Discriminante, Ramificação e Diferente

Ciléia Mazzei de Oliveira

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 - SP

Fevereiro - 2005

"A hora em que Deus
responde as nossas preces
pode não ser a nossa hora.
Mas Ele sempre responde."
(Donald E. Kohlstaedt)

À minha família,
Geni, Willer e Durval.
E ao meu namorado, Orlando
dedico.

Agradecimentos

Ao concluir este trabalho, agradeço primeiramente a Deus.

Ao Prof. Dr. Antonio Aparecido de Andrade, pelo incentivo, amizade e dedicação.

À banca examinadora: Prof. Dr. Ali Messaoudi (IBILCE - UNESP - S.J.Rio Preto), Prof. Dr. Marcelo Muniz da Silva Alves (UFPR - Curitiba), Prof. Dr. Trajano Pires da Nóbrega Neto (IBILCE - UNESP - S.J.Rio Preto) e Prof. Dr. Raul Antonio Ferraz (IME - USP - São Paulo).

À minha mãe, pela confiança, pelo incentivo e principalmente pelas palavras de amor e coragem nos momentos mais difíceis da minha vida.

À minha família que entenderam a minha ausência em momentos importantes, em particular ao meu irmão e meu padrasto.

Ao Orlando, pelo amor, incentivo, confiança e por estar sempre comigo nos momentos de alegria e nos de dificuldade.

À Sabrina pela amizade e por compartilhar momentos importantes desde o início desta etapa.

Aos amigos da pós-graduação pelo agradável convívio, em particular ao Juliano e a Carina.

Ao Márcio, por estar sempre torcendo por mim.

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

À Capes, por parte do auxílio financeiro.

Resumo

Os objetivos deste trabalho foram relacionar a ramificação com os conceitos de discriminante e diferente. Utilizando esses conceitos foram feitos aplicações em reticulados e códigos. Nessas aplicações, estudamos algumas maneiras de obtermos reticulados e também alguns códigos, chamados códigos de bloco espaço-tempo.

Palavras-chave: Discriminante, ramificação, diferente, reticulado, códigos de bloco espaço tempo.

Abstract

The aims of this work were to relate ramification with the concepts of different and discriminant. Using those concepts we made applications in lattices and codes. In those applications, we study some ways to get lattices and some codes, called block codes space-time.

Keywords: Discriminant, ramification, different, lattices, block codes space-time.

Índice de Símbolos

$\mathbb{N}$: conjunto dos números naturais

$\mathbb{Z}$: conjunto dos números inteiros

$\mathbb{Q}$: conjunto dos números racionais

$\mathbb{R}$: conjunto dos números reais

$\mathbb{C}$: conjunto dos números complexos

$\prod$: produtório

$\sum$: somatório

$\det A$: determinante de A

$D(\alpha_1, \ldots, \alpha_n)$: discriminante de uma n-upla

$N(\mathcal{I})$: norma de um ideal $\mathcal{I}$

$\phi(n)$: número de elementos de $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$ ou ϕ de Euler

ξ_n: $e^{2\pi i/n} = cos\frac{2\pi}{n} + isen\frac{2\pi}{n}$, uma raiz n-ésima primitiva da unidade

$Tr_{\mathbb{L}|\mathbb{K}}$: traço em relação à extensão $\mathbb{L}|\mathbb{K}$

$N_{\mathbb{L}|\mathbb{K}}$: norma em relação à extensão $\mathbb{L}|\mathbb{K}$

$\delta_{\mathbb{L}|\mathbb{K}}$: discriminante em relação à extensão $\mathbb{L}|\mathbb{K}$

$\Delta(B|A)$: diferente do anel B sobre A

$< \alpha_1, \ldots, \alpha_n >$: ideal gerado por $\alpha_1, \ldots, \alpha_n$

Sumário

Introdução

Neste trabalho apresentamos um estudo sobre ramificação, discriminante, diferente e também sobre reticulados. Considerando A um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ e B o anel dos inteiros de $\mathbb{L}$ em relação a A, vimos a decomposição de um ideal primo $\mathcal{P}$ não nulo em $\mathbb{L}$, onde consideramos a fatoração do ideal estendido $\mathcal{P}B$ em ideais $\mathcal{Q}_i$ de B. Através do conceito de discriminante, caracterizamos os ideais primos de A que são ramificados em $\mathbb{L}$, e com o conceito de diferente, caracterizamos os ideais primos do anel dos inteiros B que são ramificados em $\mathbb{L}$.

Forney em 1988 deu início a uma teoria que dado um reticulado conseguimos em cima dele obter reticulados equivalentes através de uma multiplicação por escalar, translação e rotação. Usando o diferente, Eva Bayer em 1999 obteve outro conceito de reticulados e por fim utilizando a idéia de Forney, Viterbo em 2004 introduziu alguns métodos de se obter reticulados rotacionados. Deste modo, como uma aplicação da teoria algébrica dos números, apresentamos o conceito de reticulados no $\mathbb{R}^n$, a obtenção de reticulados via o método de Minkowski, onde a imagem do homomorfismo canônico de ideais do anel dos inteiros são reticulados, e também a obtenção de reticulados utilizando discriminante e diferente, via os trabalhos de Eva Bayer e Viterbo.

Desta maneira, este trabalho está dividido nos seguintes capítulos.

No Capítulo 1, abordamos a teoria algébrica dos números, onde vimos os conceitos de elementos inteiros, anel dos inteiros, corpos de números, corpos quadráticos e ciclotômicos, anéis Noetherianos e de Dedekind, norma de um ideal e anéis de frações.

No Capítulo 2, apresentamos os conceitos de ramificação e discriminante, e também a relação entre eles. Apresentamos o Teorema de Kummer, que usamos para a decomposição de um ideal primo em uma extensão. Em seguida, apresentamos um breve estudo sobre reticulados, enfocando os seus principais parâmetros tais como região fundamental e volume. Também apresentamos o homomorfismo canônico de um corpo de números e a obtenção de reticulados via este homomorfismo.

No Capítulo 3, apresentamos os conceitos de diferente e ramificação enfocando suas principais propriedades. Também apresentamos as principais relações entre diferente e ramificação.

No Capítulo 4, apresentamos outros métodos de se obter reticulados de um modo diferente dos obtidos no Capítulo 2, enfocando os trabalhos de Forney e Eva Bayer. Finalizando o Capítulo, apresentamos os códigos de bloco espaço-tempo e exemplos destes códigos, os quais são construídos em uma extensão de $\mathbb{Q}(i)$.

Os anéis considerados neste trabalho são comutativos e com elemento identidade.

Capítulo 1

Teoria dos Números Algébricos

Este capítulo tem como objetivo de introduzir conceitos importantes da Teoria Algébrica dos Números, os quais são utilizados nos capítulos posteriores, tais como elementos inteiros sobre um anel, norma e traço de elementos. Sobre um corpo de números, veremos os corpos quadráticos e corpos ciclotômicos. Para finalizar, veremos as principais propriedades dos anéis Noetherianos, dos anéis de Dedekind e dos anéis de frações. Utilizamos as seguintes referências [1] e [2].

1.1 Elementos inteiros

Nesta seção, apresentamos o conceito de elementos inteiros sobre um anel, onde veremos que o conjunto desses elementos é um anel chamado anel dos inteiros. Também apresentamos um estudo sobre as suas principais propriedades.

Definição 1.1.1 *Sejam $A \subseteq B$ anéis. Dizemos que um elemento $\alpha \in B$ é inteiro sobre A, se α é uma raiz de um polinômio mônico com coeficientes em A, ou seja, se existem $a_0, \cdots, a_{n-1} \in A$, não todos nulos, tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Essa equação é chamada de equação de dependência integral de α.*

Exemplo 1.1.1 *Se $\alpha = \sqrt{5}+\sqrt{7} \in \mathbb{R}$, temos que α é inteiro sobre $\mathbb{Z}$, pois α é raiz do polinômio $x^4 - 24x^2 + 4 \in \mathbb{Z}[x]$.*

Teorema 1.1.1 *Sejam $A \subseteq B$ anéis e $\alpha \in B$. São equivalentes as seguintes afirmações:*
i) α é inteiro sobre A.
ii) O anel $A[\alpha]$ é um A-módulo finitamente gerado.
iii) Existe um subanel R do anel B tal que R é um A-módulo finitamente gerado que contém A e α.

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

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

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

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

ou seja, $\alpha^{j+1} \in \langle 1, \alpha, \cdots, \alpha^{n-1}\rangle$, para todo $j \in \mathbb{N}$. Por outro lado, temos que $\langle 1, \alpha, \cdots, \alpha^{n-1}\rangle \subset A[\alpha]$. Assim, $\langle 1, \alpha, \cdots, \alpha^{n-1}\rangle = A[\alpha]$. Portanto, $A[\alpha]$ é um A-módulo finitamente gerado por $1, \alpha, \cdots, \alpha^{n-1}$. Para ii)$\Rightarrow$ iii) temos que como $\alpha \in A[\alpha]$ e $A \subset A[\alpha]$, é suficiente tomar $R = A[\alpha]$. Finalmente, para iii)$\Rightarrow$ i) seja $R = \langle y_1, \cdots, y_n\rangle$ um A-módulo finitamente gerado tal que $A \subset R \subset B$ e $\alpha \in R$. Assim $R = Ay_1 + \cdots + Ay_n$. Como $\alpha \in R$ temos que $\alpha y_i \in R$, para todo $i = 1, \cdots, n$. Assim, existem $a_{ij} \in A$, com $1 \leq i, j \leq n$, de modo que

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

Logo,

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

Na forma matricial, temos

$$\begin{bmatrix} \alpha - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & \alpha - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & \alpha - a_{nn} \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Seja d o determinante da matriz dos coeficientes deste sistema linear. Pela regra de Cramer, temos que $dy_j = 0$, para $j = 1, \cdots, n$. Como $1 \in R$, temos que $1 = \sum_{j=1}^{n} c_j y_j$, com $c_j \in A$, e assim, $d = d \cdot 1 = d\sum_{j=1}^{n} c_j y_j = \sum_{j=1}^{n} c_j dy_j = 0$. 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 $b_i \in A$. Portanto, α é inteiro sobre A. ∎

Corolário 1.1.1 *Sejam $A \subseteq B$ anéis, e sejam $\alpha_1, \cdots, \alpha_n \in B$. Se α_1 é inteiro sobre A, α_2 é inteiro sobre $A[\alpha_1]$, $\cdots$ e α_n é inteiro sobre $A[\alpha_1, \cdots, \alpha_{n-1}]$, então $A[\alpha_1, \cdots, \alpha_n]$ é um A-módulo finitamente gerado.*

Demonstração: Se α_1 é inteiro sobre A, então pelo Teorema 1.1.1, temos que $A[\alpha_1]$ é um A-módulo finitamente gerado. Assim, por indução, suponhamos que $R = A[\alpha_1, \cdots, \alpha_{n-1}]$ seja um A-módulo finitamente gerado pelos elementos $\{v_1, v_2, \cdots, v_n\}$ e que α_n seja inteiro sobre $R = A[\alpha_1, \cdots, \alpha_{n-1}]$. Pelo Teorema 1.1.1, temos que $R[\alpha_n]$ é um R-módulo finitamente gerado. Assim existe $\{w_1, \cdots, w_s\} \subset R[\alpha_n]$ tal que

$$R[\alpha_n] = A[\alpha_1, \cdots, \alpha_n] = \sum_{i=1}^{s} Rw_i = \sum_{i=1}^{s} \left(\sum_{j=1}^{n} a_j v_j \right) w_i = \sum_{j,i} a_j v_j w_i.$$

Logo, $\{v_j w_i\}$, para $i = 1, \cdots, s$ e $j = 1, \cdots, n$, gera $R[\alpha_n]$ como um A-módulo. Portanto, $A[\alpha_1, \cdots, \alpha_n]$ é um A-módulo finitamente gerado. ∎

Corolário 1.1.2 *Sejam $A \subseteq B$ anéis. Se $\alpha, \beta \in B$ são inteiros sobre A, então $\alpha \pm \beta$, $\alpha\beta$ são inteiros sobre A.*

Demonstração: Temos que $\alpha \pm \beta$, $\alpha\beta$ pertencem a $A[\alpha, \beta]$. Pelo Corolário 1.1.1, temos que $A[\alpha, \beta]$ é um A-módulo finitamente gerado e pelo Teorema 1.1.1, segue que $\alpha \pm \beta$, $\alpha\beta$ são inteiros sobre A. ∎

Definição 1.1.2 *Sejam $A \subseteq B$ anéis. Dizemos que B é inteiro sobre A se todo elemento de B é inteiro sobre A.*

Definição 1.1.3 *Sejam $A \subseteq B$ anéis.*
(1) $\mathcal{O}_B = \{\alpha \in B : \alpha$ é inteiro sobre $A\}$ é chamado anel dos inteiros de A em B, ou fecho inteiro de A em B.
(2) Se A é um domínio e $B = \mathbb{K}$ o corpo de frações de A, dizemos que $\mathcal{O}_B$ é o anel dos inteiros de A em $\mathbb{K}$. Além disso, se $A = \mathcal{O}_B$ dizemos que A é um anel integralmente fechado.

