathbb{F}] \leq 2$.*

Demonstração: Como $\mathbb{K}|\mathbb{Q}$ é uma extensão finita e separável, segue que se H é um subgrupo de G , onde $G = \text{Gal}(\mathbb{K}|\mathbb{Q})$, então o corpo L^H , fixo por H , satisfaz $[\mathbb{K} : L^H] \leq |H|$. Agora, se tomarmos $H = \{id, \phi\}$, temos que H é um subgrupo de G , pois $\phi^2 = id$. Como $L^H = \mathbb{F}$ é o corpo fixo por H , segue que $[\mathbb{K} : \mathbb{F}] \leq |H|$. Agora, $|H| \leq 2$, pois $|H| = O(\phi) \leq 2$. Logo, $[\mathbb{K} : \mathbb{F}] \leq 2$. ■

Exemplo 7.1.1 Seja $\mathbb{K} = \mathbb{Q}(i)$ um corpo de números de grau 2. Seja $\phi : \mathbb{K} \longrightarrow \mathbb{K}$ a conjugação complexa. Temos que ϕ é uma involução, $\mathbb{F} = \{x \in \mathbb{K}; \phi(x) = x\} = \mathbb{Q}$ e $[\mathbb{K} : \mathbb{F}] = 2$.

A partir de agora, a involução será dada pela conjugação complexa.

Sejam \mathbb{K} um corpo de números totalmente real ou um CM-corpo, $\phi : \mathbb{K} \longrightarrow \mathbb{K}$ a conjugação complexa, \mathbb{F} o corpo fixo por ϕ , I um ideal fracionário não nulo de $\mathcal{O}_{\mathbb{K}}$ e $\alpha \in \mathbb{F}$ tal que $\alpha I \phi(I) \subset \Delta(\mathbb{K}|\mathbb{Q})^{-1}$.

Proposição 7.1.2 Nas condições anteriores, seja

$$b_{\alpha} : I \times I \longrightarrow \mathbb{Z}$$

$$(x, y) \longmapsto Tr_{\mathbb{K}|\mathbb{Q}}(\alpha x \phi(y)).$$

Tem-se que b_{α} está bem definida e é uma forma bilinear simétrica.

Demonstração: De fato, como $\alpha I \phi(I) \subset \Delta(\mathbb{K}|\mathbb{Q})^{-1}$, segue que $Tr_{\mathbb{K}|\mathbb{Q}}(\alpha x \phi(y)) \in \mathbb{Z}$, para todo $(x, y) \in I \times I$. Além disso, como \mathbb{K} é totalmente real ou um CM-corpo, temos que a conjugação complexa comuta com todos os homomorfismos de \mathbb{K} em \mathbb{C} . Desta forma, $b_{\alpha}(x, y) = Tr_{\mathbb{K}|\mathbb{Q}}(\alpha x \phi(y)) = Tr_{\mathbb{K}|\mathbb{Q}}(\phi(\phi(\alpha)\phi(x)y)) = \phi(Tr_{\mathbb{K}|\mathbb{Q}}(\phi(\alpha)\phi(x)y)) = Tr_{\mathbb{K}|\mathbb{Q}}(\alpha\phi(x)y) = b_{\alpha}(y, x)$. ■

Definição 7.1.2 Com as mesmas hipóteses da Proposição (7.1.2), dizemos que o par (I, b_{α}) é um **reticulado ideal** ou um **$\mathcal{O}_{\mathbb{K}}$ -reticulado**.

Definição 7.1.3 Quando $\alpha = 1$ dizemos que o reticulado ideal (I, b) é obtido por uma construção traço ou que é do **tipo traço**.

Definição 7.1.4 Sejam I um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$ e $\{v_1, v_2, \dots, v_n\}$ uma \mathbb{Z} -base de I . A matriz que representa a forma bilinear b_{α} é dada por $(b_{\alpha}(v_i, v_j))_{i,j=1}^n$. O **determinante de b_{α}** é o determinante da matriz de b_{α} em alguma base de I .

Exemplo 7.1.2 Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ um corpo quadrático e $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{2}]$ o anel de inteiros de \mathbb{K} sobre \mathbb{Z} . Temos que $\mathcal{O}_{\mathbb{K}}$ é um \mathbb{Z} -módulo livre de posto 2 com base $\{1, \sqrt{2}\}$. Seja $b : \mathbb{Z}[\sqrt{2}] \times \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{Z}$ a forma bilinear simétrica definida por $b(x, y) = Tr_{\mathbb{K}|\mathbb{Q}}(xy)$. A matriz que representa b é dada por

$$B = \begin{pmatrix} b(1, 1) & b(1, \sqrt{2}) \\ b(\sqrt{2}, 1) & b(\sqrt{2}, \sqrt{2}) \end{pmatrix} = \begin{pmatrix} Tr_{\mathbb{K}|\mathbb{Q}}(1) & Tr_{\mathbb{K}|\mathbb{Q}}(\sqrt{2}) \\ Tr_{\mathbb{K}|\mathbb{Q}}(\sqrt{2}) & Tr_{\mathbb{K}|\mathbb{Q}}(2) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}.$$

O determinante de b é $\det(b) = 8$.

Definição 7.1.5 Dizemos que o reticulado ideal (I, b_α) é **par** se $b_\alpha(x, x)$ é um número par para todo $x \in I$. Caso contrário, dizemos que é **ímpar**.

Exemplo 7.1.3 Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ um corpo de números de grau 2, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{2}]$ e

$$b : \mathbb{Z}[\sqrt{2}] \times \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{Z}$$

$$(x, y) \longmapsto \text{Tr}_{\mathbb{K}|\mathbb{Q}}(xy)$$

Temos que o reticulado ideal $(\mathcal{O}_{\mathbb{K}}, b)$ é par, pois para todo $x = a + b\sqrt{2} \in \mathcal{O}_{\mathbb{K}}$, temos que $b(x, x) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}(xx) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}((a + b\sqrt{2})^2) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}(a^2 + 2b^2 + 2ab\sqrt{2}) = 2(a^2 + 2b^2) \in 2\mathbb{Z}$.

Definição 7.1.6 O reticulado ideal (I, b_α) é **positivo** se $b_\alpha(x, x) > 0$ para todo $x \in I$ tal que $x \neq 0$. Neste caso, o **mínimo de** (I, b_α) é definido por $\min(I, b_\alpha) = \min\{b_\alpha(x, x); x \in I, x \neq 0\}$. O valor $b_\alpha(x, x)$ é chamado de **comprimento quadrático** de x .

Exemplo 7.1.4 Nas condições do Exemplo (7.1.3), temos que o reticulado ideal $(\mathcal{O}_{\mathbb{K}}, b)$ é positivo. Além disso, $\min(\mathcal{O}_{\mathbb{K}}, b) = 2$.

Proposição 7.1.3 Sejam \mathbb{K} um corpo de números tal que \mathbb{K} é totalmente real ou um CM-corpo, $\mathcal{O}_{\mathbb{K}}$ seu anel de inteiros e $\phi : \mathbb{K} \longrightarrow \mathbb{K}$ a conjugação complexa. Se existe $\gamma \in \mathcal{O}_{\mathbb{K}}$ tal que $\gamma + \phi(\gamma) = 1$, então todo $\mathcal{O}_{\mathbb{K}}$ -reticulado é par.

Demonstração: Seja I um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$ e $b_\alpha : I \times I \longrightarrow \mathbb{Z}$ tal que $b_\alpha(x, y) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha x \phi(y))$, onde $\alpha \in \mathbb{F}$ é tal que $\alpha I \phi(I) \subset \Delta(\mathbb{K}|\mathbb{Q})^{-1}$. Mostremos que o $\mathcal{O}_{\mathbb{K}}$ -reticulado (I, b_α) é par. Seja $x \in I$. Temos que $b_\alpha(x, x) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha x \phi(x)) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}((\gamma + \phi(\gamma))(\alpha x \phi(x))) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\gamma \alpha x \phi(x) + \phi(\gamma) \alpha x \phi(x)) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\gamma \alpha x \phi(x)) + \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\phi(\gamma \alpha x \phi(x))) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\gamma \alpha x \phi(x)) + \phi(\text{Tr}_{\mathbb{K}|\mathbb{Q}}(\gamma \alpha x \phi(x))) = 2\Re(\text{Tr}_{\mathbb{K}|\mathbb{Q}}(\gamma \alpha x \phi(x))) \in 2\mathbb{Z}$. Portanto, $b_\alpha(x, x)$ é um número par. ■

Exemplo 7.1.5 Sejam p um número primo ímpar e $\mathbb{Q}(\zeta_p)$ o corpo ciclotômico associado a raiz p -ésima primitiva da unidade. Seja $\phi = \bar{\cdot}$ a conjugação complexa. Temos que todo $\mathcal{O}_{\mathbb{K}}$ -reticulado é par. De fato, mostremos que existe $\gamma \in \mathcal{O}_{\mathbb{K}}$ tal que $\gamma + \bar{\gamma} = 1$. Seja $\gamma = a_1\zeta + a_2\zeta^2 + \dots + a_{p-1}\zeta^{p-1} \in \mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$. Temos que $\gamma + \bar{\gamma} = a_1\zeta + a_2\zeta^2 + \dots + a_{p-1}\zeta^{p-1} + a_1\zeta^{p-1} + a_2\zeta^{p-2} + \dots + a_{p-1}\zeta$. Agora, como $\phi_p(x) = x^{p-1} + \dots + x + 1 = \min_{\mathbb{Q}}\zeta_p$, temos que $\phi_p(\zeta) = 0$ e $\zeta^{p-1} = -\zeta^{p-2} - \dots - \zeta - 1$. Desta forma,

$$\gamma + \bar{\gamma} = (a_1 + a_{p-1})\zeta + (a_2 + a_{p-2})\zeta^2 + \dots + (a_{p-2} + a_2)\zeta^{p-2} + (a_{p-1} + a_1)\zeta^{p-1}$$

$$= (-a_1 - a_{p-1}) + (-a_1 - a_{p-1} + a_1 + a_{p-1})\zeta + (-a_1 - a_{p-1} + a_2 + a_{p-2})\zeta^2 + \cdots + (-a_1 - a_{p-1} + a_2 + a_{p-2})\zeta^{p-2}.$$

Para que $\gamma + \bar{\gamma} = 1$, devemos ter:

$$\begin{cases} -a_1 - a_{p-1} = 1 \\ -a_1 - a_{p-1} + a_2 + a_{p-2} = 0 \\ \vdots \\ -a_1 - a_{p-1} + a_{\frac{p-1}{2}} + a_{\frac{p+1}{2}} = 0. \end{cases}$$

Uma solução inteira deste sistema é $a_1 = 1, a_2 = a_3 = \cdots = a_{\frac{p-1}{2}} = -1, a_{\frac{p+1}{2}} = \cdots = a_{p-2} = 0$ e $a_{p-1} = -2$. Assim, se tomarmos $\gamma = \zeta - \zeta^2 - \zeta^3 - \cdots - \zeta^{\frac{p-1}{2}} - 2\zeta^{p-1}$, temos que $\gamma + \bar{\gamma} = 1$. Portanto, existe $\gamma \in \mathbb{Z}[\zeta_p]$ tal que $\gamma + \bar{\gamma} = 1$. Assim, pela Proposição (7.1.3), temos que todo $\mathcal{O}_{\mathbb{K}}$ -reticulado é par.

Exemplo 7.1.6 Seja $\phi = \bar{\cdot}$ a conjugação complexa. Este exemplo mostra que pode não existir $\gamma \in \mathcal{O}_{\mathbb{K}}$ tal que $\gamma + \bar{\gamma} = 1$ e o $\mathcal{O}_{\mathbb{K}}$ -reticulado ser par. Sejam $\mathbb{K} = \mathbb{Q}(\zeta_8)$, $P = \langle 2, \zeta_8 - 1 \rangle$ um ideal primo de $\mathcal{O}_{\mathbb{K}}$ com $N(P) = 2$, $\zeta = \zeta_8$ e $\alpha = \frac{1}{4}$. Seja $b_\alpha : P \times P \rightarrow \mathbb{Z}$, tal que $b_\alpha(x, y) = \frac{1}{4} \text{Tr}_{\mathbb{K}|\mathbb{Q}}(x\phi(y))$. Mostremos que o reticulado ideal (P, b_α) é par e, no entanto, não existe $\gamma \in \mathcal{O}_{\mathbb{K}}$ tal que $\gamma + \bar{\gamma} = 1$.

i-) Mostremos que b_α é par. De fato, se $x \in P = 2\mathcal{O}_{\mathbb{K}} + (\zeta - 1)\mathcal{O}_{\mathbb{K}}$, então existem $a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3 \in \mathbb{Z}$ tal que $x = 2(a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3) - (1 - \zeta)(b_0 + b_1\zeta + b_2\zeta^2 + b_3\zeta^3) = 2a_0 - b_0 - b_3 + (2a_1 - b_1 + b_0)\zeta + (2a_2 - b_2 + b_1)\zeta^2 + (2a_3 - b_3 + b_2)\zeta^3$.

Agora

$$\begin{aligned} x\phi(x) &= [(2a_0 - b_0 - b_3) + (2a_1 - b_1 + b_0)\zeta + (2a_2 - b_2 + b_1)\zeta^2 + (2a_3 - b_3 + b_2)\zeta^3][(2a_0 - b_0 - b_3) + (2a_1 - b_1 + b_0)\zeta^7 + (2a_2 - b_2 + b_1)\zeta^6 + (2a_3 - b_3 + b_2)\zeta^5] \\ &= (2a_0 - b_0 - b_3)^2 - (2a_0 - b_0 - b_3)(2a_1 - b_1 + b_0)\zeta^3 \\ &\quad - (2a_0 - b_0 - b_3)(2a_2 - b_2 + b_1)\zeta^2 - (2a_0 - b_0 - b_3)(2a_3 - b_3 + b_2)\zeta + (2a_1 - b_1 + b_0)(2a_0 - b_0 - b_3) \\ &\quad + (2a_1 - b_1 + b_0)^2 - (2a_1 - b_1 + b_0)(2a_2 - b_2 + b_1)\zeta^3 - (2a_1 - b_1 + b_0)(2a_3 - b_3 + b_2)\zeta^2 \\ &\quad + (2a_2 - b_2 + b_1)(2a_0 - b_0 - b_3)\zeta^2 + (2a_2 - b_2 + b_1)(2a_1 - b_1 + b_0)\zeta + (2a_2 - b_2 + b_1)^2 \\ &\quad - (2a_2 - b_2 + b_1)(2a_3 - b_3 + b_2)\zeta^3 + (2a_3 - b_3 + b_2)(2a_0 - b_0 - b_3)\zeta^3 + (2a_3 - b_3 + b_2)(2a_1 - b_1 + b_0)\zeta^2 \\ &\quad + (2a_3 - b_3 + b_2)(2a_2 - b_2 + b_1)\zeta + (2a_3 - b_3 + b_2)^2. \end{aligned}$$

Aplicando o traço, temos que

$$\begin{aligned} \text{Tr}_{\mathbb{K}|\mathbb{Q}}(x\phi(x)) &= 4(2a_0 - (b_0 + b_3))^2 + 4(2a_1 - b_1 + b_0)^2 + 4(2a_2 - b_2 + b_1)^2 + 4(2a_3 - b_3 + b_2)^2 \\ &= 8[2a_0^2 + 2a_1^2 + 2a_2^2 + 2a_3^2 - 2a_0(b_0 + b_3) + 2a_1(b_0 - b_1) + 2a_2(b_1 - b_2) + 2a_3(b_2 - b_3) + b_0^2 + b_1^2 + b_2^2 + b_3^2 + b_0b_3 - b_0b_1 - b_1b_2 - b_2b_3]. \end{aligned}$$

Portanto, segue que

$$\frac{1}{4}Tr_{\mathbb{K}|\mathbb{Q}}(x\phi(x)) = 2[2a_0^2 + 2a_1^2 + 2a_2^2 + 2a_3^2 - 2a_0(b_0 + b_3) + 2a_1(b_0 - b_1) + 2a_2(b_1 - b_2) + 2a_3(b_2 - b_3) + b_0^2 + b_1^2 + b_2^2 + b_3^2 + b_0b_3 - b_0b_1 - b_1b_2 - b_2b_3].$$

Logo, se $x \neq 0$, então $\frac{1}{4}Tr_{\mathbb{K}|\mathbb{Q}}(x\phi(x))$ é um número par.

ii-) Mostremos agora que não existe $\gamma \in \mathcal{O}_{\mathbb{K}}$ tal que $\gamma + \bar{\gamma} = 1$. De fato, seja $\gamma = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 \in \mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_8]$. Assim, $\gamma + \bar{\gamma} = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_0 + a_1\zeta^7 + a_2\zeta^6 + a_3\zeta^5$. Como $\phi_4(x) = x^4 + 1$, temos que $\zeta^4 = -1$, assim, segue que $\gamma + \bar{\gamma} = 2a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 - a_1\zeta^3 - a_2\zeta = 2a_0 + (a_1 - a_3)\zeta + (a_3 - a_1)\zeta^3$. Para que $\gamma + \bar{\gamma} = 1$ é necessário que

$$\begin{cases} 2a_0 = 1 \\ a_1 - a_3 = 0 \end{cases}$$

Não existe solução inteira que satisfaça este sistema. Logo, não existe $\gamma \in \mathbb{Z}[\zeta_8]$ tal que $\gamma + \bar{\gamma} = 1$.

Lema 7.1.2 *Sejam \mathbb{K} um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de \mathbb{K} sobre \mathbb{Z} . Se I é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$, existe $d \in \mathbb{Z} - \{0\}$ tal que $dI \subset \mathcal{O}_{\mathbb{K}}$.*

Demonstração: Como \mathbb{K} é um corpo de números de grau n , temos que existe $\alpha \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\alpha)$ e $\{1, \alpha, \dots, \alpha^{n-1}\}$ é uma base de \mathbb{K} sobre \mathbb{Q} . Como I é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$, então I é um \mathbb{Z} -módulo livre de posto n . Seja $\{\gamma_1, \dots, \gamma_n\}$ uma \mathbb{Z} -base de I . Para cada i , temos que $\gamma_i = \sum_{j=0}^{n-1} a_{ij}\alpha^j$ tal que $a_{ij} \in \mathbb{Q}$, para todo $i = 1, \dots, n$ e $j = 0, 1, \dots, n-1$.

Como $a_{ij} \in \mathbb{Q}$, para todo $i, j = 1, \dots, n$, segue que $a_{ij} = \frac{b_{ij}}{c_{ij}}$; $b_{ij}, c_{ij} \in \mathbb{Z}$ e $c_{ij} \neq 0$, para todo $i, j = 1, \dots, n$. Seja $d = \text{mmc}\{c_{ij}; i = 1, \dots, n, j = 0, 1, \dots, n-1\}$. Temos que $d\gamma_i \in \mathbb{Z}[\alpha]$, para todo $i = 1, \dots, n$. Como $\mathbb{Z}[\alpha] \subset \mathcal{O}_{\mathbb{K}}$, temos que $dI = d \sum_{i=1}^n \mathbb{Z}\gamma_i = \sum_{i=1}^n \mathbb{Z}d\gamma_i \subset \mathbb{Z}[\alpha] \subset \mathcal{O}_{\mathbb{K}}$, como queríamos. ■

Teorema 7.1.1 *Seja I um ideal fracionário não nulo de $\mathcal{O}_{\mathbb{K}}$. Se (I, b_α) é um reticulado ideal, então*

$$\det(b_\alpha) = N(I)^2 N_{\mathbb{K}|\mathbb{Q}}(\alpha) |\text{Disc}(\mathbb{K}|\mathbb{Q})|.$$

Demonstração: Se I é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$, então, pelo Lema (7.1.2), existem $d \in \mathbb{Z} - \{0\}$ e $A \subset \mathcal{O}_{\mathbb{K}}$ um ideal tal que $dI = A \subset \mathcal{O}_{\mathbb{K}}$. Como $\mathcal{O}_{\mathbb{K}}$ é um \mathbb{Z} -módulo livre de posto n e A é um \mathbb{Z} -submódulo de $\mathcal{O}_{\mathbb{K}}$, pelo Teorema (1.2.1), segue que existe uma \mathbb{Z} -base $\{w_1, \dots, w_n\}$ de $\mathcal{O}_{\mathbb{K}}$ e inteiros e_1, \dots, e_n tais que $\{e_1w_1, \dots, e_nw_n\}$ é uma \mathbb{Z} -base de A . Desta forma, como

$dI = A$, segue que $I = d^{-1}A$. Assim, $\{e_1d^{-1}w_1, \dots, e_nd^{-n}w_n\}$ é uma \mathbb{Z} -base de I . Temos que a matriz de b_α é dada por

$$= \begin{pmatrix} \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha e_1 d^{-1} w_1 \overline{e_1 d^{-1} w_1}) & \cdots & \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha e_1 d^{-1} w_1 \overline{e_n d^{-1} w_n}) \\ \vdots & \ddots & \vdots \\ \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha e_n d^{-1} w_n \overline{e_1 d^{-1} w_1}) & \cdots & \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha e_n d^{-1} w_n \overline{e_n d^{-1} w_n}) \\ \vdots & \ddots & \vdots \\ e_1^2 \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha d^{-1} d^{-1} w_1 \overline{w_1}) & \cdots & e_1 e_n \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha d^{-1} d^{-1} w_1 \overline{w_n}) \\ \vdots & \ddots & \vdots \\ e_1 e_n \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha d^{-1} d^{-1} w_n \overline{w_1}) & \cdots & e_n^2 \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha d^{-1} d^{-1} w_n \overline{w_n}) \end{pmatrix}.$$

Assim, segue que

$$\begin{aligned} \det(b_\alpha) &= (e_1 e_2 \cdots e_n)^2 \det \begin{pmatrix} \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha (d^{-1})^2 w_1 \overline{w_1}) & \cdots & \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha (d^{-1})^2 w_1 \overline{w_n}) \\ \vdots & \ddots & \vdots \\ \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha (d^{-1})^2 w_n \overline{w_1}) & \cdots & \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha (d^{-1})^2 w_n \overline{w_n}) \end{pmatrix} \\ &= (e_1 e_2 \cdots e_n)^2 ((d^{-1})^2)^n \det \begin{pmatrix} \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha w_1 \overline{w_1}) & \cdots & \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha w_1 \overline{w_n}) \\ \vdots & \ddots & \vdots \\ \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha w_n \overline{w_1}) & \cdots & \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha w_n \overline{w_n}) \end{pmatrix}. \end{aligned}$$

Agora, temos, pela Proposição (1.9.5), que $N(A) = |e_1 \cdots e_n|$. Logo,

$$\det(b_\alpha) = N(A)^2 ((d^{-1})^2)^n \det(H),$$

onde

$$H = \begin{pmatrix} \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha w_1 \overline{w_1}) & \cdots & \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha w_1 \overline{w_n}) \\ \vdots & \ddots & \vdots \\ \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha w_n \overline{w_1}) & \cdots & \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha w_n \overline{w_n}) \end{pmatrix}.$$

Agora, notemos que $H = MM^\perp$, onde

$$M = TA = \begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_n(w_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(w_n) & \cdots & \sigma_n(w_n) \end{pmatrix} \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sqrt{\sigma_n(\alpha)} \end{pmatrix}$$

e \perp denota a tranposta conjugada. Assim, $\det(H) = \det(M)\det(M^\perp) = \det(T)\det(A)\det(A^\perp)\det(T^\perp) = (\det(A))^2\det(T)\overline{\det(T)} = (\det(A))^2|\det(T)|^2$. Mas, temos que $(\det(A))^2 = \sigma_1(\alpha) \cdots \sigma_n(\alpha) = N_{\mathbb{K}|\mathbb{Q}}(\alpha)$. Por outro lado, $\det(T) = \det(\sigma_i(w_j))_{i,j=1}^n = \sqrt{|\text{Disc}(\mathbb{K}|\mathbb{Q})|}$. Desta forma, segue que

$$\det(b_\alpha) = N(A)^2((d^{-1})^2)^n N_{\mathbb{K}|\mathbb{Q}}(\alpha) |\text{Disc}(\mathbb{K}|\mathbb{Q})|.$$

Agora, como $d \in \mathbb{Z}$, segue que $N(I) = N(A)N_{\mathbb{K}|\mathbb{Q}}(d^{-1}) = N(A)(d^{-1})^n$. Logo, $N(I)^2 = N(A)^2((d^{-1})^n)^2$. Portanto, $\det(b_\alpha) = N(I)^2 N_{\mathbb{K}|\mathbb{Q}}(\alpha) |\text{Disc}(\mathbb{K}|\mathbb{Q})|$. ■

Exemplo 7.1.7 Consideremos o reticulado ideal (P, b_α) do Exemplo (7.1.6). Temos, pelo Teorema (7.1.1), que $\det(b_\alpha) = N(P)^2 N_{\mathbb{K}|\mathbb{Q}}(\frac{1}{4}) |\text{Disc}(\mathbb{K}|\mathbb{Q})| = 2^2 \left(\frac{1}{4}\right)^4 2^8 = 2^{10} 2^{-8} = 4$, pois, pelo Teorema (3.2.3), segue que $|\text{Disc}(\mathbb{K}|\mathbb{Q})| = 2^8$. Assim, temos que (P, b_α) é um reticulado ideal par com determinante 4.

A próxima proposição apresenta uma expressão para a diversidade de reticulados ideais (I, b_α) quando I é um ideal inteiro de $\mathcal{O}_{\mathbb{K}}$.

Proposição 7.1.4 Seja $I \subset \mathcal{O}_{\mathbb{K}}$ um ideal. Um reticulado ideal $\Lambda = (I, b_\alpha)$ tem diversidade $\text{div}(\Lambda) = r_1 + r_2$.

Demonstração: Seja $x \neq 0$ um ponto do reticulado Λ . Temos que existe $y \in I$ tal que $x = \sigma_\alpha(y) = (\sqrt{\alpha_1}\sigma_1(y), \dots, \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(y)), \dots, \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(y)))$. Como $x \neq 0$, segue que $y \neq 0$. Sendo $y \neq 0$, temos que $\sigma_i(y) \neq 0$, para todo $i = 1, \dots, n$. Logo, os primeiros r_1 coeficientes de x são não nulos. Agora, notemos que como $\sigma_{r_1+i}(y) \neq 0$, para todo $i = 1, \dots, r_2$, segue que $\Re(\sigma_{r_1+i}(y)) \neq 0$ ou $\Im(\sigma_{r_1+i}(y)) \neq 0$. Desta forma, destes $n - r_1$ coeficientes restantes de x , pelo menos $\frac{n - r_1}{2} = r_2$ são não nulos. Assim, $\text{div}(\Lambda) \geq r_1 + r_2$. Seja agora $\beta \in I$ tal que $\beta \neq 0$. Como $I \subset \mathcal{O}_{\mathbb{K}}$, segue que β é raiz de um polinômio mônico com coeficientes em \mathbb{Z} . Assim, existem $a_0, a_1, \dots, a_{m-1} \in \mathbb{Z}$ tal que $\beta^m + a_{m-1}\beta^{m-1} + \dots + a_1\beta + a_0 = 0$ e $a_0 \neq 0$. Logo, $-a_0 = \alpha^m + a_{m-1}\alpha^{m-1} + \dots + a_1\alpha \in I$. Como $-a_0 \in \mathbb{Z}$, segue que $\sigma_i(-a_0) = -a_0$, para todo $i = 1, \dots, n$. Logo, $\text{div}(-a_0) = r_1 + r_2$. Portanto, $\text{div}(\Lambda) = r_1 + r_2$. ■

Proposição 7.1.5 Seja $I \subset \mathcal{O}_{\mathbb{K}}$ um ideal. Um reticulado ideal $\Lambda = (I, b_\alpha)$ pode ser imerso no \mathbb{R}^n com

- diversidade n se \mathbb{K} é totalmente real.
- diversidade $\frac{n}{2}$ se \mathbb{K} é totalmente complexo.

Demonstração: Segue diretamente da Proposição (7.1.4). ■

O próximo teorema apresenta uma expressão para a distância produto mínima de reticulados ideais quando o corpo \mathbb{K} é totalmente real e I é um ideal inteiro de $\mathcal{O}_{\mathbb{K}}$.

Teorema 7.1.2 *Se \mathbb{K} é um corpo de números totalmente real de grau n com discriminante $Disc(\mathbb{K}|\mathbb{Q})$ e I um ideal inteiro de $\mathcal{O}_{\mathbb{K}}$, então a distância produto mínima de um reticulado ideal $\Lambda = (I, b_\alpha)$ é dada por*

$$d_{p,min}(\Lambda) = \sqrt{\frac{\det(b_\alpha)}{|Disc(\mathbb{K}|\mathbb{Q})|}} \min(I),$$

onde $\min(I) = \min_{0 \neq y \in I} \frac{|N_{\mathbb{K}|\mathbb{Q}}(y)|}{N(I)}$.

Demonstração: Como \mathbb{K} é totalmente real, segue que a diversidade de Λ é n e $\sigma_i(\mathbb{K}) \subset \mathbb{R}$, para todo $i = 1, \dots, n$. Seja $x = \sigma_\alpha(y)$ um ponto do reticulado no \mathbb{R}^n com $y \in I \subseteq \mathcal{O}_{\mathbb{K}}$ seu inteiro algébrico correspondente. Temos que

$$\begin{aligned} d_{p,min}(\Lambda) &= \min_{0 \neq x \in \Lambda} \prod_{j=1}^n |x_j| \\ &= \min_{0 \neq y \in I} \prod_{j=1}^n |\sqrt{\sigma_j(\alpha)} \sigma_j(y)| \\ &= \sqrt{N_{\mathbb{K}|\mathbb{Q}}(\alpha)} \min_{0 \neq y \in I} |N_{\mathbb{K}|\mathbb{Q}}(y)|. \end{aligned}$$

Pela Proposição (7.1.1), temos que $\det(b_\alpha) = N_{\mathbb{K}|\mathbb{Q}}(\alpha) N(I)^2 |Disc(\mathbb{K}|\mathbb{Q})|$ e, assim,

$$\sqrt{N_{\mathbb{K}|\mathbb{Q}}(\alpha)} = \frac{\sqrt{\det(b_\alpha)}}{\sqrt{N(I)^2 |Disc(\mathbb{K}|\mathbb{Q})|}}.$$

Desta forma,

$$\begin{aligned} d_{p,min}(\Lambda) &= \sqrt{\frac{\det(b_\alpha)}{|Disc(\mathbb{K}|\mathbb{Q})|}} \frac{1}{N(I)} \min_{0 \neq y \in I} |N_{\mathbb{K}|\mathbb{Q}}(y)| \\ &= \sqrt{\frac{\det(b_\alpha)}{|Disc(\mathbb{K}|\mathbb{Q})|}} \frac{\min_{0 \neq y \in I} |N_{\mathbb{K}|\mathbb{Q}}(y)|}{N(I)} \\ &= \sqrt{\frac{\det(b_\alpha)}{|Disc(\mathbb{K}|\mathbb{Q})|}} \min(I), \end{aligned}$$

o que prova o teorema. ■

Lema 7.1.3 *Seja \mathbb{K} um corpo de números. Se I é um ideal principal de $\mathcal{O}_{\mathbb{K}}$, então*

$$\min_{x \neq 0 \in I} |N_{\mathbb{K}|\mathbb{Q}}(x)| = N(I).$$

Demonstração: Como I é um ideal principal, segue que $I = \langle a \rangle$, com $a \in I$ e $N(I) = |N_{\mathbb{K}|\mathbb{Q}}(a)|$. Se $x \in I$, $x \neq 0$, então $x = ay$, para algum $y \in \mathcal{O}_{\mathbb{K}}$. Assim,

$$|N_{\mathbb{K}|\mathbb{Q}}(x)| = |N_{\mathbb{K}|\mathbb{Q}}(a)| |N_{\mathbb{K}|\mathbb{Q}}(y)| \geq N(I)$$

e a igualdade é verdadeira se, e somente se, $N_{\mathbb{K}|\mathbb{Q}}(y) = \pm 1$ se, e somente se, y é uma unidade de $\mathcal{O}_{\mathbb{K}}$. Portanto, $N_{\mathbb{K}|\mathbb{Q}}(x) = N(I)$ quando $x = ay$, com y uma unidade de $\mathcal{O}_{\mathbb{K}}$. Logo, $\min_{x \neq 0 \in I} |N_{\mathbb{K}|\mathbb{Q}}(x)| = N(I)$. ■

Quando I é principal, a distância produto mínima de um reticulando ideal (I, b_α) pode ser calculada conforme o seguinte resultado.

Corolário 7.1.1 *Se \mathbb{K} é um corpo de números totalmente real e I um ideal principal de $\mathcal{O}_{\mathbb{K}}$, então a distância produto mínima de um reticulando ideal (I, b_α) é dada por*

$$d_{p,\min}(\Lambda) = \sqrt{\frac{\det(b_\alpha)}{|Disc(\mathbb{K}|\mathbb{Q})|}}.$$

Demonstração: Segue do Teorema (7.1.2) e do Lema (7.1.3). ■

Capítulo 8

Construção de \mathbb{Z}^n -Reticulados Rotacionados via Reticulados Ideais

Dois parâmetros relacionados com a probabilidade de erros de um dado código reticulado são a diversidade e a distância produto mínima. Em [[20]], vemos que quanto maior for a diversidade l e a $d_{p,min}^l$ do reticulado, menor é a probabilidade de ocorrerem erros. Desta forma, sempre procuramos reticulados com diversidade l alta e $d_{p,min}^l$ máxima.

Neste capítulo apresentaremos a construção do reticulado \mathbb{Z}^n , $n \geq 2$, via reticulados ideais. O reticulado \mathbb{Z}^n é um reticulado n -dimensional definido por

$$\mathbb{Z}^n = \{(x_1, \dots, x_n); x_i \in \mathbb{Z}; \forall i = 1, \dots, n\}.$$

Podemos tomar como matriz geradora M de \mathbb{Z}^n a matriz identidade e, assim, $\det(\mathbb{Z}^n) = 1$.

A importância de estudar \mathbb{Z}^n -reticulados é o fato destes reticulados apresentarem implementação prática.

A fim de obtermos um reticulado ideal semelhante ao reticulado \mathbb{Z}^n , $n \geq 2$, com alta diversidade l e $d_{p,min}^l$ máxima, iremos trabalhar com corpos de números totalmente reais, pois vimos que em tais corpos a diversidade é máxima.

Sejam \mathbb{K} um corpo de números totalmente real de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de \mathbb{K} sobre \mathbb{Z} . O objetivo é encontrar um reticulado ideal $\Lambda = (\mathcal{O}_{\mathbb{K}}, b_\alpha)$ que seja um \mathbb{Z}^n -reticulado rotacionado, ou seja, um reticulado com as mesmas propriedades de \mathbb{Z}^n .

Neste capítulo apresentamos duas construções de \mathbb{Z}^n -reticulados rotacionados. Na Seção 8.1, apresentamos a construção via o subcorpo real maximal dos corpos ciclotômicos $\mathbb{Q}(\zeta_p)$; p primo e, na Seção 8.2, via o subcorpo real maximal dos corpos ciclotômicos $\mathbb{Q}(\zeta_{2^r})$, r positivo.

Notemos que dado $c \in \mathbb{Z}$, $(\sqrt{c}\mathbb{Z})^n$ é uma versão escalar de \mathbb{Z}^n obtida multiplicando todos os pontos do reticulado \mathbb{Z}^n por \sqrt{c} . Nas duas construções a serem apresentadas o primeiro passo será encontrar um elemento $\alpha \in \mathbb{K}$ totalmente positivo tal que o reticulado ideal $(\mathcal{O}_{\mathbb{K}}, b_\alpha)$ seja isomorfo ao reticulado $(\sqrt{c}\mathbb{Z})^n$. Após encontrarmos tal reticulado multiplicamos sua matriz geradora por $1/\sqrt{c}$ e assim, obtemos uma versão rotacionada de \mathbb{Z}^n .

Como $\det((\sqrt{c}\mathbb{Z})^n) = c^n$, a fim de que $(\mathcal{O}_{\mathbb{K}}, b_\alpha)$ seja isomorfo a $(\sqrt{c}\mathbb{Z})^n$, segue que o elemento α deve satisfazer a relação $N_{\mathbb{K}|\mathbb{Q}}(\alpha)|Disc(\mathbb{K}|\mathbb{Q})| = c^n$, do Teorema (7.1.1). Notemos, entretanto, que encontrar um elemento $\alpha \in \mathbb{K}$ totalmente positivo tal que $N_{\mathbb{K}|\mathbb{Q}}(\alpha)|Disc(\mathbb{K}|\mathbb{Q})| = c^n$ não garante que $(\mathcal{O}_{\mathbb{K}}, b_\alpha)$ seja isomorfo a $(\sqrt{c}\mathbb{Z})^n$. Esta é apenas uma condição necessária.

8.1 Reticulados Rotacionados via o Corpo Ciclotômico $\mathbb{Q}(\zeta_p)$.

Nesta seção, veremos a construção de \mathbb{Z}^n -reticulados rotacionados via a teoria de reticulados ideais aplicada ao subcorpo real maximal $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ dos corpos ciclotômicos $\mathbb{Q}(\zeta_p)$, com p primo, $p \geq 5$. Desta forma, serão obtidos \mathbb{Z}^n -reticulados rotacionados para $n = \frac{p-1}{2}$, p primo, $p \geq 5$.

Para isto, sejam p um número primo tal que $p \geq 5$, $\zeta = \zeta_p$ uma raiz p -ésima primitiva da unidade, $\mathcal{A} = \mathbb{Z}$, $\mathbb{L} = \mathbb{Q}(\zeta_p)$ e $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$.

Pelo Teorema (2.2.1), temos que $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$ e, pela Proposição (2.2.4), temos que $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\zeta_p + \zeta_p^{-1})] = 2$. Assim, temos que $[\mathbb{Q}(\zeta_p + \zeta_p^{-1}) : \mathbb{Q}] = \frac{p-1}{2}$.

$$p-1 \begin{pmatrix} \mathbb{Q}(\zeta_p) \\ |2 \\ \mathbb{Q}(\zeta_p + \zeta_p^{-1}) \\ |\frac{p-1}{2} \\ \mathbb{Q} \end{pmatrix}$$

Observação 8.1.1 ([20]) *Sejam p um número primo tal que $p \geq 5$ e $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Temos que $|Disc(\mathbb{K}|\mathbb{Q})| = p^{\frac{p-3}{2}}$.*

Seja $\Lambda = (\mathcal{O}_{\mathbb{K}}, b_\alpha)$. Uma condição necessária, mas não suficiente, para que Λ seja isomorfo a $(\sqrt{c}\mathbb{Z})^n$, uma versão escalar de \mathbb{Z}^n , com $c \in \mathbb{Z}$ é que $\det(\Lambda) = c^n$. Pelo Teorema (7.1.1), temos que $\det(\Lambda) = N(I)^2 N_{\mathbb{K}|\mathbb{Q}}(\alpha)|Disc(\mathbb{K}|\mathbb{Q})|$ e, se $I = \mathcal{O}_{\mathbb{K}}$, então $\det(\Lambda) = N_{\mathbb{K}|\mathbb{Q}}(\alpha)|Disc(\mathbb{K}|\mathbb{Q})|$.

Desta forma, para que Λ seja isomorfo a $(\sqrt{c}\mathbb{Z})^n$ é necessário encontrar um elemento $\alpha \in \mathbb{K}$ totalmente positivo tal que $N_{\mathbb{K}|\mathbb{Q}}(\alpha)Disc(\mathbb{K}|\mathbb{Q}) = N_{\mathbb{K}|\mathbb{Q}}(\alpha)p^{\frac{p-3}{2}} = c^{\frac{p-1}{2}}$, para algum $c \in \mathbb{Z}$. Tomando $c = p$, devemos encontrar $\alpha \in \mathbb{K}$ tal que $N_{\mathbb{K}|\mathbb{Q}}(\alpha) = p$. Pelo Exemplo (4.1.1), temos que $p\mathbb{Z}[\zeta_p] = (1 - \zeta_p)^{p-1}\mathbb{Z}[\zeta_p]$ e $N_{\mathbb{L}|\mathbb{Q}}(1 - \zeta_p) = p$. Usando a transitividade da norma, temos que

$$p = N_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(1 - \zeta_p) = N_{\mathbb{K}|\mathbb{Q}}(N_{\mathbb{Q}(\zeta_p)|\mathbb{K}}(1 - \zeta_p)) = N_{\mathbb{K}|\mathbb{Q}}((1 - \zeta_p)(1 - \zeta_p^{-1})).$$

Assim, tomando $\alpha = (1 - \zeta_p)(1 - \zeta_p^{-1}) = 2 - (\zeta_p + \zeta_p^{-1})$, temos que $N_{\mathbb{K}|\mathbb{Q}}(\alpha) = p$. Deste modo, encontramos um elemento α que satisfaz a condição inicial e, agora através de uma construção explícita iremos mostrar que $(\mathcal{O}_{\mathbb{K}}, b_\alpha)$ é isomorfo a \mathbb{Z}^n .

Pelo Teorema (2.2.3), temos que $\{e_j = \zeta_p^j + \zeta_p^{-j}\}_{j=1}^{\frac{p-1}{2}}$ é uma \mathbb{Z} -base de $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$.

Teorema 8.1.1 *Se $\alpha = 2 - (\zeta_p + \zeta_p^{-1})$ e $b_\alpha(x, y) = Tr_{\mathbb{K}|\mathbb{Q}}(\alpha xy)$, para todo $x, y \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$, então:*

1. $b_\alpha(e_i, e_i) = \begin{cases} p, & \text{se } i = n; \\ 2p, & \text{caso contrário.} \end{cases}$
2. $b_\alpha(e_i, e_j) = \begin{cases} -p, & \text{se } |i - j| = 1; \\ 0, & \text{caso contrário} \end{cases}$

Demonstração: Para simplificar a notação vamos denotar por $\sigma_k(\zeta)$ e por $\alpha_j = \sigma_j(\alpha)$, os conjugados de ζ e α , respectivamente. Temos que

$$Tr_{\mathbb{K}|\mathbb{Q}}(\zeta^k + \zeta^{-k}) = -1, \text{ para } k = 1, \dots, n.$$

De fato, como o polinômio ciclotômico de ζ é $f(x) = x^{p-1} + \dots + x + 1$ e ζ^k , $k = 1, \dots, n$ são conjugados de ζ , segue que $Tr_{\mathbb{L}|\mathbb{Q}}(\zeta^k) = -1$, $k = 1, \dots, n$. Assim, como $Tr_{\mathbb{L}|\mathbb{Q}}(\zeta^k) = Tr_{\mathbb{K}|\mathbb{Q}}(Tr_{\mathbb{L}|\mathbb{K}}(\zeta^k))$, segue que $Tr_{\mathbb{K}|\mathbb{Q}}(\zeta^k + \zeta^{-k}) = -1$, para todo $k = 1, \dots, n$. Desta forma, temos que

$$\begin{aligned} Tr_{\mathbb{K}|\mathbb{Q}}(\alpha(\zeta^k + \zeta^{-k})) &= \sum_{j=1}^n \sigma_j(\alpha)\sigma_j(\zeta^k + \zeta^{-k}) \\ &= \sum_{j=1}^n \alpha_j\sigma_j(\zeta^k + \zeta^{-k}) \\ &= \sum_{j=1}^n (2 - \sigma_j(\zeta + \zeta^{-1}))\sigma_j(\zeta^k + \zeta^{-k}) \end{aligned}$$

$$\begin{aligned}
&= -2 - \sum_{j=1}^n \sigma_j(\zeta^{k+1} + \zeta^{-k-1} + \zeta^{-k+1} + \zeta^{k-1}) \\
&= \begin{cases} -2 + 1 - 2n = -p, & \text{se } k = \pm 1 \pmod{p} \\ -2 + 1 + 1 = 0, & \text{caso contrário.} \end{cases}
\end{aligned}$$

Agora, vamos calcular $b_\alpha(e_i, e_j)$. Temos que

$$\begin{aligned}
b_\alpha(e_i, e_i) &= \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha e_i^2) = \sum_{j=1}^n \alpha_j \sigma_j(\zeta^{2i} + \zeta^{-2i} + 2) \\
&= \sum_{j=1}^n \alpha_j \sigma_j(\zeta^{2i} + \zeta^{-2i}) + 2 \sum_{j=1}^n (2 - \sigma_j(\zeta + \zeta^{-1})) \\
&= \begin{cases} p, & \text{se } i = n; \\ 2p, & \text{caso contrário.} \end{cases}
\end{aligned}$$

$$\begin{aligned}
b_\alpha(e_i, e_j) &= \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha e_i e_j) = \sum_{j=1}^n (\alpha_j \sigma_j(\zeta^{i+j} + \zeta^{-(i+j)})) + \sum_{j=1}^n (\alpha_j \sigma_j(\zeta^{i-j} + \zeta^{-(i-j)})) \\
&= \begin{cases} -p, & \text{se } |i - j| = 1; \\ 0, & \text{caso contrário,} \end{cases}
\end{aligned}$$

o que prova o teorema. ■

Corolário 8.1.1 *Se $B_\alpha(x, y) = \frac{1}{p} \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha xy)$, então a matriz de B_α na base $\{e_1, \dots, e_n\}$ é dada por*

$$\begin{pmatrix} 2 & -1 & 0 & \cdots & \cdots & 0 \\ -1 & 2 & -1 & \cdots & \vdots & \vdots \\ 0 & -1 & 2 & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & & -1 & 0 \\ \vdots & \vdots & \vdots & -1 & 2 & -1 \\ 0 & \cdots & \cdots & 0 & -1 & 1 \end{pmatrix}. \tag{8.1}$$

Demonstração: Segue diretamente do Teorema (8.1.1). ■

Lema 8.1.1 *Se $e'_n = e_n$, $e'_j = \sum_{i=j}^n e_i$, $j = 1, \dots, n-1$, então $\{e'_1, \dots, e'_n\}$ é uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta + \zeta^{-1}]$.*

Demonstração: Mostremos que $\{e'_1, \dots, e'_n\}$ é linearmente independente sobre \mathbb{Z} . De fato, seja $\sum_{i=1}^n a_i \bar{e}_i = 0$; $a_i \in \mathbb{Z}$. Temos que $\sum_{i=1}^n a_i e'_i = a_1 e_1 + (a_1 + a_2) e_2 + \dots + (a_1 + \dots + a_{n-1}) e_{n-1} + (a_1 + \dots + a_n) e_n = 0$. Como $\{e_1, \dots, e_n\}$ é uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}}$, segue que $a_1 = \dots = a_n = 0$. Mostremos agora que $\{e'_1, \dots, e'_n\}$ gera $\mathbb{Z}[\zeta + \zeta^{-1}]$. Seja $x \in \mathbb{Z}[\zeta + \zeta^{-1}]$. Temos que $x = \sum_{i=1}^n a_i e_i$; $a_i \in \mathbb{Z}$. Seja $b_1 = a_1$. Temos que $x = \sum_{i=2}^n (a_i - a_1) e_i + a_1 (e_1 + \dots + e_n) = \sum_{i=2}^n (a_i - a_1) e_i + b_1 e'_1$. Se $b_2 = (a_2 - a_1)$, então $x = \sum_{i=3}^n (a_i - a_1 - (a_2 - a_1)) e_i + b_2 e'_2 + b_1 e'_1$. Continuando desta forma, tomando $b_j = a_j - a_{j-1}$, $j = 2, \dots, n$, temos que $x = \sum_{i=1}^n b_i e'_i$. Portanto, $\{e'_1, \dots, e'_n\}$ é uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}}$. ■

Proposição 8.1.1 Se $e'_n = e_n$ e $e'_j = \sum_{i=j}^n e_i$, para $j = 1, \dots, n-1$, então $\frac{1}{p} \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha e'_i e'_j) = \delta_{ij}$, onde δ_{ij} é o delta de Kronecker.