Proposição 1.1.1 *Se $A \subseteq B$ são anéis, então $A \subseteq \mathcal{O}_B \subseteq B$.*

Demonstração: Pelo Corolário 1.1.2, temos que $\mathcal{O}_B$ é um subanel de B . Agora, se $\alpha \in A$, então α é raiz do polinômio $p(x) = x - \alpha$, o qual tem coeficientes em A, e assim $\alpha \in \mathcal{O}_B$. Portanto, $A \subseteq \mathcal{O}_B \subseteq B$. ∎

Proposição 1.1.2 *Sejam $A \subseteq B \subseteq R$ anéis. Assim, R é inteiro sobre A se, e somente se, R é inteiro sobre B e B é inteiro sobre A.*

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

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

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

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

Seja $C = A[b_0, \cdots, b_{n-1}]$. Logo, α é inteiro sobre C. Como B é inteiro sobre A, segue que os $b_i's$ são inteiros sobre A. Pelo Corolário 1.1.1, segue que $C[\alpha] = A[b_0, \cdots, b_{n-1}, \alpha]$ é um A-módulo finitamente gerado. Pelo Teorema 1.1.1, temos que α é inteiro sobre A. Portanto, R é inteiro sobre A. ∎

Proposição 1.1.3 *Sejam $A \subseteq B$ anéis, onde B é um domínio e inteiro sobre A. Então A é um corpo se, e somente se, B é um corpo.*

Demonstração: Suponhamos que A é um corpo. Seja $\alpha \in B$, $\alpha \neq 0$. Logo, α é inteiro sobre A e pelo Teorema 1.1.1, segue que $A[\alpha]$ é um espaço vetorial finitamente gerado sobre A. Seja $\varphi : A[\alpha] \longrightarrow A[\alpha]$ uma aplicação definida por $\varphi(b) = b\alpha$, $\forall b \in A[\alpha]$. Temos que φ é A-linear e bijetora, uma vez que $\forall b_1, b_2 \in A[\alpha]$, temos que

$$\varphi(b_1 + b_2) = (b_1 + b_2)\alpha = b_1\alpha + b_2\alpha = \varphi(b_1) + \varphi(b_2)$$

$$\varphi(\gamma b_1) = \gamma b_1 \alpha = \gamma \varphi(b_1).$$

Se $\varphi(b) = b\alpha = 0$ temos que $b = 0$, uma vez que B é um domínio. Portanto, φ é injetora. Como a dimensão de $A[\alpha]$ sobre A é finita segue que φ é bijetora. Assim, como $1 \in A[\alpha]$, existe $b' \in A[\alpha]$ tal que $b'\alpha = 1$. Portanto, B é um corpo. Por outro lado, suponhamos que B é um corpo. Seja $\alpha \in A$. Assim $\alpha \in A \subset B$, e portanto $\alpha^{-1} \in B$. Como B é inteiro sobre A, segue que

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

com $a_i \in A$, não todos nulos. Multiplicando por α^{n-1}, temos

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

ou seja,

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

Assim, $\alpha^{-1} \in A$. Portanto, A é um corpo. ∎

Proposição 1.1.4 *Se A é um domínio, então $\mathcal{O}_B$ é um anel integralmente fechado.*

Demonstração: Seja $\mathbb{K}$ o corpo de frações de A. Assim, $\mathbb{K}$ também é o corpo de frações de $\mathcal{O}_B$. Seja $\alpha \in \mathbb{K}$ inteiro sobre $\mathcal{O}_B$. Como $\mathcal{O}_B$ é inteiro sobre A segue da Proposição 1.1.2 que α é inteiro sobre A, e portanto $\alpha \in \mathcal{O}_B$. Assim, $\mathcal{O}_B$ é um anel integralmente fechado. ∎

Proposição 1.1.5 *Se A é um domínio principal então A é um anel integralmente fechado.*

Demonstração: Seja $\mathbb{K}$ o corpo de frações de A. Seja $\alpha \in \mathbb{K}$ inteiro sobre A tal que $\alpha = \frac{a}{b}$, com $a, b \in A$ e $mdc(a, b) = 1$. Então existem $a_i \in A$, $i = 1, \cdots, n-1$, 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

$$a^n + a_{n-1}a^{n-1}b + \cdots + a_0b^n = 0,$$

isto é,

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

Logo b divide a^n e como $mdc(a, b) = 1$, segue que b divide a, o que implica que $a = bc$. Usando novamente o fato de $mdc(a, b) = 1$, temos que existem $x_0, y_0 \in A$ tal que $ax_0 + by_0 = 1$. Assim, $bcx_0 + by_0 = 1$ o que implica que $b(cx_0 + y_0) = 1$. Assim, b é inversível em A e $\alpha = ab^{-1} \in A$. Portanto, A integralmente fechado. ∎

1.2 Norma e traço

Nesta seção, apresentamos os conceitos de norma e traço de elementos. Também apresentamos que o anel dos inteiros é um A-módulo livre, onde A é um anel principal.

Sejam $A \subseteq B$ anéis, onde B é um A-módulo livre de posto finito n. Seja $\{e_1, \cdots, e_n\}$ uma base de B sobre A e seja $\theta : B \longrightarrow B$ um homomorfismo. Assim,

$$\theta(e_1) = a_{11}e_1 + a_{12}e_2 + \cdots + a_{1n}e_n$$

$$\theta(e_2) = a_{21}e_1 + a_{22}e_2 + \cdots + a_{2n}e_n$$

$$\vdots$$

$$\theta(e_n) = a_{n1}e_1 + a_{n2}e_2 + \cdots + a_{nn}e_n,$$

com $a_{ij} \in A$, onde $1 \leq i, j \leq n$. Assim, $\begin{bmatrix} \theta(e_1) \\ \vdots \\ \theta(e_n) \end{bmatrix} = [a_{ij}] \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix}$. Definimos o traço de θ por $Tr_{B|A}(\theta) = \sum_{i=1}^{n} a_{ii}$, a norma de θ por $N_{B|A}(\theta) = \det(a_{ij})$ e o polinômio característico de θ por $m_{B|A}(x) = \det(xI - \theta)$. Assim, temos que:

$$Tr_{B|A}(\theta + \theta') = Tr_{B|A}(\theta) + Tr_{B|A}(\theta')$$

$$det(\theta\theta') = det(\theta)det(\theta')$$

$$e$$

$$m_{B|A}(x) = det(xI - \theta) = x^n - (Tr_{B|A}(\theta))x^{n-1} + \cdots + (-1)^n det(\theta).$$

Definição 1.2.1 *Seja o endomorfismo $\theta_\alpha : B \longrightarrow B$ definido por $\theta_\alpha(x) = \alpha x$, com $\alpha \in B$. O traço de $\alpha \in B$ é definido por $Tr_{B|A}(\alpha) = Tr_{B|A}(\theta_\alpha)$, a norma de $\alpha \in B$ por $N_{B|A}(\alpha) = det(\theta_\alpha)$ e o polinômio característico de α por $m_{B|A}(x) = det(xI - \theta_\alpha)$.*

Observação 1.2.1 *Se $\mathbb{K} \subseteq \mathbb{L}$ extensões de corpos, e se $\mathcal{O}_\mathbb{K}$ e $\mathcal{O}_\mathbb{L}$ os anéis dos inteiros de $\mathbb{K}$ e $\mathbb{L}$, respectivamente, então usamos a notação $Tr_{\mathbb{L}|\mathbb{K}}(\alpha)$ ou $Tr_{\mathbb{O}_\mathbb{L}|\mathbb{O}_\mathbb{K}}(\alpha)$, $N_{\mathbb{L}|\mathbb{K}}(\alpha)$ ou $N_{\mathbb{O}_\mathbb{L}|\mathbb{O}_\mathbb{K}}(\alpha)$ com $\alpha \in \mathbb{L}$.*

Exemplo 1.2.1 *Seja $\mathbb{L} = \mathbb{Q}(\sqrt{-1})$. Sejam $\alpha = 3 + \sqrt{-1} \in \mathbb{Q}(\sqrt{-1})$ e $m_\alpha(x) = x^2 - 6x + 10$ o polinômio minimal de α sobre $\mathbb{Q}$. Então $T_{\mathbb{L}|\mathbb{Q}}(\alpha) = 6$ e $N_{\mathbb{L}|\mathbb{Q}}(\alpha) = 10$.*

Sejam $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L}$ extensões de corpos finitos. Sejam $\alpha, \alpha^{'} \in \mathbb{L}$ e $a \in \mathbb{K}$. Então vale 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. $N_{\mathbb{L}|\mathbb{K}}(\alpha\alpha^{'}) = N_{\mathbb{L}|\mathbb{K}}(\alpha)N_{\mathbb{L}|\mathbb{K}}(\alpha^{'})$

se $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ são extensões de corpos temos que

7. $N_{\mathbb{L}|\mathbb{K}}(\alpha) = N_{\mathbb{M}|\mathbb{K}}(N_{\mathbb{L}|\mathbb{M}}(\alpha))$
8. $T_{\mathbb{L}|\mathbb{K}}(\alpha) = T_{\mathbb{M}|\mathbb{K}}(T_{\mathbb{L}|\mathbb{M}}(\alpha))$.