Demonstração: Sejam G a matriz do Corolário (8.1.1) e

$$T = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & 1 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Temos que $TGT^t = I_n$. Agora, $G = MM^t$, onde $M = \frac{1}{\sqrt{p}} NA$, com

$$N = \begin{pmatrix} \sigma_1(e_1) & \dots & \sigma_n(e_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_n) & \dots & \sigma_n(e_n) \end{pmatrix} \text{ e } A = \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \sqrt{\sigma_n(\alpha)} \end{pmatrix}.$$

Assim, $I_n = T(MM^t)T^t = (TM)(TM)^t$. Seja agora $e'_n = e_n$, $e'_j = \sum_{i=j}^n e_i$; $j = 1, \dots, n-1$ uma

outra base de $\mathcal{O}_{\mathbb{K}}$. Temos que

$$\begin{pmatrix} \sigma_1(e'_1) & \cdots & \sigma_n(e'_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(e'_n) & \cdots & \sigma_n(e'_n) \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} \sigma_1(e_1) & \cdots & \sigma_n(e_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_n) & \cdots & \sigma_n(e_n) \end{pmatrix}.$$

Desta forma, $\overline{M} = \frac{1}{\sqrt{p}}TNA$ é uma matriz geradora do reticulado $(\mathcal{O}_{\mathbb{K}}, b_{\alpha})$. Como $\overline{M}\overline{M}^t = \frac{1}{p}TNA A^t N^t T^t = TMM^t T^t = I_n$, segue que $\frac{1}{p}Tr_{\mathbb{K}|\mathbb{Q}}(\alpha e'_i e'_j) = \delta_{ij}$, onde δ_{ij} é o delta de Kronecker. ■

Segue, da Proposição (8.1.1), que o reticulado ideal $\Lambda = (\mathcal{O}_{\mathbb{K}}, \frac{1}{p}b_{\alpha})$, com $\alpha = 2 - (\zeta + \zeta^{-1})$ é isomorfo ao reticulado \mathbb{Z}^n .

Se considerarmos a matriz geradora

$$M = \frac{1}{\sqrt{p}}TNA, \text{ onde}$$

$$N = \begin{pmatrix} \sigma_1(e_1) & \cdots & \sigma_n(e_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_n) & \cdots & \sigma_n(e_n) \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 1 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \text{ e}$$

$$A = \text{diag}(\sqrt{\sigma_k(\alpha)}),$$

temos que $MM^t = I_n$.

Seguindo os passos desse algoritmo, pode-se construir \mathbb{Z}^n -reticulados rotacionados para $n = 2, 3, 5, 6, 8, 9, 11, 14, 15, 18, 20, 21, 23, 26, 29, 30, \dots$

Proposição 8.1.2 *Se Λ é um reticulado ideal de dimensão $n = \frac{p-1}{2}$, então $d_{p,\min}(\Lambda) = p^{\frac{3-p}{4}}$.*

Demonstração: Pelo Corolário (7.1.1), temos que a distância produto mínima de Λ é dada por $\frac{1}{\sqrt{|Disc(\mathbb{K}|\mathbb{Q})|}}$, uma vez que $\det(\Lambda) = 1$. Como o discriminante de \mathbb{K} satisfaz $|Disc(\mathbb{K}|\mathbb{Q})| = p^{\frac{p-3}{2}}$, segue que $d_{p,\min}(\Lambda) = p^{\frac{3-p}{4}}$. ■

A tabela a seguir fornece a $d_{p,\min}$ para a construção ciclotômica em algumas dimensões.

p	n	$d_{p,min}(\Lambda)$	$\sqrt[n]{d_{p,min}}$
5	2	$\frac{1}{\sqrt{5}}$	0,66870
7	3	$\frac{1}{7}$	0,522757
11	5	$\frac{1}{11^2}$	0,383215
13	6	$\frac{1}{\sqrt{13^5}}$	0,343444
17	8	$\frac{1}{\sqrt{17^7}}$	0,289520
19	9	$\frac{1}{19^4}$	0,27187
23	11	$\frac{1}{23^5}$	0,240454

Exemplo 8.1.1 *Sejam $p = 5$, $\mathbb{L} = \mathbb{Q}(\zeta_5)$ e $\mathbb{K} = \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$. Consideremos a \mathbb{Z} -base $\{e_1, e_2\}$ de $\mathbb{Z}[\zeta_5 + \zeta_5^{-1}]$, onde $e_1 = \zeta_5 + \zeta_5^{-1}$, $e_2 = \zeta_5^2 + \zeta_5^{-2}$ e $\alpha = 2 - (\zeta_5 + \zeta_5^{-1})$. Temos que o grupo de Galois de \mathbb{K} sobre \mathbb{Q} é dado por $\{\sigma_1, \sigma_2\}$, onde $\sigma_1(\zeta_5^k + \zeta_5^{-k}) = \zeta_5^k + \zeta_5^{-k}$; $k = 1, 2$ e $\sigma_2(\zeta_5^k + \zeta_5^{-k}) = \zeta_5^{2k} + \zeta_5^{-2k}$; $k = 1, 2$. Consideremos o reticulado ideal $(\mathcal{O}_{\mathbb{K}}, \frac{1}{5}b_\alpha)$, onde $b_\alpha(x, y) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}(xy)$. Vimos que $(\mathcal{O}_{\mathbb{K}}, \frac{1}{5}b_\alpha)$ é um \mathbb{Z}^2 -reticulado rotacionado com matriz geradora $M = \frac{1}{\sqrt{5}}TNA$, onde*

$$N = \begin{pmatrix} \sigma_1(e_1) & \sigma_2(e_1) \\ \sigma_1(e_2) & \sigma_2(e_2) \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad e \quad A = \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & 0 \\ 0 & \sqrt{\sigma_2(\alpha)} \end{pmatrix}.$$

Logo,

$$M = \frac{1}{\sqrt{5}} \begin{pmatrix} -1,175570506 & -1,902113035 \\ -1,902113034 & 1,175570503 \end{pmatrix}.$$

Tal reticulado possui $d_{p,min} = \frac{1}{\sqrt{5}}$, visto que $|\text{Disc}(\mathbb{K}|\mathbb{Q})| = 5$.

8.2 Reticulados Rotacionados via o Corpo Ciclotômico $\mathbb{Q}(\zeta_{2^r})$

Nesta seção veremos a construção de \mathbb{Z}^n -reticulados rotacionados via a teoria de reticulados ideais aplicada ao subcorpo real maximal $\mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$ dos corpos ciclotômicos $\mathbb{Q}(\zeta_{2^r})$, com r um inteiro positivo. Desta forma, serão obtidos \mathbb{Z}^n -reticulados rotacionados para $n = 2^{r-2}$, r inteiro positivo, $r \geq 3$.

Para isto, sejam $\zeta = \zeta_{2^r}$ uma raiz 2^r -ésima primitiva da unidade, onde r é um inteiro positivo, $r \geq 3$, $\mathbb{L} = \mathbb{Q}(\zeta)$ e $\mathbb{K} = \mathbb{Q}(\zeta + \zeta^{-1})$. Pelo Teorema (2.2.1), temos que $[\mathbb{L} : \mathbb{Q}] = 2^{r-1}$ e

como $[\mathbb{L} : \mathbb{K}] = 2$, segue que $[\mathbb{K} : \mathbb{Q}] = 2^{r-2} = n$.

$$2^{r-1} \begin{pmatrix} \mathbb{Q}(\zeta_{2^r}) \\ |2 \\ \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1}) \\ |2^{r-2} \\ \mathbb{Q} \end{pmatrix}$$

Os reticulados são construídos via o anel dos inteiros de \mathbb{K} , o subcorpo real maximal de \mathbb{L} , que possui $\{1, \zeta + \zeta^{-1}, \dots, \zeta^{n-1} + \zeta^{-(n-1)}\}$ como \mathbb{Z} -base.

Proposição 8.2.1 ([22]) *O discriminante de \mathbb{K} satisfaz $|\text{Disc}(\mathbb{K}|\mathbb{Q})| = 2^\beta$, onde $\beta = (r - 1)n - 1$. ■*

Seja $\Lambda = (\mathcal{O}_{\mathbb{K}}, b_\alpha)$. Uma condição necessária, mas não suficiente, para que Λ seja isomorfo a $(\sqrt{c}\mathbb{Z})^n$, uma versão escalar de \mathbb{Z}^n , com $c \in \mathbb{Z}$ é que $\det(\Lambda) = c^n$. Pelo Teorema (7.1.1), temos que $\det(\Lambda) = N(I)^2 N_{\mathbb{K}|\mathbb{Q}}(\alpha) |\text{Disc}(\mathbb{K}|\mathbb{Q})|$ e, se $I = \mathcal{O}_{\mathbb{K}}$, então $\det(\Lambda) = N_{\mathbb{K}|\mathbb{Q}}(\alpha) |\text{Disc}(\mathbb{K}|\mathbb{Q})|$. Desta forma, para que Λ seja isomorfo a $(\sqrt{c}\mathbb{Z})^n$ é necessário encontrar um elemento $\alpha \in \mathbb{K}$ totalmente positivo, tal que $N_{\mathbb{K}|\mathbb{Q}}(\alpha) |\text{Disc}(\mathbb{K}|\mathbb{Q})| = N_{\mathbb{K}|\mathbb{Q}}(\alpha) 2^\beta = c^n$, onde $\beta = (r - 1)n - 1$. Neste caso, tomando $c = 2^{r-1}$, temos que um elemento $\alpha \in \mathcal{O}_{\mathbb{K}}$ com norma 2 é facilmente encontrado. Temos que $2\mathbb{Z}[\zeta] = (1 - \zeta)^{\varphi(2^r)} \mathbb{Z}[\zeta]$ e $N_{\mathbb{L}|\mathbb{Q}}(1 - \zeta) = 2$. Usando a transitividade da norma, temos que

$$2 = N_{\mathbb{L}|\mathbb{Q}}(1 - \zeta) = N_{\mathbb{K}|\mathbb{Q}}(N_{\mathbb{L}|\mathbb{K}}(1 - \zeta)) = N_{\mathbb{K}|\mathbb{Q}}((1 - \zeta)(1 - \zeta^{-1})).$$

Desta forma, tomando $\alpha = (1 - \zeta)(1 - \zeta^{-1}) = 2 - (\zeta + \zeta^{-1})$, temos que $N_{\mathbb{K}|\mathbb{Q}}(\alpha) = 2$. Esta condição não garante a existência de uma versão escalar do \mathbb{Z}^n . Para mostrar a existência, faremos uma construção explícita.

Proposição 8.2.2 *Se $\mathbb{L} = \mathbb{Q}(\zeta)$, onde $\zeta = \zeta_{2^r}$ com r um inteiro positivo, então*

$$\text{Tr}_{\mathbb{L}|\mathbb{Q}}(\zeta^k) = \begin{cases} 0, & \text{se } \text{mdc}(k, 2^r) < 2^{r-1}; \\ -2^{r-1}, & \text{se } \text{mdc}(k, 2^r) = 2^{r-1}; \\ 2^{r-1}, & \text{se } \text{mdc}(k, 2^r) > 2^{r-1}. \end{cases}$$

Demonstração: Temos que o polinômio minimal de ζ sobre \mathbb{Q} é dado por $\phi_{2^r}(x) = x^{2^{r-1}} + 1$. Desta forma, segue que $Tr_{\mathbb{L}|\mathbb{Q}}(\zeta^k) = 0$, para todo k tal que $mdc(k, 2^r) = 1$, pois se $mdc(k, 2^r) = 1$, então ζ^k é conjugado de ζ . Agora, seja k tal que $mdc(k, 2^r) > 1$. Temos três casos para analisar:

1º caso: $mdc(k, 2^r) < 2^{r-1}$.

Seja $mdc(k, 2^r) = 2^s$, onde $s < r - 1$. Assim, $k = 2^s j$; $j \in \mathbb{Z}$ e $\zeta_{2^r}^k = \zeta_{2^r}^{2^s j} = \zeta_{2^{r-s}}^j$. Segue então que

$$\begin{aligned} Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_{2^r}^k) &= Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_{2^{r-s}}^j) = Tr_{\mathbb{Q}(\zeta_{2^{r-s}})|\mathbb{Q}}(Tr_{\mathbb{L}|\mathbb{Q}(\zeta_{2^{r-s}})}(\zeta_{2^{r-s}}^j)) \\ &= Tr_{\mathbb{Q}(\zeta_{2^{r-s}})|\mathbb{Q}}(p^s \zeta_{2^{r-s}}^j) = p^s Tr_{\mathbb{Q}(\zeta_{2^{r-s}})|\mathbb{Q}}(\zeta_{2^{r-s}}^j) = 0, \end{aligned}$$

pois $mdc(j, 2^{r-1}) = 1$.

2º caso: $mdc(k, 2^r) = 2^{r-1}$.

Temos que o polinômio minimal de ζ_2 sobre \mathbb{Q} é $\phi_2(x) = x + 1$. Desta forma, $Tr_{\mathbb{Q}(\zeta_2)|\mathbb{Q}}(\zeta_2^k) = -1$, para todo k tal que $mdc(k, 2) = 1$ e $\zeta_{2^r}^k = \zeta_{2^r}^{2^{r-1}j} = \zeta_2^j$, onde $k = 2^{r-1}j$ e $mdc(j, 2) = 1$. Segue, então, que

$$Tr_{\mathbb{Q}(\zeta_{2^r})|\mathbb{Q}}(\zeta_2^j) = Tr_{\mathbb{Q}(\zeta_2)|\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_{2^r})|\mathbb{Q}(\zeta_2)}(\zeta_2^j)) = 2^{r-1} Tr_{\mathbb{Q}(\zeta_2)|\mathbb{Q}}(\zeta_2) = -2^{r-1}.$$

Assim,

$$Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_{2^r}^k) = Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_2^j) = -2^{r-1}.$$

3º caso: $mdc(k, 2^r) > 2^{r-1}$.

Neste caso, temos que $mdc(k, 2^r) = 2^r$ e, desta forma,

$$Tr_{\mathbb{L}|\mathbb{Q}}(\zeta_{2^r}^k) = Tr_{\mathbb{L}|\mathbb{Q}}(1) = 2^{r-1},$$

o que prova a proposição. ■

Corolário 8.2.1 *Se $\mathbb{K} = \mathbb{Q}(\zeta + \zeta^{-1})$, então*

$$Tr_{\mathbb{K}|\mathbb{Q}}(\zeta^k + \zeta^{-k}) = \begin{cases} 0, & \text{se } mdc(k, 2^r) < 2^{r-1}; \\ -2^{r-1}, & \text{se } mdc(k, 2^r) = 2^{r-1}; \\ 2^{r-1}, & \text{se } mdc(k, 2^r) > 2^{r-1}. \end{cases}$$

Demonstração: Pela transitividade da forma traço, temos que

$$\text{Tr}_{\mathbb{L}|\mathbb{Q}}(\zeta^k) + \text{Tr}_{\mathbb{L}|\mathbb{Q}}(\zeta^{-k}) = \text{Tr}_{\mathbb{L}|\mathbb{Q}}(\zeta^k + \zeta^{-k}) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\text{Tr}_{\mathbb{L}|\mathbb{K}}(\zeta^k + \zeta^{-k})) = 2\text{Tr}_{\mathbb{K}|\mathbb{Q}}(\zeta^k + \zeta^{-k}).$$

Desta forma, se:

- $\text{mdc}(k, 2^r) < 2^{r-1}$, então $\text{Tr}_{\mathbb{L}|\mathbb{Q}}(\zeta^k) + \text{Tr}_{\mathbb{L}|\mathbb{Q}}(\zeta^{-k}) = 0$, isto é, $\text{Tr}_{\mathbb{K}|\mathbb{Q}}(\zeta^k + \zeta^{-k}) = 0$.
- $\text{mdc}(k, 2^r) = 2^{r-1}$, então $\text{Tr}_{\mathbb{L}|\mathbb{Q}}(\zeta^k) + \text{Tr}_{\mathbb{L}|\mathbb{Q}}(\zeta^{-k}) = -2^{r-1} - 2^{r-1} = 2(-2^{r-1})$, isto é, $\text{Tr}_{\mathbb{K}|\mathbb{Q}}(\zeta^k + \zeta^{-k}) = -2^{r-1}$.
- $\text{mdc}(k, 2^r) > 2^{r-1}$, então $\text{Tr}_{\mathbb{L}|\mathbb{Q}}(\zeta^k) + \text{Tr}_{\mathbb{L}|\mathbb{Q}}(\zeta^{-k}) = 2^{r-1} + 2^{r-1} = 2(2^{r-1})$, isto é, $\text{Tr}_{\mathbb{K}|\mathbb{Q}}(\zeta^k + \zeta^{-k}) = 2^{r-1}$,

o que prova o corolário. ■

Teorema 8.2.1 *Sejam $e_0 = 1$ e $e_i = \zeta^i + \zeta^{-i}$, para $i = 1, 2, \dots, n-1$, e $b_\alpha : \mathcal{O}_{\mathbb{K}} \times \mathcal{O}_{\mathbb{K}} \rightarrow \mathbb{Z}$ tal que $b_\alpha(x, y) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha xy)$. Tem-se que:*

1. Se $i = 0, 1, \dots, n-1$, então $b_\alpha(e_i, e_i) = \begin{cases} 2n, & \text{se } i = 0; \\ 4n, & \text{se } i \neq 0. \end{cases}$
2. Se $i \neq 0$, então $b_\alpha(e_i, e_0) = \begin{cases} -2n, & \text{se } i = 1; \\ 0, & \text{se } i \neq 1. \end{cases}$
3. Se $i \neq 0, j \neq 0$ e $i \neq j$, então $b_\alpha(e_i, e_j) = \begin{cases} -2n, & \text{se } |i - j| = 1; \\ 0, & \text{caso contrário.} \end{cases}$

Demonstração: Vamos calcular $b_\alpha(e_i, e_0)$, para $i = 0, 1, \dots, n-1$. Para $i = 0$, temos que

$$b_\alpha(e_0, e_0) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha e_0^2) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}(2) - \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\zeta + \zeta^{-1}) = 2(2^{r-2}) = 2^{r-1},$$

pois, pelo Corolário (8.2.1), temos que $\text{mdc}(1, 2^r) < 2^{r-1}$. Agora, para todo $i = 1, \dots, n-1$, temos que

$$\begin{aligned} b_\alpha(e_i, e_0) &= \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha e_i) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}((2 - (\zeta + \zeta^{-1}))(\zeta^i + \zeta^{-i})) \\ &= \text{Tr}_{\mathbb{K}|\mathbb{Q}}(2\zeta^i + 2\zeta^{-i} - \zeta^{i+1} - \zeta^{1-i} - \zeta^{i-1} - \zeta^{-1-i}) \\ &= 2\text{Tr}_{\mathbb{K}|\mathbb{Q}}(\zeta^i + \zeta^{-i}) - \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\zeta^{i+1} + \zeta^{-(i+1)}) - \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\zeta^{i-1} + \zeta^{-(i-1)}) \end{aligned}$$

$$= \begin{cases} -2n, & \text{se } i = 1 \\ 0, & \text{caso contrário.} \end{cases}$$

Vamos calcular $b_\alpha(e_i, e_i)$, para $i = 1, \dots, n-1$. Como $\text{mdc}(2i, 2^r), \text{mdc}(2i+1, 2^r), \text{mdc}(2i-1, 2^r) < 2^{r-1}$, para todo $i = 1, \dots, n-1$, segue que

$$\begin{aligned} b_\alpha(e_i, e_i) &= \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha e_i^2) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}((2 - \zeta + \zeta^{-1})(\zeta^{2i} + \zeta^{-2i} + 2)) \\ &= 2\text{Tr}_{\mathbb{K}|\mathbb{Q}}(\zeta^{2i} + \zeta^{-2i}) + \text{Tr}_{\mathbb{K}|\mathbb{Q}}(4) - \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\zeta^{2i+1} + \zeta^{-(2i+1)}) \\ &\quad - \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\zeta^{2i-1} + \zeta^{-(2i-1)}) \\ &= 4n. \end{aligned}$$