Proposição 1.2.1 *Seja $\mathbb{K}$ um corpo de característica 0 ou um corpo finito. Sejam $\mathbb{L}$ uma extensão algébrica de grau n de $\mathbb{K}$, α um elemento de $\mathbb{L}$ e $\alpha_1, \cdots, \alpha_n$ as raízes do polinômio minimal de α sobre $\mathbb{K}$. Então $Tr_{\mathbb{L}|\mathbb{K}}(\alpha) = \alpha_1 + \cdots + \alpha_n$, $N_{\mathbb{L}|\mathbb{K}}(\alpha) = \alpha_1 \cdots \alpha_n$ e o polinômio característico de α é $m_{\mathbb{L}|\mathbb{K}}(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$.*

Demonstração: Primeiramente faremos a demonstração para o caso em que α é um elemento primitivo de $\mathbb{L}$ sobre $\mathbb{K}$, ou seja, $\mathbb{L} = \mathbb{K}[\alpha]$. Seja $f(x)$ o polinômio minimal de α sobre $\mathbb{K}$. Então $\mathbb{L}$ é $\mathbb{K}$-isomorfo a $\mathbb{K}[x]/\langle f(x)\rangle$ e $\{1, \alpha, \cdots, \alpha^{n-1}\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Tomando $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, com $a_i \in \mathbb{K}$, temos que a matriz do endomorfismo θ_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, $\det(xI - \theta_\alpha)$ é o determinante da matriz

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

Calculando o determinante da matriz acima, obtemos o polinômio característico de α, o qual é igual a $f(x)$, o polinômio minimal de α. Por definição,

$$m_{\mathbb{L}|\mathbb{K}}(x) = \det(xI - \theta_\alpha(x)) = \det(xI_n - M) = x^n - (Tr_{\mathbb{L}|\mathbb{K}}(\theta_\alpha))x^{n-1} + \cdots + (-1)^n \det(\theta_\alpha).$$

Como α é primitivo temos que

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

Logo, $Tr_{\mathbb{L}|\mathbb{K}}(\theta_\alpha) = Tr_{\mathbb{L}|\mathbb{K}}(\alpha) = \sum_{i=1}^{n} \alpha_i$ e $N_{\mathbb{L}|\mathbb{K}}(\theta_\alpha) = N_{\mathbb{L}|\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \alpha_i$. Para o caso geral, seja $r = [\mathbb{L} : \mathbb{K}[\alpha]]$. Assim, é suficiente mostrarmos que o polinômio característico $m_{\mathbb{L}|\mathbb{K}}(x)$ 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 $\{y_1, \cdots, y_q\}$ uma base de $\mathbb{K}[\alpha]$ sobre $\mathbb{K}$ e seja $\{z_1, \cdots, z_r\}$ 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 $\{y_1, \cdots, y_q\}$. Assim, $\alpha y_i = \sum_h (a_{ih}) y_h$. Então, $\alpha(y_i z_j) = \left(\sum_h a_{ih} y_h\right) z_j = \sum_h a_{ih}(y_h z_j)$. Logo,

$$\begin{cases} \alpha y_1 z_1 = a_{11} y_1 z_1 + a_{12} y_2 z_1 + \cdots + a_{1q} y_q z_1 \\ \alpha y_2 z_1 = a_{21} y_1 z_1 + a_{22} y_2 z_1 + \cdots + a_{2q} y_q z_1 \\ \quad \vdots \\ \alpha y_q z_1 = a_{q1} y_1 z_1 + a_{q2} y_2 z_1 + \cdots + a_{qq} y_q z_1. \end{cases}$$

Ordenamos a base $\{y_i z_j\}$, de $\mathbb{L}$ sobre $\mathbb{K}$, de modo que a matriz do endomorfismo seja da seguinte forma

$$M_1 = \begin{bmatrix} M & 0 & \cdots & 0 & 0 \\ 0 & M & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & M \end{bmatrix},$$

isto é, M repete r-vezes na diagonal como blocos na matriz M_1. A matriz $xI_n - M_1$, consiste de r-blocos diagonais, onde cada um tem a forma $xI_q - M$, e assim, $\det(xI_n - M_1) = \det(xI_q - M)^r$. Consequentemente, $m_{\mathbb{L}|\mathbb{K}}(x) = det(xI_n - M)$ e $det(xI_q - M_1)$ é o polinômio característico de α sobre $\mathbb{K}$, de acordo com a primeira parte da demonstração. ∎

Observação 1.2.2 *Segue pela Proposição 1.2.1, que* $Tr_{\mathbb{L}|\mathbb{K}}(\alpha) = rTr_{\mathbb{K}[\alpha]|\mathbb{K}}(\alpha)$, $N_{\mathbb{L}|\mathbb{K}}(\alpha) = (N_{\mathbb{K}[\alpha]|\mathbb{K}}(\alpha))^r$ *e* $m_{\mathbb{L}|\mathbb{K}}(x) = (m_{\mathbb{K}[\alpha]|\mathbb{K}}(x))^r$.

Exemplo 1.2.2 *Sejam* $\mathbb{L} = \mathbb{Q}(\sqrt{5}, \sqrt{-1})$, $\mathbb{K} = \mathbb{Q}(\sqrt{-1})$ *e* $\mathbb{F} = \mathbb{Q}$. *Sejam* $\alpha = 3 + \sqrt{-1}$ *e* $r = [\mathbb{L} : \mathbb{K}]$*=2. Pelo Exemplo 1.2.1, temos que* $N_{\mathbb{K}|\mathbb{F}}(\alpha) = 10$ *e* $T_{\mathbb{K}|\mathbb{F}}(\alpha) = 6$. *Assim, pela Observação 1.2.2, temos que* $N_{\mathbb{L}|\mathbb{F}}(\alpha) = (N_{\mathbb{K}|\mathbb{F}}(\alpha))^2 = 10^2 = 100$ *e* $T_{\mathbb{L}|\mathbb{F}}(\alpha) = 2(T_{\mathbb{K}|\mathbb{F}}(\alpha)) = 2 \cdot 6 = 12$.

Proposição 1.2.2 *Sejam* A *um domínio,* $\mathbb{K}$ *seu corpo de frações,* $\mathbb{K} \subseteq \mathbb{L}$ *uma extensão finita de grau* n *e* $\alpha \in \mathbb{L}$ *um elemento inteiro sobre* A. *Então os coeficientes do polinômio característico de* α *são inteiros sobre* A. *Em particular,* $Tr_{\mathbb{L}|\mathbb{K}}(\alpha)$ *e* $N_{\mathbb{L}|\mathbb{K}}(\alpha)$ *são inteiros sobre* A.

Demonstração: Pela Proposição 1.2.1, temos que o polinômio característico de α é $m_{\mathbb{L}|\mathbb{K}}(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$. Como os coeficientes de $m_{\mathbb{L}|\mathbb{K}}(x)$ são somas e produtos dos α_i, é suficiente mostrar que os α_i são inteiros sobre A. Pela Teoria de Galois, temos que existe um $\mathbb{K}$-homomorfismo $\sigma_i : \mathbb{K}[\alpha] \longrightarrow \mathbb{K}[\alpha_i]$, definido por $\sigma_i(\alpha) = \alpha_i$, para todo $i = 1, \cdots, n$. Como α é inteiro sobre A, então

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

com $a_i \in A$, não todos nulos. 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 A. ∎

Corolário 1.2.1 *Se* A *é um anel integralmente fechado, então os coeficientes do polinômio característico de* α, $Tr_{\mathbb{L}|\mathbb{K}}(\alpha)$ *e* $N_{\mathbb{L}|\mathbb{K}}(\alpha)$ *são elementos de* A.

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

Proposição 1.2.3 *Sejam* A *um anel integralmente fechado,* $\mathbb{K}$ *seu corpo de frações,* $\mathbb{L}$ *uma extensão finita de* $\mathbb{K}$ *de grau* n *e* $\mathcal{O}_{\mathbb{L}}$ *o anel dos inteiros de* A *em* $\mathbb{L}$. *Seja* $\{\alpha_1, \cdots, \alpha_n\}$ *uma base de* $\mathbb{L}$ *sobre* $\mathbb{K}$ *onde* $\det(Tr_{\mathbb{L}|\mathbb{K}}(\alpha_i\alpha_j)) \neq 0$. *Seja* $\alpha \in \mathbb{L}$. *Se* $Tr_{\mathbb{L}|\mathbb{K}}(\alpha\beta) = 0$ *para todo* $\beta \in \mathbb{L}$, *então* $\alpha = 0$.

Demonstração: Como $\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$, onde $a_i \in \mathbb{K}$, para $i = 1, \cdots, n$, é suficiente mostrar que se $Tr(\alpha\alpha_j) = 0$, para cada $j = 1, \cdots, n$, então $\alpha = 0$. Assim, para cada $j = 1, \cdots, n$, temos que

$$0 = Tr_{\mathbb{L}|\mathbb{K}}(\alpha\alpha_j) = a_1 Tr_{\mathbb{L}|\mathbb{K}}(\alpha_1\alpha_j) + a_2 Tr_{\mathbb{L}|\mathbb{K}}(\alpha_2\alpha_j) + \cdots + a_n Tr_{\mathbb{L}|\mathbb{K}}(\alpha_n\alpha_j).$$

Na forma matricial, temos que

$$\begin{bmatrix} Tr_{\mathbb{L}|\mathbb{K}}(\alpha_1\alpha_1) & Tr_{\mathbb{L}|\mathbb{K}}(\alpha_2\alpha_1) & \cdots & Tr_{\mathbb{L}|\mathbb{K}}(\alpha_n\alpha_1) \\ Tr_{\mathbb{L}|\mathbb{K}}(\alpha_1\alpha_2) & Tr_{\mathbb{L}|\mathbb{K}}(\alpha_2\alpha_2) & \cdots & Tr_{\mathbb{L}|\mathbb{K}}(\alpha_n\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ Tr_{\mathbb{L}|\mathbb{K}}(\alpha_1\alpha_n) & Tr_{\mathbb{L}|\mathbb{K}}(\alpha_2\alpha_n) & \cdots & Tr_{\mathbb{L}|\mathbb{K}}(\alpha_n\alpha_n) \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Como $\det(Tr_{\mathbb{L}|\mathbb{K}}(\alpha_i\alpha_j)) \neq 0$ segue que $a_1 = a_2 = \cdots = a_n = 0$. Portanto, $\alpha = 0$. ∎

Corolário 1.2.2 *Com as mesmas hipóteses da Proposição 1.2.3, segue que a aplicação* $\rho : \mathbb{L} \longrightarrow Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{K})$ *definida por* $\rho(\alpha) = S_\alpha$, *onde* $S_\alpha(\beta) = Tr_{\mathbb{L}|\mathbb{K}}(\alpha\beta)$, *com* $\beta \in \mathbb{L}$ *é um isomorfismo.*

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

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

e

$$\rho(a\alpha)(\beta) = S_{a\alpha}(\beta) = Tr_{\mathbb{L}|\mathbb{K}}(a\alpha\beta) = aTr_{\mathbb{L}|\mathbb{K}}(\alpha\beta) = aS_\alpha(\beta) = a\rho(\alpha)(\beta)$$

para todo $\beta \in \mathbb{L}$. Agora, seja $\alpha \in \mathbb{L}$ tal que $\rho(\alpha) = 0$. Então, $\rho(\alpha)(\beta)$=$S_\alpha(\beta) = Tr_{\mathbb{L}|\mathbb{K}}(\alpha\beta) = 0$, $\forall\beta \in \mathbb{L}$. Pela Proposição 1.2.3, segue 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. ∎

Teorema 1.2.1 *Sejam A 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 A em* $\mathbb{L}$. *Então* $\mathcal{O}_\mathbb{L}$ *é um A-submódulo de um A-módulo livre.*

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

$$a_{n_i}\alpha_i^{n_i} + a_{n_i-1}\alpha_i^{n_i-1} + \cdots + a_{0,i} = 0.$$

Supondo que $a_{n_i} \neq 0$ e multiplicando esta equação por $a_{n_i}^{n_i-1}$, temos que $a_{n_i}\alpha_i$ é inteiro sobre A, uma vez que

$$a_{n_i}^{n_i-1}(a_{n_i}\alpha_i^{n_i} + \cdots + a_{0,i}) = (a_{n_i}\alpha_i)^{n_i} + a_{n_i-1}(a_{n_i}\alpha_i)^{n_i-1} + \cdots + a_{n_i}^{n_i-1}a_{0,i} = 0.$$

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

$$b_1a_{n_i}\alpha_1 + b_2a_{n_i}\alpha_2 + \cdots + b_na_{n_i}\alpha_n = 0.$$

Como $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ segue que $b_ia_n = 0$ e portanto $b_i = 0$ para $i = 1, \cdots, n$. Portanto, $\{z_1, \cdots, z_n\}$ é linearmente independente e como possui n elementos segue que é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Pelo Corolário 1.2.2 existe uma base dual $\{y_1, \cdots, y_n\}$ tal que