Finalmente, para todo $i \neq 0, j \neq 0$ e $i \neq j$, como $\text{mdc}(i+j, 2^r), \text{mdc}(i-j, 2^r), \text{mdc}(i+j+1, 2^r), \text{mdc}(i+j-1, 2^r) < 2^{r-1}$, segue que

$$\begin{aligned} b_\alpha(e_i, e_j) &= \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha e_i e_j) = \text{Tr}_{\mathbb{K}|\mathbb{Q}}((2 - (\zeta + \zeta^{-1}))(\zeta^i + \zeta^{-i})(\zeta^j + \zeta^{-j})) \\ &= 2\text{Tr}_{\mathbb{K}|\mathbb{Q}}(\zeta^{i+j} + \zeta^{-(i+j)}) + 2\text{Tr}_{\mathbb{K}|\mathbb{Q}}(\zeta^{i-j} + \zeta^{-(i-j)}) - \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\zeta^{i+j+1} + \zeta^{-(i+j+1)}) \\ &\quad - \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\zeta^{i-j+1} + \zeta^{-(i-j+1)}) - \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\zeta^{-i+j+1} + \zeta^{-(-i+j+1)}) - \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\zeta^{i+j-1} + \zeta^{-(i+j-1)}) \\ &= \begin{cases} -2n, & \text{se } |i-j| = 1 \\ 0, & \text{caso contrário,} \end{cases} \end{aligned}$$

o que prova o teorema. ■

Corolário 8.2.2 *Se $Q_\alpha(x, y) = \frac{1}{2^{r-1}} \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha xy)$, então a matriz de Q_α na base $\{e_0, e_1, \dots, e_{n-1}\}$ é*

$$G = \begin{pmatrix} 1 & -1 & 0 & \cdots & & & & & \\ -1 & 2 & -1 & 0 & \cdots & & & & \\ 0 & -1 & 2 & \cdots & & & & & \\ & & & & \vdots & & & & \\ & & & & & 2 & -1 & 0 & \\ & & & & & \vdots & -1 & 2 & -1 \\ & & & & & \vdots & 0 & -1 & 2 \end{pmatrix}.$$

Demonstração: Segue diretamente da Proposição (8.2.1). ■

Proposição 8.2.3 *Seja $\{f_0, f_1, \dots, f_{n-1}\}$, onde $f_i = -\sum_{j=0}^{n-1-i} e_j, \forall i = 0, 1, \dots, n-1$. Temos que $\frac{1}{2^{r-1}} \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha f_i f_j) = \delta_{ij}$, onde δ_{ij} é o delta de Kronecker.*

Demonstração: Sejam G a matriz do Corolário (8.2.2) e

$$T = \begin{pmatrix} -1 & -1 & \cdots & -1 & -1 \\ -1 & -1 & \cdots & -1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -1 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Temos que $TGT^t = I_n$. Agora, como G é a matriz de Gram do reticulado $(\mathcal{O}_{\mathbb{K}}, \frac{1}{2^{r-1}}b_\alpha)$, temos que $G = MM^t$, onde $M = \frac{1}{\sqrt{2^{r-1}}}NA$, com

$$N = \begin{pmatrix} \sigma_1(e_0) & \cdots & \sigma_n(e_0) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_{n-1}) & \cdots & \sigma_n(e_{n-1}) \end{pmatrix} \text{ e } A = \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sqrt{\sigma_n(\alpha)} \end{pmatrix}.$$

Assim, $I_n = TMM^tT^t = (TM)(TM)^t$. Seja agora $f_i = -\sum_{j=0}^{n-1-i} e_j$; $j = 0, 1, \dots, n-1$, uma outra base de $\mathcal{O}_{\mathbb{K}}$. Temos que

$$\begin{pmatrix} \sigma_1(f_0) & \cdots & \sigma_n(f_0) \\ \vdots & \ddots & \vdots \\ \sigma_1(f_{n-1}) & \cdots & \sigma_n(f_{n-1}) \end{pmatrix} = \begin{pmatrix} -1 & -1 & \cdots & -1 & -1 \\ -1 & -1 & \cdots & -1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -1 & 0 & \cdots & 0 & 0 \end{pmatrix} \begin{pmatrix} \sigma_1(e_0) & \cdots & \sigma_n(e_0) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_{n-1}) & \cdots & \sigma_n(e_{n-1}) \end{pmatrix}.$$

Logo, $\overline{M} = \frac{1}{\sqrt{2^{r-1}}}TNA$ é uma matriz geradora do reticulado $(\mathcal{O}_{\mathbb{K}}, \frac{1}{2^{r-1}}b_\alpha)$. Como $\overline{M}\overline{M}^t = \frac{1}{p}TNAA^tN^tT^t = TMM^tT^t = I_n$, segue que $\frac{1}{p}Tr_{\mathbb{K}|\mathbb{Q}}(\alpha\overline{e}_i\overline{e}_j) = \delta_{ij}$, onde δ_{ij} é o delta de Kronecker. ■

Segue da Proposição (8.2.3) que o reticulado ideal $\Lambda = (\mathcal{O}_{\mathbb{K}}, \frac{1}{2^{r-1}}b_\alpha)$, com $\alpha = (1-\zeta)(1-\zeta^{-1})$ é isomorfo ao reticulado \mathbb{Z}^n . Se tomarmos M como matriz geradora de tal reticulado, onde

$$M = \frac{1}{\sqrt{2^{r-1}}}TNA, \text{ onde}$$

$$N = \begin{pmatrix} \sigma_1(e_0) & \cdots & \sigma_n(e_0) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_{n-1}) & \cdots & \sigma_n(e_{n-1}) \end{pmatrix}, \quad T = \begin{pmatrix} -1 & -1 & \cdots & -1 & -1 \\ -1 & -1 & \cdots & -1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -1 & 0 & \cdots & 0 & 0 \end{pmatrix} \text{ e}$$

$$A = \text{diag}(\sqrt{\sigma_k(\alpha)}),$$

temos que $G = MM^t = I_n$.

Seguindo os passos desse algoritmo, pode-se construir \mathbb{Z}^n -reticulados rotacionados para $n = 2, 4, 8, 16, 32, 64, 128, 256, 512, \dots$.

Proposição 8.2.4 *Se Λ é um reticulado de dimensão 2^{r-2} , então $d_{p,\min}(\Lambda) = \frac{1}{\sqrt{2^\beta}}$, onde $\beta = (r-1)2^{r-2} - 1$.*

Demonstração: Pelo Corolário (7.1.1), temos que a distância produto mínima de Λ é dada por $\frac{1}{\sqrt{|Disc(\mathbb{K}|\mathbb{Q})|}}$, uma vez que $\det(\Lambda) = 1$. Como o discriminante de \mathbb{K} satisfaz $|Disc(\mathbb{K}|\mathbb{Q})| = 2^\beta$, onde $\beta = (r-1)2^r - 1$, segue que $d_{p,\min}(\Lambda) = \frac{1}{\sqrt{2^\beta}}$. ■

A tabela a seguir fornece a $d_{p,\min}$ para a construção ciclotômica em algumas dimensões.

r	n	$\sqrt[n]{d_{p,\min}}$
3	2	0,594604
4	4	0,385553
5	8	0,261068
6	16	0,180648
7	32	0,126361
8	64	0,0888683
9	128	0,0626695
10	256	0,044254
11	512	0,0312712
12	1024	0,0221046

Exemplo 8.2.1 *Sejam $n = 2^3$, $\zeta = \zeta_{2^3}$, $\mathbb{L} = \mathbb{Q}(\zeta)$ e $\mathbb{K} = \mathbb{Q}(\zeta + \zeta^{-1})$. Temos que uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}}$ é $\{e_0 = 1, e_1 = \zeta + \zeta^{-1}\}$, o grupo de Galois de \mathbb{L} sobre \mathbb{Q} é dado por $\text{Gal}(\mathbb{L}|\mathbb{Q}) = \{\sigma_1, \sigma_3, \sigma_5, \sigma_7\}$, onde $\sigma_i(\zeta) = \zeta^i$, para $i = 1, 3, 5, 7$ e o grupo de Galois de \mathbb{K} sobre \mathbb{Q} é dado por*

$Gal(\mathbb{K}|\mathbb{Q}) = \{\sigma_1, \sigma_3\}$. Seja $\alpha = 2 - (\zeta + \zeta^{-1})$ e $b_\alpha(x, y) = \frac{1}{4}Tr_{\mathbb{K}|\mathbb{Q}}(\alpha xy)$. A matriz G de b_α é

$$\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}.$$

Agora, uma matriz geradora do \mathbb{Z}^n -reticulado rotacionado é dada por $M = \frac{1}{\sqrt{2^{3-1}}}TNA$, onde

$$N = \begin{pmatrix} \sigma_1(e_0) & \sigma_3(e_0) \\ \sigma_1(e_1) & \sigma_3(e_1) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \zeta + \zeta^{-1} & \zeta^3 + \zeta^{-3} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \sqrt{2} & -\sqrt{2} \end{pmatrix},$$

$$T = \begin{pmatrix} -1 & -1 \\ -1 & 0 \end{pmatrix} e$$

$$A = \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & 0 \\ 0 & \sqrt{\sigma_3(\alpha)} \end{pmatrix} = \begin{pmatrix} \sqrt{2 - \sqrt{2}} & 0 \\ 0 & \sqrt{2 + \sqrt{2}} \end{pmatrix}.$$

Logo, temos que

$$M = \frac{1}{\sqrt{2^2}}TNA = \frac{1}{2} \begin{pmatrix} (-1 - \sqrt{2})\sqrt{2 - \sqrt{2}} & (-1 + \sqrt{2})\sqrt{2 + \sqrt{2}} \\ -\sqrt{2 - \sqrt{2}} & -\sqrt{2 + \sqrt{2}} \end{pmatrix}.$$

Notemos que $MM^t = I_n$.

Capítulo 9

Identificação de certos reticulados com reticulados ideais

Dado um reticulado no \mathbb{R}^n podemos vê-lo como um $\mathcal{O}_{\mathbb{K}}$ -reticulado para algum corpo de números \mathbb{K} ? Motivados por esta questão, neste capítulo apresentamos alguns reticulados ideais que podem ser identificados com os reticulados A_{p-1} , p primo, D_4 , E_6 , E_8 , K_{12} e Λ_{24} , que são conhecidos na literatura. Na Seção 9.1, apresentamos alguns resultados que serão utilizados na construção de tais reticulados ideais, o principal resultado utilizado relaciona o determinante do reticulado com a fatoração do diferente da extensão. Na Seção 9.2, apresentamos o reticulado A_{p-1} , com p primo e via o corpo ciclotômico $\mathbb{Q}(\zeta_p)$, com p primo apresentamos um reticulado ideal que apresenta as mesmas propriedades que o reticulado A_{p-1} , com p primo. Na Seção 9.3, apresentamos o reticulado D_4 e via o corpo ciclotômico $\mathbb{Q}(\zeta_8)$, apresentamos um reticulado ideal que apresenta as mesmas propriedades que o reticulado D_4 . Na Seção 9.4, apresentamos o reticulado E_8 e, via os corpos ciclotômicos $\mathbb{Q}(\zeta_{24})$, $\mathbb{Q}(\zeta_{20})$ e $\mathbb{Q}(\zeta_{15})$, apresentamos reticulados ideais isomorfos ao reticulado E_8 . Na Seção 9.5, apresentamos o reticulado E_6 e, via o corpo ciclotômico $\mathbb{Q}(\zeta_9)$, apresentamos um reticulado ideal que apresenta as mesmas propriedades que o reticulado E_6 . Na Seção 9.6, apresentamos o reticulado K_{12} e, via o corpo ciclotômico $\mathbb{Q}(\zeta_{21})$, apresentamos um reticulado ideal que apresenta as mesmas propriedades que o reticulado K_{12} . Por fim, na Seção 9.7, apresentamos o reticulado Λ_{24} e, via os corpos ciclotômicos $\mathbb{Q}(\zeta_{39})$ e $\mathbb{Q}(\zeta_{35})$, apresentamos reticulados ideais isomorfos ao reticulado Λ_{24} .

9.1 Construção

Nesta seção, veremos alguns resultados que serão utilizados para construir reticulados ideais do tipo traço com certo determinante d . O principal resultado relaciona a fatoração do diferente

de uma extensão como um produto de ideais primos. Visto que os corpos utilizados em nossa construção serão os corpos ciclotômicos, faremos um roteiro de como fatorar o diferente de uma extensão ciclotômica em um produto de ideais primos.

Sejam \mathbb{K} um corpo de números de grau n , $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de \mathbb{K} sobre \mathbb{Z} , $\bar{\cdot} : \mathbb{K} \rightarrow \mathbb{K}$ a conjugação complexa e \mathbb{F} o corpo fixo por $\bar{\cdot}$.

A próxima proposição nos diz quando é possível construir um reticulado ideal do tipo traço com certo determinante d .

Proposição 9.1.1 *Se \mathbb{K} é um corpo de números tal que \mathbb{K} é totalmente real ou \mathbb{K} é uma extensão totalmente imaginária de \mathbb{F} , de grau 2, então existe um $\mathcal{O}_{\mathbb{K}}$ -reticulado do tipo traço com determinante d se, e somente se, existem ideais I, J de $\mathcal{O}_{\mathbb{K}}$ tal que $N(J) = d$ e $\Delta(\mathbb{K}|\mathbb{Q}) = JI\bar{I}$.*

Demonstração: Suponha que existem I, J ideais de $\mathcal{O}_{\mathbb{K}}$ tal que $N(J) = d$ e $\Delta(\mathbb{K}|\mathbb{Q}) = JI\bar{I}$. Temos que $\Delta(\mathbb{K}|\mathbb{Q}) = JI\bar{I} \subseteq I\bar{I}$. Assim, $\Delta(\mathbb{K}|\mathbb{Q})^{-1}\Delta(\mathbb{K}|\mathbb{Q}) \subseteq \Delta(\mathbb{K}|\mathbb{Q})^{-1}I\bar{I}$. Assim, $\mathcal{O}_{\mathbb{K}} \subseteq \Delta(\mathbb{K}|\mathbb{Q})^{-1}I\bar{I}$, o que implica que $\mathcal{O}_{\mathbb{K}} \subseteq J^{-1}I^{-1}\bar{I}^{-1}I\bar{I} = J^{-1}$. Desta forma, $I^{-1}\bar{I}^{-1}\mathcal{O}_{\mathbb{K}} \subseteq I^{-1}\bar{I}^{-1}J^{-1} = \Delta(\mathbb{K}|\mathbb{Q})^{-1}$. Logo, $I^{-1}\bar{I}^{-1} \subseteq I^{-1}\bar{I}^{-1}\mathcal{O}_{\mathbb{K}} \subseteq \Delta(\mathbb{K}|\mathbb{Q})^{-1}$, pois $1 \in \mathcal{O}_{\mathbb{K}}$. Consideremos a aplicação:

$$b : I^{-1} \times I^{-1} \longrightarrow \mathbb{Z}$$

$$(x, y) \longmapsto \text{Tr}_{\mathbb{K}|\mathbb{Q}}(xy).$$

Como $I^{-1}\bar{I}^{-1} \subseteq \Delta(\mathbb{K}|\mathbb{Q})^{-1}$, temos que b está bem definida. Logo, (I^{-1}, b) é um $\mathcal{O}_{\mathbb{K}}$ -reticulado. Além disso, pelo Teorema (7.1.1), temos que

$$\det(b) = N(I^{-1})^2 |\text{Disc}(\mathbb{K}|\mathbb{Q})|.$$

Agora, como $|\text{Disc}(\mathbb{K}|\mathbb{Q})| = N(\Delta(\mathbb{K}|\mathbb{Q}))$, segue que $\det(b) = N(I^{-1})^2 N(I)N(\bar{I})N(J)$. Como $N(I) = N(\bar{I})$ e $N(I^{-1}) = N(I)^{-1}$, segue que

$$\det(b) = N(I)^{-2} N(I)^2 N(J) = N(J) = d.$$

Portanto, existe um $\mathcal{O}_{\mathbb{K}}$ -reticulado do tipo traço com determinante d . Reciprocamente, suponha que existe um $\mathcal{O}_{\mathbb{K}}$ -reticulado do tipo traço com determinante d . Desta forma, existe I um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$ tal que (I, b) é um reticulado ideal com determinante d , onde

$$b : I \times I \longrightarrow \mathbb{Z}$$

$$(x, y) \longmapsto \text{Tr}_{\mathbb{K}|\mathbb{Q}}(x\bar{y}).$$

Temos que, $I\bar{I} \subset \Delta(\mathbb{K}|\mathbb{Q})^{-1}$. Assim, segue que $\Delta(\mathbb{K}|\mathbb{Q})^{-1} = I\bar{I}M$, onde M é um ideal de $\mathcal{O}_{\mathbb{K}}$ e $\Delta(\mathbb{K}|\mathbb{Q}) = I^{-1}\bar{I}^{-1}M^{-1}$. Agora, temos que $d = \det(b) = N(I)^2|\text{Disc}(\mathbb{K}|\mathbb{Q})| = N(I)^2N(\Delta(\mathbb{K}|\mathbb{Q})) = N(I)^2N(I)^{-2}N(M)^{-1}$. Logo, temos que $N(M^{-1}) = d$, como queríamos. ■

Corolário 9.1.1 *Nas mesmas condições da Proposição (9.1.1), tem-se que existe um $\mathcal{O}_{\mathbb{K}}$ -reticulado unimodular do tipo traço se, e somente se, existe um ideal I de $\mathcal{O}_{\mathbb{K}}$ tal que $\Delta(\mathbb{K}|\mathbb{Q}) = I\bar{I}$.*

Demonstração: Segue diretamente da Proposição (9.1.1). ■

No que segue, iremos trabalhar com corpos ciclotômicos.

Baseados na Proposição (9.1.1), dado um certo corpo ciclotômico $\mathbb{Q}(\zeta_n)$, primeiramente iremos fatorar seu diferente e verificar se é possível construir um $\mathcal{O}_{\mathbb{K}}$ -reticulado do tipo traço com certo determinante d .

Como iremos estudar reticulados ideais que apresentam as mesmas propriedades que os reticulados A_{p-1} , p primo, D_4 , E_6 , E_8 , K_{12} e Λ_{24} , iremos trabalhar com corpos ciclotômicos cujo grau da extensão seja o mesmo da dimensão de tais reticulados.

A seguir, faremos um roteiro de como fatorar o diferente de um dado corpo ciclotômico em um produto de ideais primos do anel de inteiros $\mathcal{O}_{\mathbb{K}}$. Notemos que a Proposição (9.1.1) não exige que o diferente esteja fatorado como um produto de ideais primos, mas visto que todo ideal se fatora de forma única como um produto de ideais primos, basta considerar os ideais I , J da Proposição (9.1.1) como produto destes ideais primos.

Seja $\mathbb{Q}(\zeta_n)$ o n -ésimo corpo ciclotômico. Pelo Corolário (4.4.1), temos que aparecem na fatoração do diferente $\Delta(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ somente os ideais primos de $\mathbb{Z}[\zeta_n]$ que estão acima dos ideais primos p de \mathbb{Z} tal que p é primo e $p|n$. Desta forma, fazemos o seguinte:

- Dado n , encontramos todos os primos p_i 's que dividem n .
- Para cada um destes primos p_i utilizamos o Teorema de Kummer (4.1.3) e encontramos a fatoração do ideal estendido $p_i\mathbb{Z}[\zeta_n]$ como produto de ideais primos.

Com isto, encontramos todos os ideais primos de $\mathbb{Z}[\zeta_n]$ que dividem o diferente. Resta saber qual o índice de cada um. Para isto, utilizamos os seguintes resultados:

- Pela Proposição (4.3.1), temos que se um ideal primo P de $\mathbb{Z}[\zeta_n]$ aparece na fatoração do ideal estendido $p\mathbb{Z}[\zeta_n]$, p primo e $p|n$, com índice e , então P divide o diferente com índice s tal que $s \geq e - 1$.

- Pelo Teorema (3.2.1), temos que $N(\Delta(\mathbb{Q}(\zeta_n)|\mathbb{Q})) = |\text{Disc}(\mathbb{Q}(\zeta_n)|\mathbb{Q})|$ e, pelo Teorema (3.2.3), temos que $|\text{Disc}(\mathbb{Q}(\zeta_n)|\mathbb{Q})| = \frac{n^{\varphi(n)}}{\prod_{j=1}^r p_j^{\frac{\varphi(n)}{p_j-1}}}$, onde $n = \prod_{j=1}^r p_j^{a_j}$.

Após fatorar o diferente vemos se é possível escrevê-lo como $\Delta(\mathbb{Q}(\zeta_n)|\mathbb{Q}) = I\bar{I}J$. Para isto, utilizamos o Corolário (4.4.4). Para todo primo p tal que $p|n$, após ter fatorado o ideal $p\mathbb{Z}[\zeta_n]$, fatoramos n como $n = p^k t$, $k \geq 1$ e $p \nmid t$. Em seguida, calculamos $O_t(p)$ (ordem de p em \mathbb{Z}_t^*). Se $O_t(p) \equiv 1 \pmod{2}$, então para todo ideal primo P de $\mathbb{Z}[\zeta_n]$ que está acima de p , \bar{P} também está acima de p e $\bar{P} \neq P$.

Para a próxima proposição omitimos a demonstração por faltarem pré-requisitos suficientes para prová-la neste trabalho.

Proposição 9.1.2 ([16], pag. 76) *Se $\mathbb{K} = \mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n -ésima primitiva da unidade, onde n é livre de quadrados, $n \neq p$, $n \neq 2p$, p primo e $\varphi(n) \geq 8$, então a norma mínima de todo $\mathcal{O}_{\mathbb{K}}$ -reticulado é no mínimo 4.* ■

9.2 O reticulado A_{p-1} , p primo

Nesta seção, definiremos o reticulado A_{p-1} , com p primo e apresentaremos um reticulado ideal $(p-1)$ -dimensional, par e com o mesmo determinante que A_{p-1} , com p primo.

Definição 9.2.1 *Seja p um número primo. O reticulado A_{p-1} é um reticulado par, $(p-1)$ -dimensional, definido por*

$$A_{p-1} = \{(x_0, x_1, \dots, x_{p-1}) \in \mathbb{Z}^p \text{ tal que } x_0 + \dots + x_{p-1} = 0\}.$$

Sua densidade de centro é $\Delta = 2^{\frac{-(p-1)}{2}} p^{\frac{-1}{2}}$, sua norma mínima é 2 e seu determinante é p .

Sejam p um número primo ímpar e $\mathbb{K} = \mathbb{Q}(\zeta_p)$ o p -ésimo corpo ciclotômico. Temos que $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \varphi(p) = p-1$. Vamos fatorar o diferente $\Delta(\mathbb{Q}(\zeta_p)|\mathbb{Q})$.

- Como p é um número primo segue, pela Proposição (4.4.1), que o ideal gerado por p é o único ideal primo de \mathbb{Z} que se ramifica em $\mathbb{Z}[\zeta_p]$.
- Como $\phi_p(x) = x^{p-1} + \dots + x + 1 = \min_{\mathbb{Q}} \zeta_p$, segue que $\bar{\phi}_p(x) = x^{p-1} + \dots + x + \bar{1} = (x - \bar{1})^{p-1} \pmod{\mathbb{Z}_p[x]}$. Pelo Teorema de Kummer (4.1.3), segue que

$$p\mathbb{Z}[\zeta_p] = P^{p-1}, \text{ onde } P = \langle p, \zeta_p - 1 \rangle.$$

Assim, o único ideal primo de $\mathbb{Z}[\zeta_p]$ que se ramifica é P , o que implica que P é o único ideal primo de $\mathbb{Z}[\zeta_p]$ que divide o diferente $\Delta(\mathbb{Q}(\zeta_p)|\mathbb{Q})$. Logo, $\Delta(\mathbb{Q}(\zeta_p)|\mathbb{Q}) = P^k$, $k \geq 1$.

- Como $p^{p-1} = |N_{\mathbb{K}|\mathbb{Q}}(p)| = N(p\mathbb{Z}[\zeta_p]) = N(P)^{p-1}$, então $N(P) = p$ e como $N(\Delta(\mathbb{Q}(\zeta_p)|\mathbb{Q})) = |\text{Disc}(\mathbb{Q}(\zeta_p)|\mathbb{Q})| = p^{p-2}$, segue que $N(P)^k = p^{p-2}$, o que implica que $k = p - 2$. Desta forma, temos que

$$\Delta(\mathbb{Q}(\zeta_p)|\mathbb{Q}) = P^{p-2}.$$

- Como o ideal \bar{P} deve aparecer na fatoração de $p\mathbb{Z}[\zeta_p]$ e como $p\mathbb{Z}[\zeta_p] = P^{p-1}$, segue que $\bar{P} = P$. Assim, podemos escrever

$$\Delta(\mathbb{Q}(\zeta_p)|\mathbb{Q}) = P^{\frac{p-3}{2}} \bar{P}^{\frac{p-3}{2}} P.$$

Como o diferente se fatora desta forma, pela Proposição (9.1.1) temos que existe um $\mathcal{O}_{\mathbb{K}}$ -reticulado do tipo traço com determinante $N(P) = p$. Consideremos a aplicação:

$$\begin{aligned} b : P^{-(\frac{p-3}{2})} \times P^{-(\frac{p-3}{2})} &\longrightarrow \mathbb{Z} \\ (x, y) &\longmapsto \text{Tr}_{\mathbb{K}|\mathbb{Q}}(x\bar{y}). \end{aligned}$$

Temos, pela demonstração da Proposição (9.1.1), que $\det(b) = N(P) = p$. Agora, pelo Exemplo (7.1.5), temos que b é par. Portanto, segue que $(P^{-(\frac{p-3}{2})}, b)$ é um $\mathcal{O}_{\mathbb{K}}$ -reticulado par com determinante p . Desta forma, temos que $(P^{-(\frac{p-3}{2})}, b)$ apresenta as mesmas propriedades que o reticulado A_{p-1} .

9.3 O reticulado D_4

Nesta seção, definiremos o reticulado D_4 e apresentaremos um reticulado ideal 4-dimensional, par e com o mesmo determinante que D_4 .

Definição 9.3.1 *O reticulado D_4 é um reticulado par, 4-dimensional, definido por:*

$$D_4 = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 \text{ tal que } x_i \in \mathbb{Z}, \forall i \text{ e } \sum_{i=1}^4 x_i = 2m; m \in \mathbb{Z}\}.$$

Sua densidade de centro é $\Delta = \frac{\pi^2}{16} = 0,6169$ e é a maior densidade possível para dimensão 4. Sua norma mínima é 2 e seu determinante é 4.

Seja $\mathbb{K} = \mathbb{Q}(\zeta_8)$ o corpo ciclotômico associado a raiz oitava primitiva da unidade. Temos que $[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = \varphi(8) = 4$. Vamos fatorar o diferente $\Delta(\mathbb{Q}(\zeta_8)|\mathbb{Q})$.

- Temos que 2 é o único primo que divide 8 e, assim, pela Proposição (4.4.1), o ideal gerado por 2 é o único ideal primo de \mathbb{Z} que se ramifica em $\mathbb{Z}[\zeta_8]$.
- Como $\phi_8(x) = x^4 + 1 = \min_{\mathbb{Q}} \zeta_8$ então $\bar{\phi}_8(x) = x^4 + \bar{1} = (x - \bar{1})^4 \pmod{\mathbb{Z}_2[x]}$. Pelo Teorema de Kummer (4.1.3), temos que

$$2\mathbb{Z}[\zeta_8] = P^4, \text{ onde } P = \langle 2, \zeta_8 - 1 \rangle.$$

Assim, o único ideal primo de $\mathbb{Z}[\zeta_8]$ que divide o diferente $\Delta(\mathbb{Q}(\zeta_8)|\mathbb{Q})$ é P , pois P é o único ideal primo de $\mathbb{Z}[\zeta_8]$ que se ramifica. Logo $\Delta(\mathbb{Q}(\zeta_8)|\mathbb{Q}) = P^k$, $k \geq 1$.

- Como $2^4 = |N_{\mathbb{K}|\mathbb{Q}}(2)| = N(P)^4$, segue que $N(P) = 2$. Agora, pelo Teorema (3.2.1), temos que $N(\Delta(\mathbb{Q}(\zeta_8)|\mathbb{Q})) = |\text{Disc}(\mathbb{Q}(\zeta_8)|\mathbb{Q})| = 2^8$. Desta forma, $k = 8$ e, assim,

$$\Delta(\mathbb{Q}(\zeta_8)|\mathbb{Q}) = P^8.$$

- Notemos ainda que como o ideal \bar{P} deve aparecer na fatoração de $2\mathbb{Z}[\zeta_8]$ e como $2\mathbb{Z}[\zeta_8] = P^4$, segue que $\bar{P} = P$. Assim, podemos escrever

$$\Delta(\mathbb{Q}(\zeta_8)|\mathbb{Q}) = P^3 \bar{P}^3 P^2.$$

Como o diferente se fatora desta forma, pela Proposição (9.1.1), temos que existe um $\mathcal{O}_{\mathbb{K}}$ -reticulado do tipo traço com determinante $N(P^2) = 4$. Consideremos a aplicação:

$$b : P^{-3} \times P^{-3} \longrightarrow \mathbb{Z}$$

$$(x, y) \longmapsto \text{Tr}_{\mathbb{K}|\mathbb{Q}}(x\bar{y}).$$

De forma análoga ao que fizemos no Exemplo (7.1.6), mostramos que b é par. Agora, segue da demonstração da Proposição (9.1.1) que $\det(b) = N(P)^2 = 4$. Portanto, temos que (P^{-3}, b) é um $\mathcal{O}_{\mathbb{K}}$ -reticulado par com determinante 4. Desta forma, temos que (P^{-3}, b) apresenta as mesmas propriedades que o reticulado D_4 .

9.4 O reticulado E_8

Nesta seção, definiremos o reticulado E_8 e veremos três reticulados ideais que são isomorfos ao reticulado E_8 .

Definição 9.4.1 *O reticulado E_8 é um reticulado par, 8-dimensional, definido por:*

$$E_8 = \{(x_1, x_2, \dots, x_8) \text{ tal que } x_i \in \mathbb{Z} \text{ ou } x_i \in \mathbb{Z} + \frac{1}{2}, \forall i \text{ e } \sum x_i \equiv 0 \pmod{2}\}.$$

Sua densidade de centro é $\Delta = 0,2537$, sua norma mínima é 2 e seu determinante é 1.

9.4.1 E_8 via $\mathbb{Q}(\zeta_{24})$

Seja $\mathbb{K} = \mathbb{Q}(\zeta_{24})$ o 24-ésimo corpo ciclotômico. Temos que $[\mathbb{Q}(\zeta_{24}) : \mathbb{Q}] = \varphi(24) = 8$. Vamos fatorar o diferente $\Delta(\mathbb{Q}(\zeta_{24})|\mathbb{Q})$.

- Como 2 e 3 são os únicos primos que dividem 24 segue, pela Proposição (4.4.1), que os ideais gerados por 2 e 3, respectivamente, são os únicos ideais primos de \mathbb{Z} que se ramificam em $\mathbb{Z}[\zeta_{24}]$.
- Como $\phi_{24}(x) = x^8 - x^4 + 1 = \min_{\mathbb{Q}} \zeta_{24}$, segue que $\bar{\phi}_{24}(x) = (\bar{1} + x + x^2)^4 \pmod{\mathbb{Z}_2[x]}$ e $\bar{\phi}_{24}(x) = (\bar{2} + x + x^2)^2(\bar{2} + \bar{2}x + x^2)^2 \pmod{\mathbb{Z}_3[x]}$. Assim, pelo Teorema de Kummer (4.1.3), temos que

$$2\mathbb{Z}[\zeta_{24}] = Q^4, \text{ onde } Q = \langle 2, 1 + \zeta_{24} + \zeta_{24}^2 \rangle \text{ e}$$

$$3\mathbb{Z}[\zeta_{24}] = S^2 R^2, \text{ onde } S = \langle 3, 2 + \zeta_{24} + \zeta_{24}^2 \rangle \text{ e } R = \langle 3, 2 + 2\zeta_{24} + \zeta_{24}^2 \rangle.$$

Desta forma, os únicos ideais primos de $\mathbb{Z}[\zeta_{24}]$ que se ramificam são Q , S e R e, assim, são os únicos ideais primos de $\mathbb{Z}[\zeta_{24}]$ que dividem o diferente $\Delta(\mathbb{Q}(\zeta_{24})|\mathbb{Q})$. Logo, temos que $\Delta(\mathbb{Q}(\zeta_{24})|\mathbb{Q}) = Q^q R^r S^s$; $q, r, s \geq 1$.

- Agora, como $2^8 = |N_{\mathbb{K}|\mathbb{Q}}(2)| = N(Q)^4$, segue que $N(Q) = 4$. Além disso, pelo Exemplo (4.4.4), temos que $\bar{R} = S$, o que implica que $N(R) = N(S)$. Como $3^8 = |N_{\mathbb{K}|\mathbb{Q}}(3)| = N(R)^2 N(S)^2 = N(R)^4$, segue que $N(R) = N(S) = 3^2$. Pelo Teorema (3.2.1), temos que $N(\Delta(\mathbb{Q}(\zeta_{24})|\mathbb{Q})) = |Disc(\mathbb{Q}(\zeta_{24})|\mathbb{Q})| = 2^{16} 3^4$. Assim, segue que $2^{16} 3^4 = N(Q)^q N(R)^r N(S)^s$

$= 4^q(3^2)^r(3^2)^s = 2^{2q}3^{2(r+s)}$. Isto implica que $q = 8$ e $r + s = 2$. Assim, $q = 8$, $r = s = 1$. Portanto,

$$\Delta(\mathbb{Q}(\zeta_{24})|\mathbb{Q}) = Q^8 RS.$$

- Como $\bar{R} = S$ e $\bar{Q} = Q$, segue que

$$\Delta(\mathbb{Q}(\zeta_{24})|\mathbb{Q}) = Q^4 R \bar{Q}^4 \bar{R} = (Q^4 R) \overline{(Q^4 R)}.$$

Como o diferente se fatora desta forma, pelo Corolário (9.1.1), temos que existe um $\mathcal{O}_{\mathbb{K}}$ -reticulado unimodular do tipo traço. Seja $I = R^{-1}Q^{-4}$. Consideremos a aplicação:

$$b : I \times I \longrightarrow \mathbb{Z}$$

$$(x, y) \longmapsto \text{Tr}_{\mathbb{K}|\mathbb{Q}}(x\bar{y}).$$

Tomando $\gamma = \zeta_{24}^4 \in \mathbb{Z}[\zeta_{24}]$ temos que $\gamma + \bar{\gamma} = 1$. Assim, pela Proposição (7.1.3) temos que todo $\mathcal{O}_{\mathbb{K}}$ -reticulado é par. Agora, pelo Teorema (7.1.1), temos que $\det(b) = N(I)^2 |\text{Disc}(\mathbb{K}|\mathbb{Q})| = (3^{-2}4^{-4})^2 2^{16}3^4 = 1$. Portanto, segue que (I, b) é um $\mathcal{O}_{\mathbb{K}}$ -reticulado par com determinante 1. Em [13], vemos que E_8 é o único reticulado unimodular e par em sua dimensão. Desta forma, temos que (I, b) é isomorfo ao reticulado E_8 .

9.4.2 E_8 via $\mathbb{Q}(\zeta_{20})$

Seja $\mathbb{K} = \mathbb{Q}(\zeta_{20})$ o 20-ésimo corpo ciclotômico. Temos que $[\mathbb{Q}(\zeta_{20}) : \mathbb{Q}] = \varphi(20) = 8$. Vamos fatorar o diferente $\Delta(\mathbb{Q}(\zeta_{20})|\mathbb{Q})$.

- Temos que 2 e 5 são os únicos números primos que dividem 20. Logo, pela Proposição (4.4.1), temos que os ideais gerados por 2 e 5, respectivamente, são os únicos ideais primos de \mathbb{Z} que se ramificam em $\mathbb{Z}[\zeta_{20}]$.
- Como $\phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1 = \min_{\mathbb{Q}} \zeta_{20}$, segue que $\bar{\phi}_{20}(x) = (\bar{1} + x + x^2 + x^3 + x^4)^2 \pmod{\mathbb{Z}_2[x]}$ e $\bar{\phi}_{20}(x) = (\bar{2} + x)^4 (\bar{3} + t)^4 \pmod{\mathbb{Z}_5[x]}$. Assim, pelo Teorema de Kummer (4.1.3), segue que

$$2\mathbb{Z}[\zeta_{20}] = Q^2, \text{ onde } Q = \langle 2, 1 + \zeta_{20} + \zeta_{20}^2 + \zeta_{20}^3 + \zeta_{20}^4 \rangle \text{ e}$$

$$5\mathbb{Z}[\zeta_{20}] = S^4 R^4, \text{ onde } S = \langle 5, 2 + \zeta_{20} \rangle \text{ e } R = \langle 5, 3 + \zeta_{20} \rangle.$$

Assim, os únicos ideais primos de $\mathbb{Z}[\zeta_{20}]$ que se ramificam são Q , S e R , sendo estes os únicos ideais primos de $\mathbb{Z}[\zeta_{20}]$ que dividem o diferente $\Delta(\mathbb{Q}(\zeta_{20})|\mathbb{Q})$. Logo, temos que $\Delta(\mathbb{Q}(\zeta_{20})|\mathbb{Q}) = Q^q R^r S^s$, onde $q \geq 1$, $s, r \geq 3$, pela Proposição (4.3.1).

- Temos que $2^8 = |N_{\mathbb{K}|\mathbb{Q}}(2)| = N(Q)^2$ e, assim, $N(Q) = 2^4$. Agora, como $O_4(5) = 1 \equiv 1 \pmod{2}$, pelo Corolário (4.4.4), segue que $\bar{R} \neq R$. Logo, $\bar{R} = S$ e, assim, $N(R) = N(S)$. Desta forma, $5^8 = |N_{\mathbb{K}|\mathbb{Q}}(5)| = N(S)^4 N(R)^4 = N(S)^8$, o que implica que $N(R) = N(S) = 5$. Pelo Teorema (3.2.1), temos que $N(\Delta(\mathbb{Q}(\zeta_{20})|\mathbb{Q})) = |\text{Disc}(\mathbb{Q}(\zeta_{20})|\mathbb{Q})| = 2^8 5^6$. Assim, segue que $N(Q)^q N(R)^r N(S)^s = 2^8 5^6$, o que implica que $q = 2$ e $r = s = 3$. Portanto,

$$\Delta(\mathbb{Q}(\zeta_{20})|\mathbb{Q}) = Q^2 R^3 S^3.$$

- Como $\bar{R} = S$ e $\bar{Q} = Q$, podemos escrever

$$\Delta(\mathbb{Q}(\zeta_{20})|\mathbb{Q}) = Q^2 R^3 S^3 = QR^3 \overline{QR^3} = (QR^3) \overline{(QR^3)}.$$

Como o diferente se fatora desta forma, pelo Corolário (9.1.1), temos que existe um $\mathcal{O}_{\mathbb{K}}$ -reticulado unimodular do tipo traço. Seja $I = R^{-3}Q^{-1}$. Consideremos a aplicação:

$$b : I \times I \longrightarrow \mathbb{Z}$$

$$(x, y) \longmapsto \text{Tr}_{\mathbb{K}|\mathbb{Q}}(x\bar{y}).$$

Tomando $\gamma = \zeta_{20}^2 - \zeta_{20}^4 \in \mathbb{Z}[\zeta_{20}]$, temos que $\gamma + \bar{\gamma} = 1$. Assim, pela Proposição (7.1.3), temos que todo $\mathcal{O}_{\mathbb{K}}$ -reticulado é par. Agora, pelo Teorema (7.1.1), temos que $\det(b) = N(I)^2 |\text{Disc}(\mathbb{K}|\mathbb{Q})| = (5^{-3}2^{-4})^2 2^8 5^6 = 1$. Portanto, (I, b) é um $\mathcal{O}_{\mathbb{K}}$ -reticulado par com determinante 1. Em [13], vemos que E_8 é o único reticulado unimodular e par em sua dimensão. Desta forma, temos que (I, b) é isomorfo ao reticulado E_8 .

9.4.3 E_8 via $\mathbb{Q}(\zeta_{15})$

Seja $\mathbb{K} = \mathbb{Q}(\zeta_{15})$ o corpo ciclotômico associado a 15-ésima raiz primitiva da unidade. Temos que $[\mathbb{Q}(\zeta_{15}) : \mathbb{Q}] = \varphi(15) = 8$. Vamos fatorar o diferente $\Delta(\mathbb{Q}(\zeta_{15})|\mathbb{Q})$.

- Os únicos primos que dividem 15 são 3 e 5. Assim, pela Proposição (4.4.1), os ideais gerados por 3 e 5, respectivamente, são os únicos ideais primos de \mathbb{Z} que se ramificam em $\mathbb{Z}[\zeta_{15}]$.

- Como $\phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 = \min_{\mathbb{Q}} \zeta_{15}$, segue que $\bar{\phi}_{15}(x) = (\bar{1} + x + x^2 + x^3 + x^4)^2 \pmod{\mathbb{Z}_3[x]}$ e $\bar{\phi}_{15}(x) = (\bar{1} + x + x^2)^4 \pmod{\mathbb{Z}_5[x]}$. Assim, pelo Teorema de Kummer (4.1.3), temos que

$$3\mathbb{Z}[\zeta_{15}] = P^2, \text{ onde } P = \langle 3, 1 + \zeta_{15} + \zeta_{15}^2 + \zeta_{15}^3 + \zeta_{15}^4 \rangle \text{ e}$$

$$5\mathbb{Z}[\zeta_{15}] = Q^4, \text{ onde } Q = \langle 3, 1 + \zeta_{15} + \zeta_{15}^2 \rangle.$$

Desta forma, os únicos ideais primos de $\mathbb{Z}[\zeta_{15}]$ que se ramificam são P e Q e sendo, assim, os únicos ideais primos de $\mathbb{Z}[\zeta_{15}]$ que dividem o diferente $\Delta(\mathbb{Q}(\zeta_{15})|\mathbb{Q})$. Logo, temos que $\Delta(\mathbb{Q}(\zeta_{15})|\mathbb{Q}) = P^r Q^s$; $r, s \geq 1$

- Agora, temos que $3^8 = |N_{\mathbb{K}|\mathbb{Q}}(3)| = N(P)^2$ e $5^8 = |N_{\mathbb{K}|\mathbb{Q}}(5)| = N(Q)^4$, o que implica que $N(P) = 3^4$ e $N(Q) = 5^2$. Pelo Teorema (3.2.1), temos que $N(\Delta(\mathbb{Q}(\zeta_{15})|\mathbb{Q})) = |\text{Disc}(\mathbb{Q}(\zeta_{15})|\mathbb{Q})| = 3^4 5^6$. Desta forma, segue que $r = 1$ e $s = 3$. Logo,

$$\Delta(\mathbb{Q}(\zeta_{15})|\mathbb{Q}) = PQ^3 = PQ(Q\bar{Q}).$$

Como não é possível fatorar o diferente $\Delta(\mathbb{Q}(\zeta_{15})|\mathbb{Q})$ como o produto $\Delta(\mathbb{Q}(\zeta_{15})|\mathbb{Q}) = I\bar{I}$, pelo Corolário (9.1.1), temos que não existe um $\mathcal{O}_{\mathbb{K}}$ -reticulado do tipo traço com determinante 1. Entretanto, podem existir outros $\mathcal{O}_{\mathbb{K}}$ -reticulados que não sejam do tipo traço cujo determinante seja 1. Para isso, é necessário encontrar um elemento $\alpha \in \mathbb{K}$ totalmente positivo e um ideal I de $\mathcal{O}_{\mathbb{K}}$ tal que $N(I)^2 N_{\mathbb{K}|\mathbb{Q}}(\alpha) |\text{Disc}(\mathbb{K}|\mathbb{Q})| = 1$. Para facilitar os cálculos, tomemos $I = \mathcal{O}_{\mathbb{K}}$. Desta forma, precisamos encontrar um elemento $\alpha \in \mathbb{K}$ totalmente positivo tal que $N_{\mathbb{K}|\mathbb{Q}}(\alpha) = |\text{Disc}(\mathbb{K}|\mathbb{Q})|^{-1}$. Como $|\text{Disc}(\mathbb{K}|\mathbb{Q})| = N(\Delta(\mathbb{K}|\mathbb{Q}))$, precisamos encontrar em elemento $\alpha \in \mathbb{K}$ tal que $N_{\mathbb{K}|\mathbb{Q}}(\alpha) = N(\Delta(\mathbb{K}|\mathbb{Q}))^{-1} = N(\Delta(\mathbb{K}|\mathbb{Q})^{-1})$. Por [15], tomando $\alpha = \frac{1}{\psi'(\zeta + \zeta^{-1})} (\zeta + \zeta^{-1})(\zeta^7 + \zeta^{-7})$, onde ψ é o polinômio minimal de $(\zeta + \zeta^{-1})$, temos que α é totalmente positivo e gerador do $\Delta(\mathbb{K}|\mathbb{Q})^{-1}$. Logo, $N_{\mathbb{K}|\mathbb{Q}}(\alpha) = N(\Delta(\mathbb{K}|\mathbb{Q})^{-1})$. Desta forma, o reticulado ideal $(\mathcal{O}_{\mathbb{K}}, b_{\alpha})$, onde

$$b_{\alpha} : \mathcal{O}_{\mathbb{K}} \times \mathcal{O}_{\mathbb{K}} \longrightarrow \mathbb{Z}$$

$$(x, y) \longmapsto \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha x \bar{y})$$

é unimodular. Além disso, tomando $\gamma = 1 + \zeta_{15} + \zeta_{15}^4 + \zeta_{15}^5 + \zeta_{15}^6 \in \mathbb{Z}[\zeta_{15}]$, temos que $\gamma + \bar{\gamma} = 1$. Assim, pela Proposição (7.1.3), temos que todo $\mathcal{O}_{\mathbb{K}}$ -reticulado é par. Portanto, $(\mathcal{O}_{\mathbb{K}}, b_{\alpha})$ é um $\mathcal{O}_{\mathbb{K}}$ -reticulado par com determinante 1. Em [13], vemos que E_8 é o único reticulado unimodular

e par em sua dimensão. Desta forma, temos que $(\mathcal{O}_{\mathbb{K}}, b_\alpha)$ é isomorfo ao reticulado E_8 .