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

Agora, se $\alpha \in \mathcal{O}_{\mathbb{L}}$ então $\alpha z_i \in \mathcal{O}_{\mathbb{L}}$, para $i = 1, \cdots, n$. Pelo Corolário 1.2.1 segue que $Tr_{\mathbb{L}|\mathbb{K}}(\alpha z_i) \in A$, para $i = 1, \cdots, n$. Como $\alpha = c_1y_1 + \cdots + c_ny_n$, com $c_i \in \mathbb{K}$, para $i = 1, \cdots, n$, segue que $Tr_{\mathbb{L}|\mathbb{K}}(\alpha z_i) = c_i \in A$, para $i = 1, \cdots, n$. Portanto, $\mathcal{O}_{\mathbb{L}}$ é um submódulo de um A-módulo livre gerado por $\{z_1, \cdots, z_n\}$. ∎

Corolário 1.2.3 *Com as mesmas hipóteses do Teorema* 1.2.1*, se A é um anel principal, então $\mathcal{O}_{\mathbb{L}}$ é um A-módulo livre de posto n.*

Demonstração: Se A é principal temos que um submódulo de um A-módulo livre é livre de posto menor ou igual a n. Pelo Teorema 1.2.1, $\mathcal{O}_{\mathbb{L}}$ contém uma base de n elementos de $\mathbb{L}$ sobre $\mathbb{K}$. Logo, $\mathcal{O}_{\mathbb{L}}$ tem posto n. ∎

Corolário 1.2.4 *Com as mesmas hipóteses do Teorema* 1.2.1*, se A é um anel principal e se $\mathcal{A} \subseteq \mathcal{O}_{\mathbb{L}}$ é um ideal, então $\mathcal{A}$ é um A-módulo livre de posto n.*

Demonstração: Sejam $\{e_1, \cdots, e_n\}$ uma base de $\mathcal{O}_{\mathbb{L}}$ e $\alpha \in \mathcal{A}$, $\alpha \neq 0$. Assim, $\alpha e_1, \cdots, \alpha e_n \in \mathcal{A}$ e são linearmente independente sobre A, uma vez que se $\alpha_1\alpha e_1 + \cdots + \alpha_n\alpha e_n = 0$, com $\alpha_i \in A$, para $i = 1, \cdots, n$, então $\alpha_i\alpha = 0$ para $i = 1, \cdots, n$, e como A é um domínio segue que $\alpha_i = 0$, para $i = 1, \cdots, n$. ∎

Teorema 1.2.2 *Sejam A um anel e $\mathbb{K} \subseteq A$ um corpo tal que A é um espaço vetorial de dimensão finita sobre $\mathbb{K}$. Seja $\theta : A \longrightarrow A$ uma transformação $\mathbb{K}$-linear. Seja uma cadeia estritamente decrescente de subespaços de A, de modo que, $A = A_0 \supset A_1 \supset A_2 \supset \cdots \supset A_k = 0$ e que $\theta(A_i) \subseteq A_i$, para $i = 1, \cdots, k$. Então $m_{A|\mathbb{K}}(\theta) = \prod_{i=1}^{k} m_{(A_{i-1}/A_i|\mathbb{K})}(\theta_i)$, onde $\theta_i = A_{i-1}/A_i \longrightarrow A_{i-1}/A_i$, para $i = 1, \cdots, k$, é uma transformação linear induzida por θ.*

Demonstração: Os elementos do $\mathbb{K}$-espaço vetorial A_{i-1}/A_i são as classes $z + A_i$, onde $z \in A_{i-1}$, para $i = 1, \cdots, k$. Temos que θ induz uma transformação linear $\theta_i : A_{i-1}/A_i \longrightarrow A_{i-1}/A_i$ definida por $\theta_i(z + A_i) = \theta(z) + A_i$, para $z \in A_{i-1}$. Por hipótese temos que A_j são subespaços,e assim cada θ_i está bem definida. Para cada índice $i = 1, \cdots, k$, seja $B_i = \{z_{i1}, \cdots, z_{im_i}\}$ um conjunto de elementos de A_{i-1} tal que o conjunto das classes $\{z_{i1} + A_i, \cdots, z_{im_i} + A_i\}$ forma uma base do espaço vetorial A_{i-1}/A_i. Então para cada $i = 1, \cdots, k$, temos que $B_i \cup B_{i+1} \cup \cdots \cup B_k$ constitui uma base do $\mathbb{K}$-espaço vetorial A_{i-1}. Em particular, $B = B_1 \cup B_2 \cup \cdots \cup B_k$ é uma base do $\mathbb{K}$-espaço vetorial A. Seja a matriz $M(\theta)$ com relação a base B. Esta matriz pode ser expressa em termos das matrizes $M(\theta_i)$ com relação a B_i, da seguinte forma:

$$M(\theta) = \begin{pmatrix} M(\theta_1) & 0 & \cdots & 0 \\ M_{21} & M(\theta_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ M_{k1} & M_{k2} & \cdots & M(\theta_k) \end{pmatrix},$$

onde $M_{ij}(i > j)$ são matrizes com coeficientes em $\mathbb{K}$, pois como $\theta(z_{ij}) \in A_{i-1}$ então $\theta(z_{ij})$ pode ser expresso em termos da base $B_i \cup B_{i+1} \cup \cdots \cup B_k$ uma vez que

$$\theta(z_{ij}) = \sum_{h=1}^{m_i} a_{ih_j} z_{ih} + \sum_{h=1}^{m_i} a_{i+1,h_j} z_{i+1,h} + \cdots + \sum_{h=1}^{m_i} a_{kh_j} z_{kh},$$

onde coeficientes $a_{th_j} \in \mathbb{K}$. Assim, $\theta_i(z_{ij} + A_i) = \sum_{h=1}^{m_i} a_{ih_j}(z_{ih} + A_i) + A_i = \sum_{h=1}^{m_i} a_{ih_j} z_{ih} + A_i$. Assim, o polinômio característico, das transformações lineares $\theta, \theta_1, \theta_2, \cdots, \theta_k$ é dado por

$$m_{A|\mathbb{K}}(\theta) = \prod_{i=1}^{k} m_{(A_{i-1}/A_i|\mathbb{K})}(\theta_i). \qquad \blacksquare$$

Teorema 1.2.3 *Sejam A um anel e $\mathbb{K} \subseteq A$ um corpo tal que A é um espaço vetorial de dimensão finita sobre $\mathbb{K}$. Seja $\theta : A \longrightarrow A$ uma transformação $\mathbb{K}$-linear. Seja uma cadeia estritamente decrescente de subespaços de A, $A = A_0 \supset A_1 \supset A_2 \supset \cdots \supset A_k = 0$ tal que $\theta(A_i) \subseteq A_i$, para $i = 1, \cdots, k$ e suponhamos que*

1) A_i é um ideal de A, para $i = 1, \cdots, k$.

2) Para todo $i = 1, \cdots, k$ não existe ideal $\mathcal{I}$ de A tal que $A_{i-1} \supset \mathcal{I} \supset A_i$.

3) Se $y \in A_1$ e $z \in A_{i-1}$ então $yz \in A_i$, para $i = 1, \cdots, k$.

4) Se $y, z \in A, yz \in A_i$ e $y \notin A_1$ então $z \in A_i$, para $i = 1, \cdots, k$.

Se $x \in A$ e $\theta = \theta(x)$ então para $i = 1, \cdots, k$, temos que $m_{(A_{i-1}/A_i|\mathbb{K})}(\theta_i) = m_{A|\mathbb{K}}(\theta)$ e $m_{A|\mathbb{K}}(\theta) = [m_{(A/A_1|\mathbb{K})}(\theta_1)]^k$.

Demonstração: Temos que para cada $i = 1, \cdots, k$, existe um isomorfismo de A-módulos $\lambda_i : A_{i-1}/A_i \longrightarrow A/A_1$ tal que $\theta_1 \circ \lambda_i = \lambda_i \circ \theta_i$, uma vez que se $u \in A_{i-1}$ e $u \notin A_i$, então $A_i \subset A_i + Au \subset A_{i-1}$. Por 1) e 2) temos que $A_{i-1} = A_i + Au$. Dado um elemento $y + A_i \in A_{i-1}/A_i$, seja $y = y^{'}u + y^{''}$, com $y^{'} \in A$ e $y^{''} \in A_i$. Definimos $\lambda_i(y + A_i) = y^{'} + A_1$. A função $\lambda_i : A_{i-1}/A_i \longrightarrow A/A_1$ esta bem definida, uma vez que se $y + A_i = z + A_i$ com $z \in A_{i-1}$ e $z = z^{'}u + z^{''}$, $z^{'} \in A$, $z^{''} \in A_i$, então

$$y - z = (y^{'} - z^{'})u + (y^{''} - z^{''}).$$

Assim, $(y^{'} - z^{'})u \in A_i$. Como $u \notin A_i$, segue de 4) que $y^{'} - z^{'} \in A_1$ e assim, $y^{'} + A_1 = z^{'} + A_1$. Temos também que λ_i é um homomorfismo de A-módulos. Além disso, se $y = y^{'}u + y^{''}$, com $y^{'} \in A_1$ então por 3) temos que $y \in A_i$. Portanto se $\lambda_i(y + A_i) = \bar{0} \in A/A_1$ então $y + A_i = \bar{0} \in A_{i-1}/A_i$, e assim é injetora. Agora para provarmos que λ_i é sobrejetora, seja $y^{'} \in A$. Assim, $y = y^{'}u \in A_{i-1}$ é tal que $\lambda_i(y + A_i) = y^{'} + A_1$. Portanto, λ_i é um isomorfismo. Falta mostrarmos que $\theta_1 \circ \lambda_i = \lambda_i \circ \theta_i$. Seja $y \in A_{i-1}$. Se $y = y^{'}u + y^{''}$, com $y^{'} \in A$ e $y^{''} \in A_i$, então $xy = (xy^{'})u + xy^{''}$, com $xy^{'} \in A$, $xy^{''} \in A_i$. Assim,

$$\begin{aligned} \theta_1(\lambda_i(y + A_i)) &= \theta_1(y^{'} + A_1) = \theta(y^{'}) + A_1 \\ &= xy^{'} + A_1 = \lambda_i(xy + A_i) = \lambda_i(\theta(xy) + A_i) = \lambda_i(\theta_i(y + A_i)). \end{aligned}$$

Pela demonstração do Teorema 1.2.2, temos que se $\bar{B}$ é uma base do $\mathbb{K}$-espaço vetorial A_{i-1}/A_i e $\lambda_i(\bar{B}_i)$ é a base correspondente do espaço vetorial isomorfo a A/A_1 então as matrizes de θ_i com relação $\bar{B}_i$ e de θ_1 com relação a $\lambda_i(\bar{B}_i)$ são as mesmas. Assim, $m_{(A_{i-1}/A_i|\mathbb{K})}(\theta_i) = m_{A|\mathbb{K}}(\theta)$ e portanto $m_{A|\mathbb{K}}(\theta) = [m_{(A/A_1|\mathbb{K})}(\theta_1)]^k$. ∎

Proposição 1.2.4 *Sejam A um anel e B um A-módulo livre. Sejam $\psi : B \longrightarrow \bar{B}$ um homomorfismo de B em um anel $\bar{B}$ e que $\psi(A) = \bar{A}$. Suponha que existe uma base $\{z_1, \cdots, z_n\}$ do A-módulo B tal que $\{\bar{z}_1, \cdots, \bar{z}_n\}$ é uma base do $\bar{A}$-módulo $\bar{B}$ onde $\bar{z} = \psi(z), \forall z \in B$. Se $x \in B$ então $\psi(m_{B|A}(x)) = m_{\bar{B}|\bar{A}}(\bar{x})$, $\psi(Tr_{B|A}(x)) = Tr_{\bar{B}|\bar{A}}(\bar{x})$ e $\psi(N_{B|A}(x)) = N_{\bar{B}|\bar{A}}(\bar{x})$.*