9.5 O reticulado E_6

Nesta seção, definiremos o reticulado E_6 e apresentaremos um reticulado ideal 6-dimensional, par e com o mesmo determinante que o reticulado E_6 .

Definição 9.5.1 *O reticulado E_6 é um reticulado par, 6-dimensional, definido por:*

$$E_6 = \{x \in E_8 \text{ tal que } x.v = 0, \forall v \in V\}.$$

Sua densidade de centro é $\Delta = \frac{\pi^3}{48\sqrt{3}} = 0,3729$, sua norma mínima é 2 e seu determinante é 3.

Seja $\mathbb{K} = \mathbb{Q}(\zeta_9)$ o 9-ésimo corpo ciclotômico. Temos que $[\mathbb{Q}(\zeta_9) : \mathbb{Q}] = \varphi(9) = 6$. Vamos fatorar o diferente $\Delta(\mathbb{Q}(\zeta_9)|\mathbb{Q})$.

- Temos que 3 é o único primo que divide 9. Logo, pela Proposição (4.4.1), temos que o ideal gerado por 3 é o único ideal primo de \mathbb{Z} que se ramifica em $\mathbb{Z}[\zeta_9]$.
- Como $\phi_9(x) = x^6 + x^3 + 1 = \min_{\mathbb{Q}} \zeta_9$, temos que $\bar{\phi}_9(x) = (\bar{2} + x)^6 \pmod{\mathbb{Z}_3[x]}$. Assim, pelo Teorema de Kummer (4.1.3), temos que

$$3\mathbb{Z}[\zeta_9] = P^6, \text{ onde } P = \langle 3, 2 + \zeta_9 \rangle.$$

Desta forma, o único ideal primo de $\mathbb{Z}[\zeta_9]$ que se ramifica é P , sendo assim, o único ideal primo de $\mathbb{Z}[\zeta_9]$ que divide o diferente $\Delta(\mathbb{Q}(\zeta_9)|\mathbb{Q})$. Temos, assim, que $\Delta(\mathbb{Q}(\zeta_9)|\mathbb{Q}) = P^r$ onde $r \geq 5$, pela Proposição (4.3.1).

- Agora, como $3^6 = |N_{\mathbb{K}|\mathbb{Q}}(3)| = N(P)^6$, segue que $N(P) = 3$. Pelo Teorema (3.2.1), temos que $N(\Delta(\mathbb{Q}(\zeta_9)|\mathbb{Q})) = |\text{Disc}(\mathbb{Q}(\zeta_9)|\mathbb{Q})| = 3^9$. Assim, segue que $r = 9$. Logo,

$$\Delta(\mathbb{Q}(\zeta_9)|\mathbb{Q}) = P^9 = P^4 \bar{P}^4 P.$$

Como o diferente se fatora desta forma, pela Proposição (9.1.1), temos que existe um $\mathcal{O}_{\mathbb{K}}$ -reticulado do tipo traço com determinante $N(P) = 3$. Seja $I = P^{-4}$. Consideremos a aplicação:

$$b : I \times I \longrightarrow \mathbb{Z}$$

$$(x, y) \longmapsto \text{Tr}_{\mathbb{K}|\mathbb{Q}}(x\bar{y}).$$

Tomando $\gamma = 1 + \zeta_9 + \zeta_9^2 + \zeta_9^3 + \zeta_9^5 \in \mathbb{Z}[\zeta_9]$, temos que $\gamma + \bar{\gamma} = 1$. Assim, pela Proposição (7.1.3), temos que todo $\mathcal{O}_{\mathbb{K}}$ -reticulado é par. Agora, pela demonstração da Proposição (9.1.1), temos que $\det(b) = N(P) = 3$. Portanto, (I, b) é um $\mathcal{O}_{\mathbb{K}}$ -reticulado par de dimensão 6 com determinante 3. Desta forma, temos que (I, b) apresenta as mesmas propriedades que o reticulado E_6 .

9.6 O reticulado Coxeter-Todd K_{12}

Nesta seção, definiremos o reticulado K_{12} e apresentaremos um reticulado ideal 12-dimensional, par e com o mesmo determinante que o reticulado K_{12} .

Definição 9.6.1 *O reticulado K_{12} é um reticulado par, 12-dimensional, com densidade de centro $\Delta = 0,04945$, norma mínima 4 e determinante 729.*

Seja $\mathbb{K} = \mathbb{Q}(\zeta_{21})$ o 21-ésimo corpo ciclotômico. Temos que $[\mathbb{Q}(\zeta_{21}) : \mathbb{Q}] = \varphi(21) = 12$. Vamos fatorar o diferente $\Delta(\mathbb{Q}(\zeta_{21})|\mathbb{Q})$.

- Temos que $21 = 3 \cdot 7$. Logo, pela Proposição (4.4.1), temos que os ideais gerados por 3 e 7, respectivamente, são os únicos ideais primos de \mathbb{Z} que se ramificam em $\mathbb{Z}[\zeta_{21}]$.
- Como $\phi_{21}(x) = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1 = \min_{\mathbb{Q}} \zeta_{21}$, segue que $\bar{\phi}_{21}(x) = (\bar{1} + x + x^2 + x^3 + x^4 + x^5 + x^6)^2 \pmod{\mathbb{Z}_3[x]}$ e $\bar{\phi}_{21}(x) = (\bar{3} + x)^6(\bar{5} + x)^6 \pmod{\mathbb{Z}_7[x]}$. Assim, pelo Teorema de Kummer (4.1.3), temos que

$$3\mathbb{Z}[\zeta_{21}] = P^2, \text{ onde } P = \langle 3, 1 + \zeta_{21} + \zeta_{21}^2 + \zeta_{21}^3 + \zeta_{21}^4 + \zeta_{21}^5 + \zeta_{21}^6 \rangle \text{ e}$$

$$7\mathbb{Z}[\zeta_{21}] = S^6 R^6, \text{ onde } S = \langle 7, 5 + \zeta_{21} \rangle \text{ e } R = \langle 7, 3 + \zeta_{21} \rangle.$$

Desta forma, os únicos ideais primos de $\mathbb{Z}[\zeta_{21}]$ que se ramificam são P , S e R , sendo estes, os únicos ideais primos de $\mathbb{Z}[\zeta_{21}]$ que dividem o diferente $\Delta(\mathbb{Q}(\zeta_{21})|\mathbb{Q})$. Logo, temos que $\Delta(\mathbb{Q}(\zeta_{21})|\mathbb{Q}) = P^t R^r S^s$, onde $t \geq 1$; $s, r \geq 5$, pela Proposição (4.3.1).

- Agora, temos que $3^{12} = |N_{\mathbb{K}|\mathbb{Q}}(3)| = N(P)^2$ e $7^{12} = N_{\mathbb{K}|\mathbb{Q}}(7) = N(S)^6 N(R)^6$. Como $O_3(7) = 1 \equiv 1 \pmod{2}$, pelo Corolário (4.4.4), segue que $\bar{R} \neq R$ e, assim, $\bar{R} = S$. Logo, temos que $N(R) = N(S)$ e, desta forma, segue que $N(P) = 3^6$ e $N(R) = N(S) = 5$. Pelo Teorema (3.2.1), temos que $N(\Delta(\mathbb{Q}(\zeta_{21})|\mathbb{Q})) = |\text{Disc}(\mathbb{Q}(\zeta_{21})|\mathbb{Q})| = 3^6 7^{10}$. Portanto,

$$\Delta(\mathbb{Q}(\zeta_{21})|\mathbb{Q}) = PR^5 S^5.$$

- Como $\overline{R} = S$, podemos escrever

$$\Delta(\mathbb{Q}(\zeta_{21})|\mathbb{Q}) = PR^5\overline{R}^5 = PR^5\overline{R}^5.$$

Como o diferente se fatora desta forma, pela Proposição (9.1.1), temos que existe um $\mathcal{O}_{\mathbb{K}}$ -reticulado do tipo traço com determinante $N(P) = 729$. Seja $I = R^{-5}$. Consideremos a aplicação:

$$\begin{aligned} b : I \times I &\longrightarrow \mathbb{Z} \\ (x, y) &\longmapsto \text{Tr}_{\mathbb{K}|\mathbb{Q}}(x\bar{y}). \end{aligned}$$

Tomando $\gamma = 1 + \zeta_{21} + \zeta_{21}^6 + \zeta_{21}^7 + \zeta_{21}^8 \in \mathbb{Z}[\zeta_{21}]$, temos que $\gamma + \bar{\gamma} = 1$. Assim, pela Proposição (7.1.3), temos que todo $\mathcal{O}_{\mathbb{K}}$ -reticulado é par. Agora, pela demonstração da Proposição (9.1.1), temos que $\det(b) = N(P) = 729$. Portanto, (I, b) é um $\mathcal{O}_{\mathbb{K}}$ -reticulado par com determinante 729. Desta forma, temos que (I, b) apresenta as mesmas propriedades que o reticulado K_{12} .

9.7 O reticulado Λ_{24}

Nesta seção, definiremos o reticulado Λ_{24} e apresentaremos dois reticulados ideais que são isomorfos ao reticulado Λ_{24} .

Definição 9.7.1 *O reticulado de Leech Λ_{24} é um reticulado par, 24-dimensional. É o mais denso em sua dimensão e pode ser caracterizado como o único reticulado par, unimodular, de dimensão 24 que possui norma mínima 4.*

9.7.1 Λ_{24} via $\mathbb{Q}(\zeta_{39})$

Seja $\mathbb{K} = \mathbb{Q}(\zeta_{39})$ o 39-ésimo corpo ciclotômico. Temos que $[\mathbb{Q}(\zeta_{39}) : \mathbb{Q}] = \varphi(39) = 24$. Vamos fatorar o diferente $\Delta(\mathbb{Q}(\zeta_{39})|\mathbb{Q})$.

- Como $39 = 3 \cdot 13$ segue, pela Proposição (4.4.1), que os ideais gerados por 3 e 13, respectivamente, são os únicos ideais primos de \mathbb{Z} que se ramificam em $\mathbb{Z}[\zeta_{39}]$.
- Como $\phi_{39}(x) = x^{24} - x^{23} + x^{21} - x^{20} + x^{18} - x^{17} + x^{15} - x^{14} + x^{12} - x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1$, segue que $\bar{\phi}_{39}(x) = (2+2x+x^3)^2(2+x^2+x^3)^2(2+x+x^2+x^3)^2(2+2x+2x^2+x^3)^2 \pmod{\mathbb{Z}_3[x]}$ e $\bar{\phi}_{39}(x) = (4+x)^{12}(10+x)^{12} \pmod{\mathbb{Z}_{13}[x]}$. Assim, pelo Teorema de Kummer (4.1.3), temos que

$$3\mathbb{Z}[\zeta_{39}] = P_1^2 P_2^2 P_3^2 P_4^2 \text{ e}$$

$$13\mathbb{Z}[\zeta_{39}] = T^{12}U^{12}.$$

Desta forma, os ideais primos de $\mathbb{Z}[\zeta_{39}]$ que se ramificam são P_1, P_2, P_3, P_4, T e U . Sendo, assim, os ideais primos de $\mathbb{Z}[\zeta_{39}]$ que dividem o diferente $\Delta(\mathbb{Q}(\zeta_{39})|\mathbb{Q})$. Logo, $\Delta(\mathbb{Q}(\zeta_{39})|\mathbb{Q}) = P_1^p P_2^q P_3^r P_4^s T^t U^u$; $p, q, r, s \geq 1$ e $t, u \geq 11$.

- Segue do Teorema (4.3.1) que

$$\Delta(\mathbb{Q}(\zeta_{39})|\mathbb{Q}) = P_1 P_2 P_3 P_4 T^{11} U^{11}.$$

- Agora, notemos que $O_{13}(3) = 3 \equiv 1 \pmod{2}$ e $O_3(13) = 1 \equiv 1 \pmod{2}$. Assim, pelo Corolário (4.4.4), temos que $\overline{P}_i \neq P_i, i = 1, 2, 3, 4$ e $\overline{T} = U$. Podemos reindexar os índices $\{1, 2, 3, 4\}$ de forma que $\overline{P}_1 = P_3$ e $\overline{P}_2 = P_4$. Desta forma, o diferente pode ser escrito como

$$\Delta(\mathbb{Q}(\zeta_{39})|\mathbb{Q}) = P_1 P_2 T^{11} \overline{P}_1 \overline{P}_2 \overline{T}^{11}.$$

Como o diferente se fatora desta forma, pelo Corolário (9.1.1), temos que existe um $\mathcal{O}_{\mathbb{K}}$ -reticulado unimodular do tipo traço. Seja $I = P_1^{-1} P_2^{-1} T^{-11}$. Consideremos a aplicação:

$$b : I \times I \longrightarrow \mathbb{Z}$$

$$(x, y) \longmapsto \text{Tr}_{\mathbb{K}|\mathbb{Q}}(x\bar{y}).$$

Tomando $\gamma = 1 + \zeta_{39} + \zeta_{39}^{12} + \zeta_{39}^{13} + \zeta_{39}^{14} \in \mathbb{Z}[\zeta_{39}]$, temos que $\gamma + \bar{\gamma} = 1$. Assim, pela Proposição (7.1.3), temos que todo $\mathcal{O}_{\mathbb{K}}$ -reticulado é par. Agora, pelo Teorema (7.1.1), temos que $\det(b) = N(I)^2 |\text{Disc}(\mathbb{K}|\mathbb{Q})| = 1$. Portanto, (I, b) é um $\mathcal{O}_{\mathbb{K}}$ -reticulado par com determinante 1. Agora, pela Proposição (9.1.2), como 39 não é primo, $2 \nmid 39$ e $\varphi(39) = 24 \geq 8$, segue que a norma mínima de (I, b) é 4. Assim, de [13], segue que (I, b) é isomorfo ao reticulado Λ_{24} , pois Λ_{24} é o único reticulado par, unimodular e com norma mínima 4 em sua dimensão.

9.7.2 Λ_{24} via $\mathbb{Q}(\zeta_{35})$

Seja $\mathbb{K} = \mathbb{Q}(\zeta_{35})$ o 35-ésimo corpo ciclotômico. Temos que $[\mathbb{Q}(\zeta_{35}) : \mathbb{Q}] = \varphi(35) = 24$.

- Como $35 = 5 \cdot 7$ temos, pela Proposição (4.4.1), que os ideais gerados por 5 e 7, respectivamente, são os únicos ideais primos de \mathbb{Z} que se ramificam em $\mathbb{Z}[\zeta_{35}]$.
- Como $\phi_{35}(x) = x^{24} - x^{23} + x^{19} - x^{18} + x^{17} - x^{16} + x^{14} - x^{13} + x^{12} - x^{11} + x^{10} - x^8 + x^7 - x^6 + x^5 - x + 1$, temos que $\bar{\phi}_{35}(x) = (1 + x + x^2 + x^3 + x^4 + x^5 + x^6)^4 \pmod{\mathbb{Z}_5[x]}$ e

$\bar{\phi}_{35}(x) = (1 + x + x^2 + x^3 + x^4)^6 \pmod{\mathbb{Z}_7[x]}$. Assim, pelo Teorema de Kummer (4.1.3), temos que

$$5\mathbb{Z}[\zeta_{35}] = P^4 \quad \text{e}$$

$$7\mathbb{Z}[\zeta_{35}] = Q^6.$$

Desta forma, os ideais primos de $\mathbb{Z}[\zeta_{35}]$ que se ramificam são P e Q sendo, assim, os ideais primos de $\mathbb{Z}[\zeta_{35}]$ que dividem o diferente $\Delta(\mathbb{Q}(\zeta_{35})|\mathbb{Q})$. Logo, $\Delta(\mathbb{Q}(\zeta_{35})|\mathbb{Q}) = P^r Q^s$; $r \geq 3$, $s \geq 5$.

- Como $N(\Delta(\mathbb{K}|\mathbb{Q})) = |\text{Disc}(\mathbb{K}|\mathbb{Q})| = 5^8 7^{20}$, segue que

$$\Delta(\mathbb{Q}(\zeta_{35})|\mathbb{Q}) = P^3 Q^5 = P Q P \bar{P} Q^2 \bar{Q}^2.$$

Desde que não é possível fatorar o diferente $\Delta(\mathbb{Q}(\zeta_{35})|\mathbb{Q})$ como o produto $\Delta(\mathbb{Q}(\zeta_{35})|\mathbb{Q}) = I\bar{I}$, pelo Corolário (9.1.1), temos que não existe um $\mathcal{O}_{\mathbb{K}}$ -reticulado do tipo traço com determinante 1. Assim, por [15], tomando $\alpha = \frac{(\zeta^3 + \zeta^{-3})(\zeta^6 + \zeta^{-6})(\zeta^9 + \zeta^{-9})(\zeta^{11} + \zeta^{-11})}{\psi'(\zeta + \zeta^{-1})}$, onde ψ é o polinômio minimal de $\zeta + \zeta^{-1}$, temos que α é totalmente positivo e $N_{\mathbb{K}|\mathbb{Q}}(\alpha) = |\text{Disc}(\mathbb{K}|\mathbb{Q})|^{-1}$. Desta forma, o reticulado ideal $(\mathcal{O}_{\mathbb{K}}, b_\alpha)$, onde

$$b_\alpha : \mathcal{O}_{\mathbb{K}} \times \mathcal{O}_{\mathbb{K}} \longrightarrow \mathbb{Z}$$

$$(x, y) \longmapsto \text{Tr}_{\mathbb{K}|\mathbb{Q}}(\alpha x \bar{y})$$

é unimodular. Além disso, tomando $\gamma = 1 - \zeta_{35} + \zeta_{35}^2 - \zeta_{35}^4 + \zeta_{35}^5 - \zeta_{35}^6 + \zeta_{35}^7 - \zeta_{35}^{11} + \zeta_{35}^{12} \in \mathbb{Z}[\zeta_{35}]$, temos que $\gamma + \bar{\gamma} = 1$. Assim, pela Proposição (7.1.3), temos que todo $\mathcal{O}_{\mathbb{K}}$ -reticulado é par. Portanto, $(\mathcal{O}_{\mathbb{K}}, b_\alpha)$ é um $\mathcal{O}_{\mathbb{K}}$ -reticulado par com determinante 1. Agora, pela Proposição (9.1.2), como 35 não é primo, $2 \nmid 35$ e $\varphi(35) = 24 \geq 8$, temos que a norma mínima de $(\mathcal{O}_{\mathbb{K}}, b_\alpha)$ é 4. Assim, por [13], temos que $(\mathcal{O}_{\mathbb{K}}, b_\alpha)$ é isomorfo ao reticulado Λ_{24} , pois Λ_{24} é o único reticulado par, unimodular e com norma mínima 4 em sua dimensão.

Capítulo 10

Reticulados Ideais Complexos

Neste capítulo apresentamos reticulados ideais complexos, algumas de suas principais propriedades e algumas construções de certos reticulados ideais complexos isomorfos ao $\mathbb{Z}[i]^n$ -reticulado. Na Seção 10.1, apresentamos a definição de um reticulado ideal complexo e algumas de suas propriedades. Na Seção 10.2, apresentamos via a construção ciclotômica sobre $\mathbb{Q}(\zeta_{2^r})$, alguns reticulados ideais isomorfos ao $\mathbb{Z}[i]^n$ -reticulado. Por fim, na Seção 10.3, apresentamos via a construções reais a construção de reticulados ideais complexos isomorfos ao $\mathbb{Z}[i]^n$ -reticulado.

10.1 Definição

Nesta seção, apresentamos a definição de ideais reticulados complexos e algumas de suas propriedades.

Definição 10.1.1 *Seja M uma matriz com entradas complexas, cujos vetores que estão nas suas linhas são linearmente independentes sobre \mathbb{C} . Chamamos de **reticulado complexo** ao conjunto de pontos*

$$\Lambda^c = \{\lambda M; \lambda \in \mathbb{Z}[i]^n\}.$$

Definição 10.1.2 *A matriz M da Definição (10.1.1) é chamada de **matriz geradora** do reticulado Λ^c e a matriz $G = MM^H$, onde H denota a transposta conjugada é chamada de **matriz de Gram** de Λ^c .*

Sejam \mathbb{L} uma extensão de $\mathbb{Q}(i)$ de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de \mathbb{L} sobre $\mathbb{Z}[i]$. Notemos que $\mathbb{Q}(i)$ é o corpo de frações de $\mathbb{Z}[i]$. Como o anel $\mathbb{Z}[i]$ é principal segue, pelo Corolário (1.5.7), que todo ideal de $\mathcal{O}_{\mathbb{L}}$ é um $\mathbb{Z}[i]$ -módulo livre de posto n . Uma representação gráfica das extensões é dada por:

$$\begin{array}{c} \mathbb{L} \\ |n \\ \mathbb{Q}(i) \\ |2 \\ \mathbb{Q} \end{array}$$

Definição 10.1.3 *Sejam $\{\sigma_1, \dots, \sigma_n\}$ os n homomorfismos distintos de \mathbb{L} em \mathbb{C} que fixam $\mathbb{Q}(i)$. Definimos o homomorfismo injetivo*

$$\begin{aligned} \sigma : \mathbb{L} &\longrightarrow \mathbb{C}^n \\ x &\longmapsto \sigma(x) = (\sigma_1(x), \dots, \sigma_n(x)) \end{aligned}$$

e o chamamos de **homomorfismo canônico** de \mathbb{L} em \mathbb{C}^n .