Demonstração: Se $x \in B$ então $xz_j = \sum_{i=1}^{n} a_{ij}z_i$, com $j = 1, \cdots, n$ e $a_{ij} \in A$. Logo $\bar{x}\bar{z}_j = \sum_{i=1}^{n} \overline{a_{ij}z_i}$, para $j = 1, \cdots, n$. Sejam as matrizes $M = (a_{ij})$, com relação a base $\{z_1, \cdots, z_n\}$, e $\overline{M} = \overline{(a_{ij})}$ com relação a base $\{\bar{z}_1, \cdots, \bar{z}_n\}$. Aplicando ψ aos coeficientes do polinômio característico $m_{B|A}(x) = \det(xI - (a_{ij}))$, obtemos $\det(xI - \overline{(a_{ij})}) = m_{\bar{B}|\bar{A}}(\bar{x})$. O traço e a

norma segue analogamente, pois $Tr_{B|A}(x) = \sum_{i=1}^{n} a_{ii}$ e assim se aplicarmos ψ temos que

$$\psi(Tr_{B|A}(x)) = \psi\left(\sum_{i=1}^{n} a_{ii}\right) = \sum_{i=1}^{n} \psi(a_{ii}) = \sum_{i=1}^{n} \overline{a_{ii}} = Tr_{\bar{B}|\bar{A}}(\bar{x})$$

e como $N_{B|A}(x) = \det(a_{ij})$ então $\psi(N_{B|A}(x)) = \psi(\det(a_{ij})) = \det \psi(a_{ij}) = \det \overline{(a_{ij})} = N_{\bar{B}|\bar{A}}(\bar{x})$, o que demonstra a Proposição. ∎

1.3 Corpos quadráticos

Nesta seção apresentamos o estudo dos corpos quadráticos juntamente com seu anel de inteiros.

Definição 1.3.1 *Um corpo de números é uma extensão finita de $\mathbb{Q}$. Um corpo quadrático é uma extensão de grau 2 de $\mathbb{Q}$.*

Proposição 1.3.1 *Um corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados.*

Demonstração: Se $\mathbb{K}$ é um corpo quadrático, então todo elemento $\alpha \in \mathbb{K}$ tal que $\alpha \notin \mathbb{Q}$ é de grau 2 sobre $\mathbb{Q}$. Pelo Teorema do Elemento Primitivo temos que $\mathbb{K} = \mathbb{Q}(\alpha)$. Seja $m_\alpha(x) = x^2 + bx + c$, o polinômio minimal de $\alpha \in \mathbb{K} = \mathbb{Q}(\alpha)$. 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 $u, v \in \mathbb{Z}$, temos que $\mathbb{Q}(\sqrt{b^2 - 4c}) = \mathbb{Q}(\sqrt{uv})$. Como $uv \in \mathbb{Z}$, temos que uv é fatorado em produtos de primos. Assim, $\mathbb{Q}(\sqrt{uv}) = \mathbb{Q}(\sqrt{d})$, onde d é inteiro livre de quadrados. ∎

Observação 1.3.1 *O elemento $\sqrt{d}$ é uma raiz do polinômio irredutível $x^2 - d$. O conjugado de $\sqrt{d}$ é -$\sqrt{d}$, ou seja, existe um automorfismo $\sigma : \mathbb{Q}(\sqrt{d}) \longrightarrow \mathbb{Q}(\sqrt{d})$ tal que $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$.*

Lema 1.3.1 *Seja $\mathcal{O}_\mathbb{K}$ o anel dos inteiros de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com d livre de quadrados, sobre $\mathbb{Z}$. Se $\alpha = a + b\sqrt{d} \in \mathcal{O}_\mathbb{K}$, então $2a \in \mathbb{Z}$ e $2b \in \mathbb{Z}$.*

Demonstração: Pela Observação 1.3.1, segue que existe um automorfismo σ de $\mathbb{K}$ tal que $\sigma(\alpha) = \sigma(a + b\sqrt{d}) = a - b\sqrt{d}$. Como $\sigma(\alpha)$ também é raiz da mesma equação de dependência integral de α, segue que $\sigma(\alpha) \in \mathcal{O}_\mathbb{K}$. Como α e $\sigma(\alpha) \in \mathcal{O}_\mathbb{K}$, pelo Corolário 1.1.2, temos que $\alpha + \sigma(\alpha) \in \mathcal{O}_\mathbb{K}$ e $\alpha\sigma(\alpha) \in \mathcal{O}_\mathbb{K}$. Além disso, $\alpha + \sigma(\alpha) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a \in \mathbb{Q}$ e

$\alpha\sigma(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 \in \mathbb{Q}$. Como $\mathbb{Z}$ é um anel de ideais principais, pela Proposição 1.1.5, temos que $\mathbb{Z}$ é integralmente fechado e portanto

$$2a \in \mathbb{Z} \text{ } e \text{ } a^2 - db^2 \in \mathbb{Z}. \tag{1.1}$$

Pela equação (1.1) temos que $(2a)^2 - d(2b)^2 \in \mathbb{Z}$. Como $2a \in \mathbb{Z}$, segue que $(2a)^2 \in \mathbb{Z}$. Por outro lado, se $2b \notin \mathbb{Z}$, o seu denominador teria um fator primo p e este fator apareceria como p^2 no denominador de $d(2b)^2$. Sendo d livre de quadrados, segue que $d(2b)^2 \notin \mathbb{Z}$, o que é um absurdo. Portanto, $2b \in \mathbb{Z}$. ∎

Teorema 1.3.1 *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, com $d \in \mathbb{Z}$ livre de quadrados, ou seja, $d \not\equiv 0(modulo\ 4)$.*
a) Se $d \equiv 2$ ou $d \equiv 3(modulo\ 4)$, então o anel dos inteiros $\mathcal{O}_{\mathbb{K}}$, consiste de todos os elementos da forma $a + b\sqrt{d}$, com $a, b \in \mathbb{Z}$.
b) Se $d \equiv 1(modulo\ 4)$, então o anel dos inteiros $\mathcal{O}_{\mathbb{K}}$, consiste de todos os elementos da forma $\frac{1}{2}(a + b\sqrt{d})$, com $a, b \in \mathbb{Z}$, e de mesma paridade.

Demonstração: Seja $\alpha = a + b\sqrt{d} \in \mathcal{O}_{\mathbb{K}}$. Pelo Lema 1.3.1 temos que

$$a = \frac{u}{2} \text{ } e \text{ } b = \frac{v}{2}, \text{ } com \text{ } u, v \in \mathbb{Z}.$$

Da equação (1.1) temos que

$$u^2 - dv^2 \in 4\mathbb{Z}.$$

a) Se $d \equiv 2$ ou $d \equiv 3(modulo\ 4)$, temos que u, v são pares, pois se v fosse ímpar, teríamos $v^2 \equiv 1(modulo\ 4)$. Como $u^2 - dv^2 \in 4\mathbb{Z}$ temos que $u^2 - d(4k + 1) \in 4\mathbb{Z}$ o que implica que $u^2 - d \in 4\mathbb{Z}$. Assim, $u^2 \equiv d(modulo\ 4)$. Portanto, $d \equiv 1(modulo\ 4)$ ou $d \equiv 0(modulo\ 4)$, o que contradiz a hipótese. Sendo v par, temos que $v^2 \equiv 0(modulo\ 4)$ e portanto $u^2 \in 4\mathbb{Z}$. Assim u também é par. Então $a, b \in \mathbb{Z}$ e $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ e portanto, $\mathcal{O}_{\mathbb{K}} \subset \mathbb{Z}[\sqrt{d}]$. Por outro lado, tomando $\alpha \in \mathbb{Z}[\sqrt{d}]$, temos que α é raiz do polinômio

$$x^2 - 2ax + a^2 - db^2 \in \mathbb{Z}[x].$$

Portanto, $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_{\mathbb{K}}$. Assim, $\mathbb{Z}[\sqrt{d}] = \mathcal{O}_{\mathbb{K}}$.
b) Se $d \equiv 1(modulo\ 4)$, temos que u, v tem a mesma paridade. Se u e v são pares então $a, b \in \mathbb{Z}$, e portanto $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Se u e v são ímpares, então $\alpha = \frac{u}{2} + \frac{v\sqrt{d}}{2} \in \mathbb{Z}\left[\frac{1 + \sqrt{d}}{2}\right]$.
Portanto, $\mathcal{O}_{\mathbb{K}} \subset \mathbb{Z}\left[\frac{1 + \sqrt{d}}{2}\right]$. Por outro lado, se

$$\alpha = a + b\left(\frac{1 + \sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1 + \sqrt{d}}{2}\right]$$

com $a, b \in \mathbb{Z}$, temos que α é raiz do polinômio $x^2 - (2a+b)x + \left(a^2 + ab - \frac{(1-d)b^2}{4}\right) \in \mathbb{Z}[x]$, pois $d \equiv 1(modulo\ 4)$. Assim, $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subset \mathcal{O}_{\mathbb{K}}$. Portanto, $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathcal{O}_{\mathbb{K}}$. ■

1.4 Corpos ciclotômicos

Nesta seção apresentamos os corpos ciclotômicos $\mathbb{Q}(\xi_p)$, onde ξ_p é uma raiz p-ésima primitiva da unidade, e p um número primo. Também veremos que $\mathbb{Z}[\xi_p]$ é o anel dos inteiros de $\mathbb{Q}(\xi_p)$.

Definição 1.4.1 *Seja $\mathbb{K}$ um corpo. Um elemento $\xi \in \mathbb{K}$ tal que $\xi^n = 1$ é chamado uma raiz n-ésima da unidade. Dizemos que ξ é uma raiz n-ésima primitiva da unidade se $\xi^n = 1$ e $\xi^m \neq 1$ para $1 < m < n$.*

Definição 1.4.2 *Um corpo ciclotômico é um corpo gerado por uma raiz n-ésima da unidade.*

Observação 1.4.1 *Se p é um número primo e ξ_p é uma raiz p-ésima primitiva da unidade, então $[\mathbb{Q}[\xi_p] : \mathbb{Q}] = \varphi(p) = p - 1$, onde φ é a função de Euler, e $\{1, \xi, \cdots, \xi^{p-2}\}$ é uma base de $\mathbb{Q}[\xi_p]$ sobre $\mathbb{Q}$.*

Definição 1.4.3 *O polinômio $\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$ é chamado polinômio ciclotômico.*

Teorema 1.4.1 *O polinômio $x^{p-1} + x^{p-2} + \cdots + x + 1$ é irredutível sobre $\mathbb{Q}$, onde p é um número primo.*

Demonstração: Considere $x = y + 1$. Assim,

$$\frac{x^p - 1}{x - 1} = \frac{(y+1)^p - 1}{(y+1) - 1} = \frac{\binom{p}{0} y^p + \binom{p}{1} y^{p-1} + \cdots + \binom{p}{p-1} y + \binom{p}{p} y^0 - 1}{y}$$
$$= \frac{y^p + py^{p-1} + \cdots + py + 1 - 1}{y} = y^{p-1} + py^{p-2} + \cdots + p.$$

Notemos que p divide $\binom{p}{i}$, para cada $i = 1, \cdots, p-1$ e p^2 não divide p. Então pelo Critério de Eisenstein segue que este polinômio é irredutível sobre $\mathbb{Q}$. ■

Lema 1.4.1 *Sejam p um números primo e ξ uma raiz p-ésima primitiva da unidade. Então:*
1) $Tr(\xi^j) = -1$, *para* $j = 1, \cdots, p-1$.
2) $Tr(1-\xi^j) = p$, *para* $j = 1, \cdots, p-1$.
3) $N(\xi - 1) = (-1)^{p-1}p$ *e* $N(1-\xi) = p$.
4) $p = (1-\xi)(1-\xi^2)\cdots(1-\xi^{p-1})$.