Proposição 10.1.1 [20] *Se I é um ideal inteiro de $\mathcal{O}_{\mathbb{L}}$, $\{w_1, \dots, w_n\}$ uma $\mathbb{Z}[i]$ -base de I e σ o homomorfismo canônico de \mathbb{L} em \mathbb{C}^n , então a imagem $\sigma(I)$ em \mathbb{C}^n é um reticulado complexo em \mathbb{C}^n com base $\{\sigma(w_1), \dots, \sigma(w_n)\}$. ■*

Nas condições da Proposição (10.1.1), temos que uma matriz geradora do reticulado $\sigma(I)$ é dada por

$$M = \begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_n(w_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(w_n) & \cdots & \sigma_n(w_n) \end{pmatrix}.$$

Similarmente ao caso real, definimos diversidade complexa e distância produto mínima complexa de um reticulado complexo.

Definição 10.1.4 *Definimos a **diversidade complexa** de um reticulado complexo Λ^c como a menor distância de Hamming entre quaisquer dois vetores do reticulado, isto é,*

$$\text{div}(\Lambda^c) = \min_{0 \neq x \in \Lambda^c} \#\{i \mid x_i \neq 0, i = 1, \dots, n\},$$

com $x = (x_1, \dots, x_n)$, $x_i \in \mathbb{C}$, para todo i .

Definição 10.1.5 *Seja $x = (x_1, \dots, x_n) \in \Lambda^c$, $x_i \in \mathbb{C}$, para todo $i = 1, \dots, n$. Definimos a*

distância produto mínima complexa como

$$d_{p,min}(\Lambda^c) = \min_{0 \neq x \in \Lambda^c} \prod_{x_i \neq 0} |x_i|.$$

Proposição 10.1.2 *Se I é um ideal de $\mathcal{O}_{\mathbb{L}}$, então diversidade complexa do reticulado complexo $\Lambda^c = (I, b)$ é n .*

Demonstração: Sejam $\{w_1, \dots, w_n\}$ uma $\mathbb{Z}[i]$ -base de I e $x = (x_1, \dots, x_n)$; $x_i \in \mathbb{C}$ para todo $i = 1, \dots, n$, um ponto do reticulado Λ^c diferente da origem. Suponha que existe $j \in \{1, \dots, n\}$ tal que $x_j = 0$. Temos que $x = \lambda M$, onde $\lambda = (\lambda_1, \dots, \lambda_n) \in \mathbb{Z}[i]^n$ e $M = (a_{ij}) = (\sigma_j(w_i))$. Assim,

$$0 = x_j = \sum_{i=1}^n \lambda_i \sigma_j(w_i) = \sigma_j\left(\sum_{i=1}^n \lambda_i w_i\right), \lambda_i \in \mathbb{Z}[i], \text{ para todo } i = 1, \dots, n.$$

Isto implica que $\sum_{i=1}^n \lambda_i w_i = 0$. Mas, como $x \neq 0$, segue que $\lambda \neq 0$, o que contradiz o fato de $\{w_i\}_{i=1}^n$ ser uma $\mathbb{Z}[i]$ -base. ■

Definição 10.1.6 *Um reticulado ideal complexo é um par (I, b) , onde I é um ideal de $\mathcal{O}_{\mathbb{L}}$ e $b : I \times I \rightarrow \mathbb{Z}[i]$ é dada por $b(x, y) = \text{Tr}_{\mathbb{L}|\mathbb{Q}(i)}(x\bar{y})$, com $\bar{}$ denotando a conjugação complexa.*

Proposição 10.1.3 *Sejam I um ideal inteiro de $\mathcal{O}_{\mathbb{L}}$, $\{w_1, \dots, w_n\}$ uma $\mathbb{Z}[i]$ -base de I , σ o homomorfismo canônico e $M = (a_{ij}) = (\sigma_j(w_i))$ a matriz geradora do reticulado $\sigma(I)$. Se \mathbb{L} for um CM-corpo, temos que a matriz de Gram é dada por $MM^H = (a_{ij})_{i,j=1}^n$, onde $a_{ij} = \text{Tr}_{\mathbb{L}|\mathbb{Q}(i)}(w_i \bar{w}_j)$.*

Demonstração: Temos que

$$\begin{aligned} MM^H &= \begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_n(w_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(w_n) & \cdots & \sigma_n(w_n) \end{pmatrix} \begin{pmatrix} \overline{\sigma_1(w_1)} & \cdots & \overline{\sigma_1(w_n)} \\ \vdots & \ddots & \vdots \\ \overline{\sigma_n(w_1)} & \cdots & \overline{\sigma_n(w_n)} \end{pmatrix} \\ &= \begin{pmatrix} \sum_{i=1}^n \sigma_i(w_1) \overline{\sigma_i(w_1)} & \cdots & \sum_{i=1}^n \sigma_i(w_1) \overline{\sigma_i(w_n)} \\ \vdots & \ddots & \vdots \\ \sum_{i=1}^n \sigma_i(w_n) \overline{\sigma_i(w_1)} & \cdots & \sum_{i=1}^n \sigma_i(w_n) \overline{\sigma_i(w_n)} \end{pmatrix}. \end{aligned}$$

Como \mathbb{L} é um CM-corpo, segue que a conjugação complexa comuta com σ_i , $i = 1, \dots, n$. Assim, segue que

$$MM^H = \begin{pmatrix} \sum_{i=1}^n \sigma_i(w_1 \bar{w}_1) & \cdots & \sum_{i=1}^n \sigma_i(w_1 \bar{w}_n) \\ \vdots & \ddots & \vdots \\ \sum_{i=1}^n \sigma_i(w_n \bar{w}_1) & \cdots & \sum_{i=1}^n \sigma_i(w_n \bar{w}_n) \end{pmatrix} = \begin{pmatrix} Tr_{\mathbb{L}|\mathbb{Q}(i)}(w_1 \bar{w}_1) & \cdots & Tr_{\mathbb{L}|\mathbb{Q}(i)}(w_1 \bar{w}_n) \\ \vdots & \ddots & \vdots \\ Tr_{\mathbb{L}|\mathbb{Q}(i)}(w_n \bar{w}_1) & \cdots & Tr_{\mathbb{L}|\mathbb{Q}(i)}(w_n \bar{w}_n) \end{pmatrix},$$

o que prova a proposição. ■

Visto que a matriz de Gram de $\sigma(I)$ coincide com a matriz de b , temos que estudar reticulados complexos $\sigma(I)$ equivale a estudar o par (I, b) . Assim, denotamos o reticulado $\sigma(I)$ por $\Lambda^c = (I, b)$.

No que segue, trabalhamos com corpos de números \mathbb{L} tal que \mathbb{L} é um CM-corpo e $\mathbb{Q}(i) \subset \mathbb{L}$.

Proposição 10.1.4 *Se \mathbb{L} é um CM-corpo contendo $\mathbb{Q}(i)$, então \mathbb{L} é o composto de $\mathbb{Q}(i)$ e \mathbb{K} , onde \mathbb{K} é um subcorpo de \mathbb{L} totalmente real tal que $[\mathbb{L} : \mathbb{K}] = 2$.*

Demonstração: Consideremos o seguinte diagrama

$$\begin{array}{ccc} & \mathbb{L} & \\ & | & \\ & \mathbb{K}\mathbb{Q}(i) & \\ / & & \backslash \\ \mathbb{K} & & \mathbb{Q}(i) \\ \backslash & & / \\ & \mathbb{Q} & \end{array}$$

Temos que $[\mathbb{K}\mathbb{Q}(i) : \mathbb{K}]$ divide $[\mathbb{L} : \mathbb{K}] = 2$. Assim, $[\mathbb{K}\mathbb{Q}(i) : \mathbb{K}] = 1$ ou 2 . Se $[\mathbb{K}\mathbb{Q}(i) : \mathbb{K}] = 1$, então $\mathbb{K}\mathbb{Q}(i) = \mathbb{K}$, o que implica que $i \in \mathbb{K}$. Desta forma, para todo $\sigma \in Gal(\mathbb{K}|\mathbb{Q})$, tem-se $\sigma(i) = \pm i$, o que é um absurdo, pois \mathbb{K} é totalmente real. Logo $[\mathbb{K}\mathbb{Q}(i) : \mathbb{K}] = 2$ e assim, $[\mathbb{L} : \mathbb{K}\mathbb{Q}(i)] = 1$. Portanto, $\mathbb{L} = \mathbb{K}\mathbb{Q}(i)$. ■

Assim, como no caso real, a distância produto mínima complexa de um reticulado complexo pode ser relacionada com o discriminante.

Proposição 10.1.5 *Se $I = \alpha\mathcal{O}_{\mathbb{L}}$ é um ideal principal de $\mathcal{O}_{\mathbb{L}}$ e $\Lambda^c = (I, b)$ com*

$$b : I \times I \longrightarrow \mathbb{Z}[i]$$

$$(x, y) \longmapsto cTr_{\mathbb{L}|\mathbb{Q}(i)}(x\bar{y})$$

é um reticulado ideal complexo sobre $\mathbb{Z}[i]$, onde c é um fator normalizador, então

$$|\det(\Lambda^c)| = c^n |N_{\mathbb{L}|\mathbb{Q}(i)}(\alpha)|^2 |Disc(\mathbb{L}|\mathbb{Q}(i))|.$$

Demonstração: Seja $\{w_1, \dots, w_n\}$ uma $\mathbb{Z}[i]$ -base de $\mathcal{O}_{\mathbb{L}}$. Temos que $\{\alpha w_1, \dots, \alpha w_n\}$ é uma $\mathbb{Z}[i]$ -base de I . Assim, por definição, temos que $|\det(\Lambda^c)| = |\det(cTr_{\mathbb{L}|\mathbb{Q}(i)}(\alpha w_j \overline{\alpha w_k}))| = c^n |\det(Tr_{\mathbb{L}|\mathbb{Q}(i)}(\alpha w_j \overline{\alpha w_k}))|$. Notemos que $(Tr_{\mathbb{L}|\mathbb{Q}(i)}(\alpha w_j \overline{\alpha w_k}))_{j,k=1}^n = MAA^H M^H$, onde

$$M = \begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_n(w_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(w_n) & \cdots & \sigma_n(w_n) \end{pmatrix} \quad \text{e} \quad A = \begin{pmatrix} \sigma_1(\alpha) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sigma_n(\alpha) \end{pmatrix}.$$

Desta forma, $\det(Tr_{\mathbb{L}|\mathbb{Q}(i)}(\alpha w_j \overline{\alpha w_k})) = \det(MAA^H M^H) = \det(M)\det(A)\det(A^H)\det(M^H)$. Mas, temos que $\det(A) = N_{\mathbb{L}|\mathbb{Q}(i)}(\alpha)$ e $\det(A^H) = \overline{\det(A)} = \overline{N_{\mathbb{L}|\mathbb{Q}(i)}(\alpha)}$, o que implica que $\det(Tr_{\mathbb{L}|\mathbb{Q}(i)}(\alpha w_j \overline{\alpha w_k})) = \det(M) \det(M^H) N_{\mathbb{L}|\mathbb{Q}(i)}(\alpha) \overline{N_{\mathbb{L}|\mathbb{Q}(i)}(\alpha)} = \det(M) \det(M^H) |N_{\mathbb{L}|\mathbb{Q}(i)}(\alpha)|^2 = \det(M) \overline{\det(M)} |N_{\mathbb{L}|\mathbb{Q}(i)}(\alpha)|^2 = (Disc(\mathbb{L}|\mathbb{Q}(i)))^{1/2} \overline{(Disc(\mathbb{L}|\mathbb{Q}(i)))^{1/2}} |N_{\mathbb{L}|\mathbb{Q}(i)}(\alpha)|^2$. Logo, $\det(Tr_{\mathbb{L}|\mathbb{Q}(i)}(\alpha w_j \overline{\alpha w_k})) = |Disc(\mathbb{L}|\mathbb{Q}(i))| |N_{\mathbb{L}|\mathbb{Q}(i)}(\alpha)|^2$, o que conclui a prova. \blacksquare

Teorema 10.1.1 *Nas mesmas condições da Proposição (10.1.5), temos que*

$$d_{p,min}(\Lambda^c) = \sqrt{\frac{|\det(\Lambda^c)|}{|Disc(\mathbb{L}|\mathbb{Q}(i))|}}.$$

Demonstração: Seja $\{w_1, \dots, w_n\}$ uma $\mathbb{Z}[i]$ -base de $\mathcal{O}_{\mathbb{L}}$. Temos que $\{\alpha w_1, \dots, \alpha w_n\}$ é uma $\mathbb{Z}[i]$ -base de I . Desta forma, dado $x \in \Lambda^c$ temos que $x = \sqrt{c}\lambda M$, onde $\lambda = (\lambda_1, \dots, \lambda_n) \in \mathbb{Z}[i]^n$ e $M = (a_{ij}) = (\sigma_j(w_i))$. Vimos que Λ^c tem diversidade n . Assim,

$$\begin{aligned} d_{p,min}(\Lambda^c) &= \min_{0 \neq x \in \Lambda^c} |x_j| = \prod_{j=1}^n |x_j| = \prod_{j=1}^n |\sqrt{c} \sum_{i=1}^n \lambda_i \sigma_j(\alpha w_i)| \\ &= \sqrt{c^n} \min_{0 \neq y \in \mathcal{O}_{\mathbb{L}}} |N_{\mathbb{L}|\mathbb{Q}(i)}(\alpha \sum_{i=1}^n \lambda_i w_i)| = \sqrt{c^n} |N_{\mathbb{L}|\mathbb{Q}(i)}(\alpha)|, \end{aligned}$$

pois $\alpha \in I$ e $|N_{\mathbb{L}|\mathbb{Q}(i)}(\alpha)| \leq |N_{\mathbb{L}|\mathbb{Q}(i)}(\alpha \sum_{i=1}^n \lambda_i w_i)|$. Usando a Proposição (10.1.5), temos que

$$d_{p,min}(\Lambda^c) = \sqrt{c^n} |N_{\mathbb{L}|\mathbb{Q}(i)}(\alpha)| = \sqrt{c^n} \sqrt{\frac{|\det(\Lambda^c)|}{c^n |Disc(\mathbb{L}|\mathbb{Q}(i))|}} = \sqrt{\frac{|\det(\Lambda^c)|}{|Disc(\mathbb{L}|\mathbb{Q}(i))|}}. \quad \blacksquare$$

Corolário 10.1.1 Se $Disc(\mathbb{K}|\mathbb{Q})$ é um número ímpar, então $d_{p,min}(\Lambda^c) = \sqrt{\frac{|det(\Lambda^c)|}{|Disc(\mathbb{K}|\mathbb{Q})|}}$.

Demonstração: Como $Disc(\mathbb{Q}(i)|\mathbb{Q}) = -4$ e $Disc(\mathbb{K}|\mathbb{Q})$ é um número ímpar, temos que $mdc(Disc(\mathbb{K}|\mathbb{Q}), Disc(\mathbb{Q}(i)|\mathbb{Q})) = 1$. Assim, pela Proposição (3.2.2), temos que uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{L}}$ é dada pelo produto de uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}}$ por uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{Q}(i)}$. Temos que $\{1, i\}$ é uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{Q}(i)}$. Se $\{w_1, \dots, w_n\}$ é uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}}$, então $\{w_1, \dots, w_n, iw_1, \dots, iw_n\}$ é uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{L}}$. Mostremos que $\{w_1, \dots, w_n\}$ é uma $\mathbb{Z}[i]$ -base de $\mathcal{O}_{\mathbb{L}}$. Como $\{w_1, \dots, w_n, iw_1, \dots, iw_n\}$ é uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{L}}$, segue que para todo $x \in \mathcal{O}_{\mathbb{L}}$, existem $a_j, b_j \in \mathbb{Z}$ tal que

$$x = \sum_{j=1}^n a_j w_j + \sum_{j=1}^n b_j i w_j = \sum_{j=1}^n (a_j + i b_j) x_j \in \sum_{j=1}^n \mathbb{Z}[i] x_j.$$

Como $\sum_{j=1}^n \mathbb{Z}[i] x_j \subset \mathcal{O}_{\mathbb{L}}$, segue que $\{w_1, \dots, w_n\}$ gera $\mathcal{O}_{\mathbb{L}}$ sobre $\mathbb{Z}[i]$. Agora, suponha que

$\sum_{j=1}^n c_j w_j = 0$; $c_j \in \mathbb{Z}[i]$. Como $c_j \in \mathbb{Z}[i]$, segue que $c_j = a_j + i b_j$; $a_j, b_j \in \mathbb{Z}$, para todo $i, j =$

$1, \dots, n$. Desta forma, $\sum_{j=1}^n c_j w_j = \sum_{j=1}^n a_j w_j + \sum_{j=1}^n b_j i w_j = 0$. Como $\{w_1, \dots, w_n, iw_1, \dots, iw_n\}$ é uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{L}}$, temos que $a_j, b_j = 0$, para todo i, j . Portanto, $\{w_1, \dots, w_n\}$ é linearmente independente sobre $\mathbb{Z}[i]$ e assim, uma $\mathbb{Z}[i]$ -base de $\mathcal{O}_{\mathbb{L}}$. Assim, pelo Teorema (1.3.4), como $\mathbb{K} \cap \mathbb{Q}(i) = \mathbb{Q}$ temos que $Disc(\mathbb{L}|\mathbb{Q}(i)) = (det(\sigma_i(w_j)))^2 = (det(\sigma_{i_{\mathbb{K}}}(w_j)))^2 = Disc(\mathbb{K}|\mathbb{Q})$. ■

10.2 Construção Ciclotômica sobre $\mathbb{Q}(\zeta_{2^r})$

Sejam $\zeta = \zeta_{2^r}$ uma raiz 2^r -ésima primitiva da unidade e $\mathbb{L} = \mathbb{Q}(\zeta)$. Notemos que $\mathbb{L} = \mathbb{Q}(\zeta + \zeta^{-1})\mathbb{Q}(i)$. Logo, \mathbb{L} é um CM-corpo. Nesta seção apresentamos a construção de reticulados complexos via reticulados ideais complexos $\Lambda^c = (\mathcal{O}_{\mathbb{L}}, b)$, onde $\mathcal{O}_{\mathbb{L}}$ é o anel de inteiros de \mathbb{L} sobre $\mathbb{Z}[i]$. O reticulado construído é isomorfo ao $\mathbb{Z}[i]$ -reticulado complexo.

Proposição 10.2.1 Tem-se que $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\zeta]$ é um $\mathbb{Z}[i]$ -módulo livre de posto 2^{r-2} e uma $\mathbb{Z}[i]$ -base de $\mathcal{O}_{\mathbb{L}}$ é dada por $\{1, \zeta, \zeta^2, \dots, \zeta^{2^{r-2}-1}\}$.

Demonstração: Seja $x \in \mathbb{Z}[\zeta]$. Temos que $\mathbb{Z}[\zeta]$ é um \mathbb{Z} -módulo livre com base $\{1, \zeta, \dots, \zeta^{2^{r-1}-1}\}$. Assim,

$$x = \sum_{k=0}^{2^{r-1}-1} a_k \zeta^k = \sum_{k=0}^{2^{r-2}-1} a_k \zeta^k + \sum_{k=2^{r-2}}^{2^{r-1}-1} a_k \zeta^k, \quad a_k \in \mathbb{Z}$$

$$\begin{aligned}
&= \sum_{k=0}^{2^{r-2}-1} a_k \zeta^k + \sum_{l=0}^{2^{r-2}-1} i a_l^* \zeta^l; \quad a_l^* = a_{l+2^{r-2}} \in \mathbb{Z} \\
&= \sum_{k=0}^{2^{r-2}-1} (a_k + i a_k^*) \zeta^k; \quad a_k + i a_k^* \in \mathbb{Z}[i].
\end{aligned}$$

Além disso, esta representação de x é única. Portanto, $\{1, \zeta, \dots, \zeta^{2^{r-2}-1}\}$ é uma $\mathbb{Z}[i]$ -base de $\mathcal{O}_{\mathbb{L}}$. ■

Lema 10.2.1 *Seja $g(x) = x^n - a \in \mathbb{C}[x]$ tal que $|a| = 1$ e $\alpha_1, \dots, \alpha_n$ são raízes de g em \mathbb{C} , então*

$$\begin{aligned}
S_p &= \sum_{k=1}^n \alpha_k^p = \alpha_1^p + \dots + \alpha_n^p = 0, \quad \text{se } 1 \leq p \leq n-1, \\
S &= \sum_{k=1}^n |\alpha_k|^2 = |\alpha_1|^2 + \dots + |\alpha_n|^2 = n.
\end{aligned}$$

Demonstração: Seja $w = e^{\frac{2\pi i}{n}}$ uma raiz de $f(x) = x^n - 1$. Temos que as raízes de f são dadas por $R_f = \{1, w, \dots, w^{n-1}\}$. Desta forma,

$$\sum_{k=0}^{n-1} (w^p)^k = 1 + w^p + (w^p)^2 + \dots + (w^p)^{n-1} = 0,$$

pois $x^n - 1 = (x-1)(x^{n-1} + \dots + x + 1)$ e w^p , onde $1 \leq p \leq n-1$ é raiz de $x^{n-1} + \dots + x + 1$. Agora, temos que as raízes de g são dadas por $R_g = \{b, bw, bw^2, \dots, bw^{n-1}\}$, onde b é uma raiz n -ésima de a . Assim

$$\begin{aligned}
S_p &= \sum_{k=1}^n \alpha_k^p = b^p + (bw)^p + \dots + (bw^{n-1})^p \\
&= b^p(1 + w^p + \dots + (w^p)^{n-1}) = 0, \quad \text{se } 1 \leq p \leq n-1.
\end{aligned}$$

Deste modo, como $|b| = 1$ e $|w^k| = 1$, $k = 0, 1, \dots, n-1$, segue que

$$\begin{aligned}
S &= \sum_{k=1}^n |\alpha_k|^2 = |b|^2 + |bw|^2 + \dots + |bw^{n-1}|^2 \\
&= |b|^2(1 + |w|^2 + \dots + |w^{n-1}|^2) = n,
\end{aligned}$$

o que prova o lema. ■

Temos que $\mathbb{L} = \mathbb{Q}(i)(\zeta) = \mathbb{Q}(i)(R_m)$, onde $m(x) = x^{2^{r-2}} - i = \min_{\mathbb{Q}(i)} \zeta$. Agora, temos que $R_m = \{\theta_1, \dots, \theta_{2^{r-2}}\}$, onde $\theta_i = e^{\frac{\pi/2 + 2(i-1)\pi}{2^{r-2}}}$, para $i = 1, \dots, 2^{r-2}$ e $|\theta_i| = 1$, para todo

$i = 1, \dots, 2^{r-2}$.