Demonstração: 1) O polinômio ciclotômico de ξ é dado por $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. Como ξ^j, para $j = 1, 2, \cdots, p-1$ são as raízes de $f(x)$, temos que $Tr(\xi^j) = -1$, para $j = 1, \cdots, p-1$. Além disso, como $[\mathbb{Q}[\xi] : \mathbb{Q}] = p-1$ temos que $Tr(1) = p-1$.
2) $Tr(1-\xi^j) = Tr(1) - Tr(\xi^j) = p - 1 + 1 = p$, para $j = 1, \cdots, p-1$.
3) Como $\xi - 1$ é uma raiz do polinômio $f(y) = y^{p-1} + \sum_{j=p-1}^{1} \begin{pmatrix} p \\ j \end{pmatrix} y^{j-1}$ segue que,

$$N(\xi - 1) = (-1)^{p-1}p$$

e $N(1-\xi) = N((-1)(\xi-1)) = N(-1)N(\xi-1) = (-1)^{p-1}(-1)^{p-1}p = (-1)^{2(p-1)}p = p$.
4) Como $x^{p-1} + x^{p-2} + \cdots + x + 1 = (x-\xi)(x-\xi^2)\cdots(x-\xi^{p-1})$, temos para $x = 1$ que $(1-\xi)(1-\xi^2)\cdots(1-\xi^{p-1}) = p$. ∎

Lema 1.4.2 *Com as mesmas notações do Lema 1.4.1 temos que*
1) Se $\mathcal{O}_{\mathbb{K}}$ *é o anel dos inteiros de* $\mathbb{K} = \mathbb{Q}(\xi_p)$, *então* $(1-\xi_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z} = \langle p \rangle$.
2) $Tr(y(1-\xi)) \in p\mathbb{Z}$, $\forall y \in \mathcal{O}_{\mathbb{K}}$.

Demonstração: 1) Pelo item 4) do Lema 1.4.1, temos que

$$p = (1-\xi)(1-\xi^2)\cdots(1-\xi^{p-1}).$$

Então p $\in (1-\xi)\mathcal{O}_{\mathbb{K}}$. Logo, $\langle p \rangle \subset (1-\xi)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z}$. Por outro lado, suponhamos que o ideal $p\mathbb{Z} \subsetneq (1-\xi)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} \subset \mathbb{Z}$. Como $p\mathbb{Z}$ é maximal, segue que $(1-\xi)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = \mathbb{Z}$. Logo, $1 \in \mathbb{Z}$, e então $1 = (1-\xi)a$, com $a \in \mathcal{O}_{\mathbb{K}}$. Assim, $1-\xi$ é inversível, e portanto $1-\xi^j$ são inversíveis em $\mathcal{O}_{\mathbb{K}}$. Então, $(1-\xi)(1-\xi^2)\cdots(1-\xi^{p-1}) = p$ é inversível em $\mathbb{Z}$, o que é um absurdo. Portanto,

$$p\mathbb{Z} = (1-\xi)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z}.$$

2) Cada conjugado $y_i(1-\xi^i)$ de $y(1-\xi)$ é um múltiplo de $1-\xi^i$ em $\mathcal{O}_{\mathbb{K}}$ onde $i = 1, 2, \cdots, p-1$. Como

$$1 - \xi^i = (1-\xi)(\xi^{i-1} + \xi^{i-2} + \cdots + \xi + 1),$$

segue que $1-\xi^i$ é um múltiplo de $1-\xi$ em $\mathcal{O}_{\mathbb{K}}$. Sendo o traço a soma dos conjugados, então

$$Tr(y(1-\xi)) = y_1(1-\xi) + y_2(1-\xi^2) + \cdots + y_p(1-\xi^p) = \alpha(1-\xi),$$

com $\alpha \in \mathcal{O}_{\mathbb{K}}$. Portanto, $Tr(y(1-\xi)) \in \mathcal{O}_{\mathbb{K}}$. Como $\mathbb{Z}$ é integralmente fechado, segue que $Tr(y(1-\xi)) \in \mathbb{Z}$. Assim,

$$Tr(y(1-\xi)) \in (1-\xi_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}.$$ ■

Teorema 1.4.2 *Se p é um número primo e ξ_p é uma raiz p-ésima primitiva da unidade, então $\mathbb{Z}[\xi_p]$ é o anel dos inteiros de $\mathbb{K} = \mathbb{Q}(\xi_p)$ e $\{1, \xi, \cdots, \xi^{p-2}\}$ é uma base de $\mathbb{Z}[\xi_p]$ como um $\mathbb{Z}$-módulo.*

Demonstração: Seja $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{Q}(\xi_p)$. Temos que $\mathbb{Z}[\xi_p] \subset \mathcal{O}_{\mathbb{K}}$. Agora, vamos provar que $\mathcal{O}_{\mathbb{K}} \subset \mathbb{Z}[\xi_p]$. Considere $\alpha \in \mathcal{O}_{\mathbb{K}} \subset \mathbb{Q}(\xi_p)$. Assim,

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

com $a_i \in \mathbb{Q}$. Logo, $\alpha(1-\xi) = a_0(1-\xi) + a_1(\xi - \xi^2) + \cdots + a_{p-2}(\xi^{p-2} - \xi^{p-1})$. Assim,

$$Tr(\alpha(1-\xi)) = a_0 Tr(1-\xi) + a_1 Tr(\xi - \xi^2) + \cdots + a_{p-2} Tr(\xi^{p-2} - \xi^{p-1}) \in p\mathbb{Z},$$

pelo Lema 1.4.2. Então $a_0 Tr(1-\xi) = a_0 p \in p\mathbb{Z}$ e $a_0 \in \mathbb{Z}$. De modo análogo, temos que $\xi^{-1} = \xi^{p-1} \in \mathcal{O}_{\mathbb{K}}$, e assim

$$(\alpha - a_0)\xi^{-1} = a_1 + a_2\xi + \cdots + a_{p-2}\xi^{p-3}.$$

Multiplicando por $1-\xi$ temos que $(\alpha - a_0)\xi^{-1}(1-\xi) = a_1(1-\xi) + a_2\xi(1-\xi) + \cdots + a_{p-2}\xi^{p-3}(1-\xi)$ e assim

$$Tr((\alpha - a_0)\xi^{-1}(1-\xi)) = a_1 Tr(1-\xi) + a_2 Tr(\xi - \xi^2) + \cdots + a_{p-2} Tr(\xi^{p-3} - \xi^{p-2}).$$

Logo, $a_1 Tr(1-\xi) = a_1 p \in p\mathbb{Z}$ e $a_1 \in \mathbb{Z}$. Prosseguindo, analogamente, temos que $a_i \in \mathbb{Z}$, para cada $i = 1, \cdots, n$. Assim, $\alpha \in \mathbb{Z}[\xi_p]$. Portanto, $\mathbb{Z}[\xi_p] = \mathcal{O}_{\mathbb{K}}$. ■

1.5 Anéis Noetherianos

Nesta seção apresentamos os conceitos de módulos e anéis Noetherianos, enfocando suas principais propriedades.

Definição 1.5.1 *Sejam A um anel e M um A-módulo. Dizemos que M é um A-módulo Noetheriano se satisfaz uma das seguintes condições:*

1) Toda família não vazia de A-submódulos de M tem um elemento maximal.

2) Toda sequência crescente de A-submódulos de M é estacionária.

3) Todo A-submódulo de M é finitamente gerado.

Dizemos que um anel A é Noetheriano se A considerado como um A-módulo for Noetheriano.

Proposição 1.5.1 *Todo anel principal A é Noetheriano.*

Demonstração: Considere a sequência crescente de A-submódulos de A,

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots .$$

Como A é principal, todos os ideais de A são principais e como os submódulos de A são exatamente os ideais de A, segue que os submódulos de A são principais. Temos que $I = \bigcup_{n\in N} I_n$ é um ideal de A. Agora, notemos que $I_n \subset I = \langle a\rangle$, $\forall n \in \mathbb{N}$ e $a \in I_{n_0}$, para algum $n_0 \in \mathbb{N}$, pois $a \in \langle a\rangle = I = \bigcup_{n\in\mathbb{N}} I_n$. Como $a \in I_{n_0}$ e $a \in \langle a\rangle$ então $I = \langle a\rangle \subset I_{n_0}$. Portanto, $I = I_{n_0}$. Assim, $\exists n_0 \in \mathbb{N}$ tal que $\forall n \geq n_0$ temos que $I_n = I_{n_0}$. ∎

Proposição 1.5.2 *Sejam A um anel, M um A-módulo e L um submódulo de M. Então M é Noetheriano se, e somente se, M/L e L são Noetherianos.*

Demonstração: Suponhamos que M é Noetheriano. Seja $(M_n)_{n\geq 0}$ uma sequência crescente de A-submódulos de L. Então $(M_n)_{n\geq 0}$ também é uma sequência crescente de A-submódulos de M. Como M é Noetheriano, segue que $(M_n)_{n\geq 0}$ é estacionária. Portanto, L é Noetheriano. Para mostrar que M/L é Noetheriano, sejam $S = \{$ conjunto dos submódulos de M que contém $L\}$ e $T = \{$ conjunto dos submódulos de $M/L\}$. A aplicação $\varphi : S \longrightarrow T$ definida por $\varphi(N) = N/L$, com $N \in S$, é uma bijeção de S em T. Assim, se $(M_n)_{n\geq 0}$ é uma sequência crescente de A-submódulos de M/L, então $\varphi^{-1}(M_n)_{n\geq 0}$ também é uma sequência crescente 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, M/L é Noetheriano. Reciprocamente, suponhamos que M/L e L são Noetherianos. Seja $(M_n)_{n\geq 0}$ uma sequência crescente de A-submódulos de M. Então $(L \cap M_n)_{n\geq 0}$ é uma sequência crescente de A-submódulos L. Como L é Noetheriano, segue que $(L \cap M_n)_{n\geq 0}$ é estacionária, ou seja, $\exists k \in \mathbb{N}$ tal que

$$M_n \cap L = M_{n+1} \cap L,\ \forall n \geq k \ e\ \frac{M_n}{L} = \frac{M_{n+1}}{L},\ \forall n \geq k.$$

Sabemos, que $M_n \subseteq M_{n+1}\ \forall n \geq k$. Seja $x \in M_{n+1}$, então existe $y \in M_n$ tal que $x + L = y + L$. Assim, $x - y \in L \cap M_{n+1} = L \cap M_n$. Logo, $x - y \in M_n$ e como $y \in M_n$ segue que $x \in M_n$. Portanto, $M_n = M_{n+1}$, $\forall n \geq k$ e assim, M é Noetheriano. ∎

Corolário 1.5.1 *Se $M_1, \cdots, M_n$ são A-módulos Noetherianos então o produto $M_1 \times \cdots \times M_n$ é um 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 $\varphi(0, y) = y$. Como φ é um homomorfismo sobrejetor, temos que $\dfrac{M_1 \times M_2}{\ker \varphi} \simeq M_2$, onde $\ker \varphi = M_1 \times \{0\}$. Logo, $\dfrac{M_1 \times M_2}{M_1 \times \{0\}} \simeq M_2$. Como M_2 é Noetheriano, temos que $\dfrac{M_1 \times M_2}{M_1 \times \{0\}} \simeq M_2$ é Noetheriano e pela Proposição 1.5.2, segue que $M_1 \times M_2$ é Noetheriano. Suponhamos agora, por hipótese de indução, que $M = M_1 \times \cdots \times M_{n-1}$ é Noetheriano. Como M_n é Noetheriano, segue do caso $n = 2$, que $M = M_1 \times \cdots \times M_n$ é um A-módulo Noetheriano. ∎

Corolário 1.5.2 *Se A é um anel Noetheriano e M é um A-módulo finitamente gerado, então M é um A-módulo Noetheriano.*

Demonstração: Seja $\{e_1, \cdots, e_n\}$ um conjunto de geradores do A-módulo M. A aplicação $\varphi : A^n \longrightarrow M$ definida por $\varphi(a_1, \cdots, a_n) = a_1e_1 + \cdots + a_ne_n$, é um homomorfismo sobrejetor. Assim, $\dfrac{A^n}{\ker \varphi} \simeq M$. Como A é Noetheriano, pelo Corolário 1.5.1, segue que A^n é Noetheriano. Pela Proposição 1.5.2, segue que M é um A-módulo Noetheriano. ∎

Proposição 1.5.3 *Seja A um anel Noetheriano e integralmente fechado. Sejam $\mathbb{K}$ o corpo de frações de A, $\mathbb{K} \subseteq \mathbb{L}$ uma extensão finita de grau n e $\mathcal{O}_\mathbb{L}$ o anel dos inteiros de A em $\mathbb{L}$. Então $\mathcal{O}_\mathbb{L}$ é um A-módulo finitamente gerado e $\mathcal{O}_\mathbb{L}$ é um anel Noetheriano.*

Demonstração: Pelo Teorema 1.2.1, temos que $\mathcal{O}_\mathbb{L}$ é um submódulo de um A-módulo livre de posto n. Pelo Corolário 1.5.2, temos que $\mathcal{O}_\mathbb{L}$ é um A-módulo Noetheriano e portanto finitamente gerado. Como os ideias de $\mathcal{O}_\mathbb{L}$ são A- submódulos de $\mathcal{O}_\mathbb{L}$, segue que satisfazem a condição de maximilidade da Definição 1.5.1. Portanto, $\mathcal{O}_\mathbb{L}$ é um anel Noetheriano. ∎

Lema 1.5.1 *Se $A \subseteq B$ são anéis e $\mathcal{P} \subset B$ é um ideal primo, então $\mathcal{P} \cap A$ é um ideal primo de A.*

Demonstração: Consideremos a aplicação $\varphi : A \xrightarrow{i} B \xrightarrow{\pi} B/\mathcal{P}$, onde i é a inclusão e π é a projeção. A função $\varphi = \pi \circ i$ é um homomorfismo, pois π e i são homomorfismo e

$\ker(\varphi) = A \cap \mathcal{P}$, pois $\varphi(x) = \pi \circ i(x) = \pi(x) = x + \mathcal{P}$ e $\varphi(x) = \bar{0}$ se, e somente se, x $\in \mathcal{P} \cap A$. Portanto, pelo Teorema do Homomorfismo, $A/\mathcal{P} \cap A \simeq Im(\varphi) \subset B/\mathcal{P}$. Como $B/\mathcal{P}$ é um domínio, segue que $A/\mathcal{P} \cap A$ é um domínio. Portanto, $\mathcal{P} \cap A$ é um ideal primo de A. ∎

Lema 1.5.2 *Sejam A um anel e $\mathcal{P}$ um ideal primo de A. Se $\mathcal{P}$ contém um produto de ideais $\mathcal{A}_1, \cdots, \mathcal{A}_n$ de A então $\mathcal{P}$ contém alguns deles.*

Demonstração: Se $\mathcal{A}_j \not\subseteq \mathcal{P}$, $\forall j = 1, \cdots, n$, então existe $\alpha_j \in \mathcal{A}_j$ e $\alpha_j \notin \mathcal{P}$. Como $\mathcal{P}$ é primo, segue que $\alpha_1 \cdots \alpha_n \notin \mathcal{P}$. Mas $\alpha_1 \cdots \alpha_n \in \mathcal{A}_1 \cdots \mathcal{A}_n \subset \mathcal{P}$, o que é um absurdo. Portanto, $\mathcal{P}$ contém $\mathcal{A}_j$ para algum $j = 1, \cdots, n$. ∎

Lema 1.5.3 *Em um anel A Noetheriano, todo ideal contém um produto de ideais primos.*

Demonstração: Sejam A um anel Noetheriano e F o conjuntos dos ideais de A que não contém um produto de ideais primos. Suponhamos $F \neq \emptyset$. Como A é Noetheriano, F tem um elemento maximal M. Temos que M não é um ideal maximal, pois caso contrário, M seria primo e assim, $M \notin F$. Assim, existem $x, y \in A - M$ 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,

$$\mathcal{P}_1\mathcal{P}_2 \cdots \mathcal{P}_n \subseteq \langle x \rangle + M \text{ e } \mathcal{Q}_1\mathcal{Q}_2 \cdots \mathcal{Q}_n \subseteq \langle y \rangle + M,$$

onde $\mathcal{P}_i, \mathcal{Q}_j$ são ideais primos de A. Portanto,

$$(\mathcal{P}_1\mathcal{P}_2 \cdots \mathcal{P}_n)(\mathcal{Q}_1\mathcal{Q}_2 \cdots \mathcal{Q}_n) \subseteq (\langle x \rangle + M)(\langle y \rangle + M) \subseteq M,$$

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

Corolário 1.5.3 *Em um domínio Noetheriano, todo ideal não nulo contém um produto de ideais primos não nulos.*

Demonstração: Análoga ao Lema 1.5.3. ∎

Definição 1.5.2 *Seja $\mathbb{K}$ um corpo de números. Um $\mathcal{O}_{\mathbb{K}}-$módulo $\mathcal{I}$ de $\mathbb{K}$ é um ideal fracionário se existe $d \in \mathcal{O}_{\mathbb{K}}$ não nulo tal que $d\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$. Em particular, os ideais inteiros de A são ideais fracionários com d=1.*

Proposição 1.5.4 *Se A é um domínio Noetheriano, então todo ideal fracionário $\mathcal{I}$ de A é um A-módulo finitamente gerado.*

Demonstração: Como $\mathcal{I}$ é um ideal fracionário de A, então existe $d \in A - \{0\}$ tal que $d\mathcal{I} \subseteq A$. Assim, $\mathcal{I} \subseteq d^{-1}A$. A aplicação $\varphi : A \longrightarrow d^{-1}A$, tal que $\varphi(x) = d^{-1}x$, $x \in A$, é um isomorfismo. Assim, A é isomorfo a $d^{-1}A$. Como A é Noetheriano, temos que $d^{-1}A$ é Noetheriano. Logo, $\mathcal{I}$ é um A-módulo finitamente gerado. ∎

1.6 Anéis de Dedekind

Nesta seção apresentamos o conceito de um anel de Dedekind juntamente com suas principais propriedades. Observamos que a fatoração não é única para elementos do anel dos inteiros, pois se considerarmos $\mathbb{Z}[\sqrt{-5}]$ o anel dos inteiros do corpo $\mathbb{Q}(\sqrt{-5})$, teremos que $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Mas veremos, nesta seção, que a fatoração é única para ideais de um anel de Dedekind.

Definição 1.6.1 *Dizemos que um domínio A é um anel de Dedekind se satisfaz as seguintes condições:*
1) A é integralmente fechado.
2) A é Noetheriano
3) Todo ideal primo não nulo de A é maximal.

Teorema 1.6.1 *Sejam A 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 A em $\mathbb{L}$. Então $\mathcal{O}_{\mathbb{L}}$ é um anel Dedekind.*

Demonstração: Pelas Proposições 1.1.4 e 1.5.3, temos que $\mathcal{O}_{\mathbb{L}}$ é integralmente fechado e noetheriano, respectivamente. Assim, falta mostrar que todo ideal primo não nulo de $\mathcal{O}_{\mathbb{L}}$ é maximal. Seja $\mathcal{P} \subset \mathcal{O}_{\mathbb{L}}$ um ideal primo não nulo. Como $A \subset \mathcal{O}_{\mathbb{L}}$ então pelo Lema 1.5.1, segue que $\mathcal{P} \cap A$ é um ideal primo de A. Vamos mostrar que $\mathcal{P} \cap A$ é não nulo. Seja $\alpha \in \mathcal{P}$ e $\alpha \neq 0$. Como $\mathcal{P} \subset \mathcal{O}_{\mathbb{L}}$ segue que $\alpha \in \mathcal{O}_{\mathbb{L}}$. Assim, existem $a_i \in A$, $i = 0, \cdots, n-1$, não todos nulos tal que

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

e que n seja mínimo. Logo, $a_0 \neq 0$, pois caso contrário, obteríamos uma equação de grau menor. Assim,

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

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

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

Como $\mathcal{O}_{\mathbb{L}}$ é inteiro sobre A, segue que $\mathcal{O}_{\mathbb{L}}/\mathcal{P}$ é inteiro sobre $A/\mathcal{P} \cap A$. Pela Proposição 1.1.3, temos que $\mathcal{O}_{\mathbb{L}}/\mathcal{P}$ é um corpo. Portanto, $\mathcal{P}$ é maximal. ∎

Lema 1.6.1 *Sejam A um anel de Dedekind que não é um corpo e $\mathbb{K}$ o seu corpo de frações. Então todo ideal maximal $\mathcal{M}$ de A é inversível.*

Demonstração: Seja $\mathcal{M}$ um ideal maximal de A. Como A não é um corpo, segue que $\mathcal{M} \neq \{0\}$. Consideremos $\mathcal{N} = \{x \in \mathbb{K} : x\mathcal{M} \subset A\}$. Temos que $\mathcal{N}$ é um ideal fracionário, pois $\mathcal{N}$ é um A-módulo tal que $\mathcal{N} \subseteq \mathbb{K}$ e se $c \in \mathcal{M}$, $c \neq 0$, temos que $c\mathcal{N} \subseteq A$. Vamos mostrar que $\mathcal{N}\mathcal{M} = A$. Pela definição de $\mathcal{N}$ temos $\mathcal{N}\mathcal{M} \subset A$. Por outro lado, $A \subset \mathcal{N}$, pois $\mathcal{M}$ é um ideal de A. Assim, $\mathcal{M} = \mathcal{M}A \subset \mathcal{M}\mathcal{N} \subset A$. Como $\mathcal{M}$ é maximal, segue que $\mathcal{M} = \mathcal{N}\mathcal{M}$ ou $\mathcal{N}\mathcal{M} = A$. Suponhamos que $\mathcal{M} = \mathcal{N}\mathcal{M}$ e consideremos $\alpha \in \mathcal{N}$. Então $\alpha\mathcal{M} \subset \mathcal{M}$, $\alpha^2\mathcal{M} \subset \alpha\mathcal{M} \subset \mathcal{M}$ e $\alpha^n\mathcal{M} \subset \mathcal{M}$, para todo $n \in \mathbb{N}$. Seja $d \in \mathcal{M}$, $d \neq 0$. Então, $d\alpha^n \in A$. Portanto, $A[\alpha]$ é um ideal fracionário. Como A é noetheriano, pela Proposição 1.5.4, segue que $A[\alpha]$ é um A-módulo finitamente gerado. Pelo Teorema 1.1.1, segue que α é inteiro sobre A. Sendo A integralmente fechado, segue que $\alpha \in A$. Assim, $\mathcal{N} \subset A$ e como $A \subset \mathcal{N}$ segue que $\mathcal{N} = A$. Falta mostrar que esta igualdade é impossível. Seja $a \in \mathcal{M}$. Pelo Lema 1.5.3, temos que $\langle a \rangle = aA \supset \mathcal{P}_1\mathcal{P}_2 \cdots \mathcal{P}_n$, onde os $\mathcal{P}_i's$ são ideais primos não nulos de A, com n o menor valor possível. Assim, $\mathcal{M} \supset aA \supset \mathcal{P}_1\mathcal{P}_2 \cdots \mathcal{P}_n$. Pelo Lema 1.5.2, $\mathcal{M}$ contém um dos $\mathcal{P}_i$, para algum $i = 1, \cdots, n$. Sem perda de generalidade, digamos que seja $\mathcal{P}_1$, isto é, $\mathcal{M} \supset \mathcal{P}_1$. Como A é Dedekind, segue que $\mathcal{M} = \mathcal{P}_1$, pois $\mathcal{P}_1$ é maximal. Agora, consideremos $\mathcal{Q} = \mathcal{Q}_2 \cdots \mathcal{Q}_n$. Então $aA \supset \mathcal{M}\mathcal{Q}$ e pela minimalidade de n segue que $aA \not\supset \mathcal{Q}$. Logo, existe $b \in \mathcal{Q}$ com $b \notin \langle a \rangle$ tal que $\mathcal{M}b \subset \langle a \rangle$. Logo, $\frac{b}{a}\mathcal{M} \subseteq A$ e assim $\frac{b}{a} \in \mathcal{N}$. Como $b \notin \langle a \rangle$ segue que $\frac{b}{a} \notin A$. Assim, $\mathcal{N} \neq A$. Portanto, $\mathcal{M}\mathcal{N} = A$. ∎

Teorema 1.6.2 *Seja A um anel de Dedekind, que não é um corpo. Então:*
1) Todo ideal fracionário $\mathcal{B}$ não nulo de A é um produto de ideais primos de A, de modo único, isto é, $\mathcal{B} = \prod_{i=1}^{n} \mathcal{P}_i^{e_i}$, onde $e_1, \cdots, e_n$ são inteiros positivos.
2) O conjunto dos ideais fracionários de A formam um grupo.