Observação 10.2.1 O grupo de Galois $Gal(\mathbb{L}|\mathbb{Q}(i))$ é dado por $Gal(\mathbb{L}|\mathbb{Q}(i)) = \{\sigma_1, \dots, \sigma_{2^{r-2}}\}$, onde $\sigma_i(\zeta) = \theta_i$, para todo $i = 1, \dots, 2^{r-2}$.

Consideremos o homomorfismo canônico σ . Vimos que $\sigma(\mathcal{O}_{\mathbb{L}})$ é um reticulado complexo com matriz geradora M dada por

$$\begin{aligned} M &= \begin{pmatrix} \sigma_1(1) & \sigma_2(1) & \cdots & \sigma_{2^{r-2}}(1) \\ \sigma_1(\zeta) & \sigma_2(\zeta) & \cdots & \sigma_{2^{r-2}}(\zeta) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\zeta^{2^{r-2}-1}) & \sigma_2(\zeta^{2^{r-2}-1}) & \cdots & \sigma_{2^{r-2}}(\zeta^{2^{r-2}-1}) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \theta_1 & \theta_2 & \cdots & \theta_{2^{r-2}} \\ \vdots & \vdots & \ddots & \vdots \\ \theta_1^{2^{r-2}-1} & \theta_2^{2^{r-2}-1} & \cdots & \theta_{2^{r-2}}^{2^{r-2}-1} \end{pmatrix}. \end{aligned}$$

Seja $\overline{M} = \frac{1}{\sqrt{2^{r-2}}}M$. Temos que cada entrada da matriz de Gram $G = \overline{M}\overline{M}^H$, onde H denota a transposta conjugada, é dada por

$$a_{ij} = \frac{1}{2^{r-2}} \sum_{k=1}^{2^{r-2}} \theta_k^{i-1} \overline{\theta_k^{j-1}}, \quad 1 \leq i, j \leq 2^{r-2}.$$

Proposição 10.2.2 Nas condições anteriores, se a matriz de Gram é dada por $\overline{M}\overline{M}^H = (a_{ij})_{i,j=1}^{2^{r-2}}$, então $a_{ij} = 1$, se $i = j$ e $a_{ij} = 0$, se $i \neq j$.

Demonstração: Temos para $i = 1, \dots, 2^{r-2}$ que

$$a_{ii} = \frac{1}{2^{r-2}} \sum_{k=1}^{2^{r-2}} \theta_k^{i-1} \overline{\theta_k^{i-1}} = \frac{1}{2^{r-2}} \sum_{k=1}^{2^{r-2}} |\theta_k^{i-1}|^2 = \frac{1}{2^{r-2}} \sum_{k=1}^{2^{r-2}} 1 = 1,$$

pois $|\theta_k| = |i|^{1/2^{r-2}} = 1$. Agora, para $1 \leq j < i \leq 2^{r-2}$, temos que

$$a_{ij} = \frac{1}{2^{r-2}} \sum_{k=1}^{2^{r-2}} \theta_k^{i-1} \overline{\theta_k^{j-1}} = \frac{1}{2^{r-2}} \sum_{k=1}^{2^{r-2}} \theta_k^{i-j} = 0.$$

Como $a_{ij} = \overline{a_{ji}}$, segue que $a_{ij} = 0$, para todo $i \neq j$, o que prova a proposição. ■

Segue da Proposição (10.2.2) que o reticulado ideal complexo $\Lambda^c = (\mathcal{O}_{\mathbb{L}}, \frac{1}{2^{r-2}}b)$, onde $b : \mathcal{O}_{\mathbb{L}} \times \mathcal{O}_{\mathbb{L}} \longrightarrow \mathbb{Z}[i]$ é dada por $b(x, y) = Tr(xy)$, é isomorfo ao $\mathbb{Z}[i]^n$ -reticulado. Vamos, agora, calcular a distância produto mínima para esta construção. Notemos que como $\mathbb{L} = \mathbb{Q}(\zeta) = \mathbb{Q}(\zeta + \zeta^{-1})\mathbb{Q}(i)$ e $|\det(\lambda^c)| = 1$, segue que

$$d_{p,min}(\Lambda^c) = \frac{1}{\sqrt{|Disc(\mathbb{L}|\mathbb{Q}(i))|}}.$$

Proposição 10.2.3 *O discriminante $Disc(\mathbb{Q}(\zeta)|\mathbb{Q}(i))$ satisfaz $|Disc(\mathbb{Q}(\zeta)|\mathbb{Q}(i))| = (2^{r-2})^{2^{r-2}}$.*

Demonstração: Temos que $|Disc(\mathbb{Q}(\zeta)|\mathbb{Q}(i))| = |N_{\mathbb{Q}(\zeta)|\mathbb{Q}(i)}(f'(\zeta))|$, onde $f = \min_{\mathbb{Q}(i)}\zeta$. Como $f(x) = x^{2^{r-2}} - i = \min_{\mathbb{Q}(i)}\zeta$ e $f'(\zeta) = 2^{r-2}i\zeta^{-1}$, segue que

$$N_{\mathbb{Q}(\zeta)|\mathbb{Q}(i)}(f'(\zeta)) = (2^{r-2}i)^{2^{r-2}}N_{\mathbb{Q}(\zeta)|\mathbb{Q}(i)}(\zeta^{-1}).$$

Olhando o termo independente de f , temos que $|N_{\mathbb{Q}(\zeta)|\mathbb{Q}(i)}(\zeta^{-1})| = 1$. Assim $|Disc(\mathbb{Q}(\zeta)|\mathbb{Q}(i))| = (2^{r-2})^{2^{r-2}}$. ■

Corolário 10.2.1 *A distância produto mínima do reticulado ideal complexo $\Lambda^c = (\mathcal{O}_{\mathbb{L}}, b)$ é $d_{p,min}(\Lambda^c) = (2^{r-2})^{-2^{r-3}}$.*

Demonstração: Temos que $d_{p,min}(\Lambda^c) = \frac{1}{|Disc(\mathbb{L}|\mathbb{Q}(i))|^{1/2}} = \frac{1}{((2^{r-2})^{2^{r-2}})^{1/2}}$. Segue então que $d_{p,min}(\Lambda^c) = \frac{1}{(2^{r-2})^{\frac{2^{r-2}}{2}}} = \frac{1}{(2^{r-2})^{2^{r-3}}} = (2^{r-2})^{-2^{r-3}}$. ■

Exemplo 10.2.1 *Sejam $\zeta = \zeta_{2^4} = \zeta_{16}$ e $\mathbb{L} = \mathbb{Q}(\zeta)$. Temos que $\{1, \zeta, \zeta^2, \zeta^3\}$ é uma $\mathbb{Z}[i]$ -base de $\mathcal{O}_{\mathbb{L}}$. Seja $m(x) = x^4 - i = \min_{\mathbb{Q}(i)}\zeta$. Temos que $R_m = \{\theta_1, \theta_2, \theta_3, \theta_4\}$, onde $\theta_i = e^{\frac{\pi/2+2(i-1)\pi}{4}i}$. Assim, $R_m = \{e^{\frac{\pi i}{8}}, e^{\frac{5\pi i}{8}}, e^{\frac{9\pi i}{8}}, e^{\frac{13\pi i}{8}}\}$. Além disso, temos que $H = Gal(\mathbb{L}|\mathbb{Q}(i)) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$, onde $\sigma_i(\zeta) = \theta_i$. Assim, segue que*

$$M = \frac{1}{2} \begin{pmatrix} \sigma_1(1) & \sigma_2(1) & \sigma_3(1) & \sigma_4(1) \\ \sigma_1(\zeta) & \sigma_2(\zeta) & \sigma_3(\zeta) & \sigma_4(\zeta) \\ \sigma_1(\zeta^2) & \sigma_2(\zeta^2) & \sigma_3(\zeta^2) & \sigma_4(\zeta^2) \\ \sigma_1(\zeta^3) & \sigma_2(\zeta^3) & \sigma_3(\zeta^3) & \sigma_4(\zeta^3) \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ \theta_1 & \theta_2 & \theta_3 & \theta_4 \\ \theta_1^2 & \theta_2^2 & \theta_3^2 & \theta_4^2 \\ \theta_1^3 & \theta_2^3 & \theta_3^3 & \theta_4^3 \end{pmatrix}$$

é a matriz geradora de um reticulado ideal complexo Λ^c isomorfo ao $\mathbb{Z}[i]^n$ -reticulado. Além disso, $d_{p,min}(\Lambda^c) = (2^{4-2})^{-2^{4-3}} = 0,0625$.

10.3 Construções Complexas a partir de Construções Reais

Nesta seção, apresentamos um método para construir $\mathbb{Z}[i]^n$ -reticulados rotacionados a partir de construções de \mathbb{Z}^n -reticulados de corpos de números totalmente reais. Para isso, sejam \mathbb{K} um corpo de números totalmente real com discriminante $Disc(\mathbb{K}|\mathbb{Q})$ ímpar e $\mathbb{L} = \mathbb{K}\mathbb{Q}(i)$ o composto de \mathbb{K} e $\mathbb{Q}(i)$. Estamos interessados na extensão $\mathbb{L}|\mathbb{Q}(i)$.

Seja $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros de \mathbb{L} sobre $\mathbb{Z}[i]$. A seguir vamos encontrar uma $\mathbb{Z}[i]$ -base de $\mathcal{O}_{\mathbb{L}}$.

Lema 10.3.1 *Seja $Disc(\mathbb{K}|\mathbb{Q})$ um número ímpar, se $B_K = \{v_j\}_{j=1}^n$ é uma \mathbb{Z} -base de \mathbb{K} , então B_K é uma $\mathbb{Z}[i]$ -base de \mathbb{L} . Além disso, se $B_L = \{w_j\}_{j=1}^n$ é uma $\mathbb{Z}[i]$ -base de \mathbb{L} , então $\{iw_j\}_{j=1}^n$ é também uma $\mathbb{Z}[i]$ -base de \mathbb{L} .*

Demonstração: Seja $x \in \mathcal{O}_{\mathbb{L}}$. Como $mdc(Disc(\mathbb{K}|\mathbb{Q}), Disc(\mathbb{Q}(i)|\mathbb{Q})) = 1$, segue que uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{L}}$ é dada por $\{v_1, \dots, v_n, iv_1, \dots, iv_n\}$. Assim, $x = \sum_{j=1}^n (a_j + ib_j)v_j$, $a_j, b_j \in \mathbb{Z}$, para todo $j = 1, \dots, n$. Logo $\{v_i\}_{i=1}^n$ é um conjunto de geradores de $\mathcal{O}_{\mathbb{L}}$ visto como $\mathbb{Z}[i]$ -módulo. Suponha que $\sum_{j=1}^n \beta_j v_j = 0$; onde $\beta_j = a_j + ib_j$, com $a_j, b_j \in \mathbb{Z}$, para todo $j = 1, \dots, n$.

Assim, $\sum_{j=1}^n \beta_j v_j = \sum_{j=1}^n a_j v_j + \sum_{j=1}^n b_j i v_j = 0$. Então $a_j = b_j = 0$, para todo $j = 1, \dots, n$, pois $\{v_1, \dots, v_n, iv_1, \dots, iv_n\}$ é linearmente independente. Portanto $\{v_1, \dots, v_n\}$ é uma $\mathbb{Z}[i]$ -base de $\mathcal{O}_{\mathbb{L}}$. Agora como $\{w_j\}_{j=1}^n$ é uma $\mathbb{Z}[i]$ -base de $\mathcal{O}_{\mathbb{L}}$ segue que para todo $x \in \mathcal{O}_{\mathbb{L}}$, tem-se $x = \sum_{j=1}^n a_j w_j = \sum_{j=1}^n (-ia_j) i w_j$, $a_j \in \mathbb{Z}[i]$. Portanto $\{i w_j\}_{j=1}^n$ gera $\mathcal{O}_{\mathbb{L}}$. Agora, se $\sum_{j=1}^n \beta_j i w_j = 0$ então $i \beta_j = 0$, para todo $j = 1, \dots, n$, pois $\{w_j\}_{j=1}^n$ é base. Assim $\beta_j = 0$, para todo $j = 1, \dots, n$. Logo $\{i w_j\}_{j=1}^n$ é uma $\mathbb{Z}[i]$ -base de $\mathcal{O}_{\mathbb{L}}$. ■

Proposição 10.3.1 *Se $B_I = \{w_j = iv_j\}_{j=1}^n$ é uma $\mathbb{Z}[i]$ -base de um ideal $I \subset \mathcal{O}_{\mathbb{L}}$, então $Tr_{\mathbb{L}|\mathbb{Q}(i)}(w_j \bar{w}_k) = Tr_{\mathbb{K}|\mathbb{Q}}(v_j v_k)$.*

Demonstração: Temos que $Tr_{\mathbb{L}|\mathbb{Q}(i)}(w_j \bar{w}_k) = Tr_{\mathbb{L}|\mathbb{Q}(i)}(iv_j (-i\bar{v}_j)) = Tr_{\mathbb{L}|\mathbb{Q}(i)}(v_j \bar{v}_k) = Tr_{\mathbb{K}|\mathbb{Q}}(v_j v_k)$, pois, temos que $Gal(\mathbb{L}|\mathbb{Q}(i)) = Gal(\mathbb{K}|\mathbb{Q})$. ■

Agora, veremos como é feita a construção de tais reticulados complexos.

Seja $I_{\mathbb{K}}$ um ideal de $\mathcal{O}_{\mathbb{K}}$ com \mathbb{Z} -base $\{v_1, \dots, v_n\}$ tal que $\frac{1}{c} Tr_{\mathbb{K}|\mathbb{Q}}(v_i v_j) = \delta_{ij}$, para $i, j = 1, \dots, n$, onde c é um fator normalizador. Seja $I_{\mathbb{L}}$ um ideal de $\mathcal{O}_{\mathbb{L}}$ cuja $\mathbb{Z}[i]$ -base de $I_{\mathbb{L}}$ é

$\{iv_1, \dots, iv_n\} = \{w_1, \dots, w_n\}$. Temos que

$$M = \frac{1}{\sqrt{c}} \begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_n(w_1) \\ \vdots & & \vdots \\ \sigma_1(w_n) & \cdots & \sigma_n(w_n) \end{pmatrix}$$

é uma matriz geradora de $\Lambda^c = (I_{\mathbb{L}}, \frac{1}{c}b)$. Note que $MM^H = Id$, pois $\frac{1}{c}Tr_{\mathbb{L}|\mathbb{Q}(i)}(w_i\bar{w}_j) = \frac{1}{c}Tr_{\mathbb{K}|\mathbb{Q}}(v_iv_j) = \delta_{ij}$. Temos que $d_{p,min}(\Lambda^c) = \frac{1}{\sqrt{Disc(\mathbb{K}|\mathbb{Q})}} = d_{p,min}(\Lambda)$, onde $\Lambda = (I_{\mathbb{K}}, \frac{1}{c}b)$.

Referências Bibliográficas

- [1] DOMINGUES, H. H.; IEZZI, G. **Álgebra moderna**. São Paulo: Atual, 1982.
- [2] MILIES, F. C. P. **Anéis e módulos**. São Paulo: L.P.M, 1972.
- [3] SAMUEL, P. **Algebraic theory of numbers**. Paris: Hermann, 1970.
- [4] STEWART, I. N.; TALL, D. O. **Algebraic number theory**. London: Chapman & Hall, 1987.
- [5] RIBENBOIM, P. **Algebraic numbers**. New-York: Wiley-Interscience, 1972.
- [6] MARCUS, D. A. **Numbers fields**. New York: Springer-Verlag, 1977.
- [7] WASHINGTON, L. C. **Introduction to cyclotomic fields**. New York: Springer-Verlag, 1982.
- [8] LANG, S. **Algebraic number theory**. New York: Addison-Wesley, 1970.
- [9] LANG, S. **Algebra**. New York: Addison-Wesley, 1965.
- [10] ENDLER, O. **Teoria dos números algébricos**. Rio de Janeiro: Impa, 1986.
- [11] SWINNERTON-DYER, H. P. F. **A brief guide to algebraic number theory**. Cambridge: University of Cambridge, 2001.
- [12] FLORES, A. L. **Reticulados em corpos abelianos**. 2000, 115f. Tese (Doutorado em Engenharia Elétrica), Faculdade de Engenharia Elétrica e da Computação, Universidade Estadual de Campinas, Campinas, 2000.
- [13] CONWAY, J. H.; SLOANE, N. J. A. **Sphere packings, lattices and groups**. New-York: Springer-Verlag, 1988.
- [14] MAZUCCHI, E. C. **Reticulados numéricos**. 2006, 137f. Dissertação (Mestrado em Matemática), Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2006.
- [15] BAYER-FLUCKIGER, E. Definite unimodular lattices having an automorphism of given characteristic polynomial. **Commentarii Mathematici Helvetici**, Suíça, v. 59, p. 509-538, 1984.

- [16] BAYER-FLUCKIGER, E. Lattices and number fields. **Contemporary Mathematics**, Providence, v. 241, p. 69-84, 1999.
- [17] BAYER-FLUCKIGER, E.; OGGIER, F.; VITERBO, E. Algebraic lattice constellations bounds on performance. **IEEE Transactions on Information Theory**, New-York, v. 52, n. 1, p. 319-327, Jan. 2006.
- [18] BOUTROS, J.; VITERBO, E.; RASTELLO, C.; BELFIORI, J. C. Good lattice constellations for both rayleigh fading and gaussian channels. **IEEE Transactions on Information Theory**, New-York, v. 42, n. 2, p. 502-517, Mar. 1996.
- [19] BAYER-FLUCKIGER, E.; OGGIER, F.; VITERBO, E. New algebraic constructions of rotated \mathbb{Z}^n -lattice constellations for the Rayleigh fading channel. **IEEE Transactions on Information Theory**, New-York, v. 50, n. 4, p. 702-714, Apr. 2004.
- [20] OGGIER, F. **Algebraic methods for channel coding**. 2005, 125f. Tese (Doutorado em Matemática e Informática), École Polytechnique Fédérale de Lausanne, Lausanne, 2005.
- [21] ANDRADE, A. A.; ALVES, C.; CARLOS, T. B. Rotated lattices via the cyclotomic field $\mathbb{Q}(\zeta_{2^r})$, **International Journal of Applied Mathematics**, Sofia, v. 19, n. 3, p. 321-331, 2006.
- [22] LOPES, J. O. D. Discriminants of subfields of $\mathbb{Q}(\zeta_{2^r})$. **Journal of Algebra and Its Applications**, New Jersey, v. 2, p. 463-469, 2003.
- [23] GIRAUD, X.; BOUTILLON, E.; BELFIORE, J. C. Algebraic tools to build modulation schemes for fading channels. **IEEE Transaction on Information Theory**, New-York, v. 43, n. 3, p. 938-952, May 1997.

Índice Remissivo

- Anel, 15
- Anel de Dedekind, 43
- Anel de frações, 51
- Anel de integridade, 15
- Anel de inteiros, 31
- Anel integralmente fechado, 33
- Anel reduzido, 19

- Base complementar, 65
- Base de um reticulado, 108

- CM-corpo, 25
- Codiferente, 63
- Corpo, 15
- Corpo ciclotômico, 59
- Corpo composto, 25
- Corpo de números, 24
- Corpo fixo da involução, 124
- Corpo quadrático, 57
- Corpo totalmente imaginário, 24
- Corpo totalmente real, 24

- Densidade de centro, 115
- Densidade de empacotamento, 115
- Determinante do reticulado, 111
- Diferente, 70
- Diferente de uma extensão sobre P , 74
- Discriminante absoluto, 39
- Discriminante de n -upla, 37
- Discriminante de corpos ciclotômicos, 77
- Discriminante de uma extensão, 38
- Distância produto mínima, 114
- Distância produto mínima complexa, 164
- Diversidade, 113
- Diversidade complexa, 163

- Elemento inteiro, 28
- Elemento nilpotente, 19
- Empacotamento esférico, 114
- Empacotamento reticulado, 114
- Extensão de corpos, 24

- Grau da extensão, 24
- Grau de inércia, 81
- Grupo, 14
- Grupo de decomposição, 93

- Homomorfismo de anéis, 16
- Homomorfismo de módulos, 20
- Homomorfismo de Minkowski, 117
- Homomorfismo torcido, 121

- Ideais fracionários, 42
- Ideais inteiros, 42
- Ideais primos conjugados, 92
- Ideal, 15
- Ideal estendido, 79
- Ideal maximal, 17
- Ideal primo, 17

Ideal ramificado, 82, 109
 Índice de ramificação, 81
 Inteiro algébrico, 31
 Involução, 124

 Módulo, 19
 Módulo noetheriano, 21
 Módulo quociente, 20
 Matriz de Gram, 110, 162
 Matriz geradora de um reticulado, 110, 162

 Norma de um elemento, 26
 Norma de um ideal fracionário, 50
 Norma de um ideal inteiro, 46
 Norma mínima, 114

 O reticulado Λ_{24} , 159
 O reticulado A_{p-1} com p primo, 150
 O reticulado D_4 , 151
 O reticulado E_6 , 157
 O reticulado E_8 , 153
 O reticulado K_{12} , 158

 Polinômio característico, 26
 Polinômio ciclotômico, 59
 Polinômio minimal, 24

 Raiz n -ésima da unidade, 59
 Raiz n -ésima primitiva da unidade, 59
 Região fundamental, 109
 Reticulado ideal, 125
 Reticulado ideal complexo, 162, 164
 Reticulado no \mathbb{R}^n , 108
 Reticulado par, 126

 Subcorpo maximal real de $\mathbb{Q}(\zeta_n)$, 62
 Submódulo, 19

 Subreticulado, 112

 Teorema da igualdade fundamental, 86
 Teorema de Kummer, 89
 Teorema do isomorfismo de anéis, 16
 Teorema do isomorfismo de módulos, 21
 Traço de um elemento, 26

 Versão escalar, 113
 Volume da região fundamental, 111