Demonstração: 1) Se $\mathcal{B}$ é um ideal fracionário de A, então existe $d \in A - \{0\}$ tal que $d\mathcal{B} \subseteq A$. Notemos que, $\mathcal{B} = (d\mathcal{B})(d^{-1}A)$, assim, é suficiente mostrar o resultado para ideais inteiros. Seja F a família dos ideais inteiros de A, não nulos, que não são um produto de ideais primos de A. Suponha que $F \neq \emptyset$. Como A é noetheriano, segue que F tem um elemento maximal M. Temos que $M \neq A$, pois A é o produto da coleção vazia de ideias primos. Assim, $M \subseteq \mathcal{P}$, onde $\mathcal{P}$ é um ideal maximal de A. Pelo Lema 1.6.1, temos que $\mathcal{Q} = \{x \in \mathbb{K} : x\mathcal{P} \subset A\}$ é tal que $\mathcal{P}\mathcal{Q} = A$. Como $M \subseteq \mathcal{P}$ segue que $M\mathcal{Q} \subseteq \mathcal{P}\mathcal{Q} = A$. Além disso, como $A \subset \mathcal{Q}$, segue que $M = MA \subset M\mathcal{Q} \subset A$. Temos que $M \subsetneq M\mathcal{Q}$, pois se $M = M\mathcal{Q}$ e se $\alpha \in \mathcal{Q}$, 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 $d\alpha^n \in M \subseteq A$. Portanto, $A[\alpha]$ é um ideal fracionário de A. Como A é noetheriano, pela Proposição 1.5.4, segue que $A[\alpha]$ é um A-módulo finitamente gerado. Pelo Teorema 1.1.1, segue que α é inteiro sobre A, e sendo A integralmente fechado, segue que $\alpha \in A$. Portanto, $\mathcal{Q} \subset A$ e assim $\mathcal{Q} = A$. Mas isto é impossível, pois se $\mathcal{Q} = A$, então $\mathcal{P} = \mathcal{P}A = \mathcal{P}\mathcal{Q} = A$, o que é um absurdo, pois $\mathcal{P}$ é um ideal primo. Pela maximalidade de M e como $M \subseteq M\mathcal{Q}$ temos que $M\mathcal{Q} \notin F$, ou seja, $M\mathcal{Q} = \mathcal{P}_1 \cdots \mathcal{P}_n$, onde $\mathcal{P}_i, i = 1, \cdots, n$, são ideais primos de A. Multiplicando por $\mathcal{P}$ ambos os lados, temos que $M = \mathcal{P}_1 \cdots \mathcal{P}_n \mathcal{P}$, o que é um absurdo, pois $M \in F$. Portanto, $F = \emptyset$.
2) Pelo Lema 1.6.1, temos que todo ideal $\mathcal{M}$ de A é inversível. Além disso, A é o elemento neutro e a multiplicação de ideais é associativa. ■

Definição 1.6.2 *Sejam A um domínio e $\mathbb{K}$ seu corpo de frações. Sejam $\mathcal{B}$ e $\mathcal{C}$ ideais fracionários de A. Dizemos que $\mathcal{B}$ divide $\mathcal{C}$ se existe $\mathcal{D}$ um ideal inteiro de A tal que $\mathcal{C} = \mathcal{B}\mathcal{D}$.*

Lema 1.6.2 *Sejam A um domínio e $\mathbb{K}$ seu corpo de frações. Sejam $\mathcal{B}$ e $\mathcal{C}$ ideais fracionários de A. Então $\mathcal{B}$ divide $\mathcal{C}$ se, e somente se, $\mathcal{C} \subseteq \mathcal{B}$*

Demonstração: Se $\mathcal{B}$ divide $\mathcal{C}$ então existe um ideal $\mathcal{D} \subseteq A$ tal que $\mathcal{C} = \mathcal{B}\mathcal{D} \subseteq \mathcal{B}$. Por outro lado, se $\mathcal{C} \subseteq \mathcal{B}$ então $\mathcal{C}\mathcal{B}^{-1} \subseteq \mathcal{B}\mathcal{B}^{-1} = A$. Isto implica que $\mathcal{C}\mathcal{B}^{-1}$ é um ideal inteiro tal que $(\mathcal{C}\mathcal{B}^{-1})\mathcal{B} = \mathcal{C}$. Portanto, $\mathcal{B}$ divide $\mathcal{C}$. ■

Definição 1.6.3 *Sejam A um anel de Dedekind e $\mathbb{K}$ seu corpo de frações. O grupo quociente $C(A) = I(A)/F(A)$ é chamado grupo das classes de ideais de A, onde $I(A)$ é o grupo dos ideais fracionários não nulos de A, e $F(A)$ é o subgrupo dos ideais fracionários principais de A. **Notação:** $h = \#C(A)$.*

Observação 1.6.1 *Seja A um domínio de Dedekind. Então, A é principal se, e somente se, $h = 1$.*

Proposição 1.6.1 *Se $\mathcal{J}$ é um ideal fracionário de um anel A de Dedekind então $\mathcal{J}^h$ é um ideal fracionário principal de A.*

Demonstração: Notemos que h é a ordem do grupo $C(A) = I(A)/F(A)$ das classes de ideais de A. Pelo Teorema de Lagrange segue que $\mathcal{J}^h \in F(A)$. ■

1.7 Norma de um ideal

Nesta seção apresentamos o conceito de norma de um ideal do anel dos inteiros de um corpo de números, onde consideramos $\mathbb{K}$ o corpo de números de grau finito n e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$. Também apresentamos algumas propriedades da norma de um ideal, dentre elas que a norma é multiplicativa.

Definição 1.7.1 *Seja $\mathcal{A}$ um ideal de $\mathcal{O}_{\mathbb{K}}$. A norma de $\mathcal{A}$ é definida como $N(\mathcal{A}) = \#\mathcal{O}_{\mathbb{K}}/\mathcal{A}$.*

Observação 1.7.1 *Se $\alpha \in \mathcal{O}_{\mathbb{K}}$ e $\alpha \neq 0$ então pelo Corolário* 1.2.1*, temos que $N(\alpha) \in \mathbb{Z}$.*

Proposição 1.7.1 *Se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então $|N(\alpha)| = \#\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{K}}\alpha$, onde $\mathcal{O}_{\mathbb{K}}\alpha = \langle\alpha\rangle$.*

Demonstração: Pelo Corolário 1.2.3, temos que $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n. Como $\varphi : \mathcal{O}_{\mathbb{K}} \longrightarrow \mathcal{O}_{\mathbb{K}}\alpha$ definida por $\varphi(a) = a\alpha$, $\alpha \in \mathcal{O}_{\mathbb{K}}$, é um isomorfismo, então $\mathcal{O}_{\mathbb{K}}\alpha$ 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 então existe uma base $\{e_1, \cdots, e_n\}$ de $\mathcal{O}_{\mathbb{K}}$ e $c_1, \cdots, c_n \in \mathbb{Z}$ tal que $c_1e_1, \cdots, c_ne_n$ é uma base de $\mathcal{O}_{\mathbb{K}}\alpha$. A aplicação $\psi : \mathcal{O}_{\mathbb{K}} \longrightarrow \mathbb{Z}/c_1\mathbb{Z} \times \cdots \times \mathbb{Z}/c_n\mathbb{Z}$ definida por $\psi(\sum a_ie_i) = (\bar{a_1}, \bar{a_2}, \cdots, \bar{a_n})$ é um homomorfismo sobrejetor, e $\ker(\psi) = \mathcal{O}_{\mathbb{K}}\alpha$, pois $a \in \ker(\psi)$ se, e somente se, $\psi(a) = \bar{0}$ se, e somente se, $\bar{a_i} = \bar{0}$, para $i = 1, \cdots, n$, se, e somente se, $a_i \in c_i\mathbb{Z}$, para $i = 1, \cdots, n$, se, e somente se, c_i divide a_i, para $i = 1, \cdots, n$, se, e somente se, $a = \sum_{i=1}^{n} a_ie_i = \sum_{i=1}^{n} b_ic_ie_i$. Como $b_i \in \mathbb{Z}$ temos que $a \in \mathcal{O}_{\mathbb{K}}\alpha$. Pelo Teorema do Homomorfismo, temos que

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

Assim, $\#\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{K}}\alpha = c_1c_2\cdots c_n$. Seja a aplicação $\mathbb{Z}$-linear $\mu : \mathcal{O}_{\mathbb{K}} \longrightarrow \mathcal{O}_{\mathbb{K}}\alpha$, definida por $\mu(e_i) = c_ie_i$, para $i = 1, \cdots, n$. Logo, $\mu(e_1) = c_1e_1 + 0e_2 + \cdots + 0e_n, \cdots, \mu(e_n) = 0e_1 + \cdots + c_ne_n$ e $\det(\mu) = c_1c_2\cdots c_n$. Por outro lado, temos que $B = \{c_1e_1, \cdots, c_ne_n\}$ e $C = \{\alpha e_1, \cdots, \alpha e_n\}$ são bases de $\mathcal{O}_{\mathbb{K}}\alpha$, e portanto existe um automorfismo $v : \mathcal{O}_{\mathbb{K}}\alpha \longrightarrow \mathcal{O}_{\mathbb{K}}\alpha$ tal que $v(c_ie_i) = \alpha e_i$, para $i = 1, \cdots, n$. Como a matriz mudança de base é inversível, segue que $\det(v)$ é inversível em $\mathbb{Z}$, isto é, $\det(v) = \pm 1$. Também, $(v \circ \mu)(e_i) = v(\mu(e_i)) = v(c_ie_i) = \alpha e_i$, para $i = 1, \cdots, n$. Assim, $(v \circ \mu)(a) = \alpha a$. Finalmente, $N(\alpha) = \det(v \circ \mu) = \det(v)\det(\mu) = \pm 1c_1c_2\cdots c_n = \pm\#\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{K}}\alpha$. Portanto, $|N(\alpha)| = \#\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{K}}\alpha$. ∎

Proposição 1.7.2 *Se $\mathcal{A}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então $N(\mathcal{A})$ é finita.*

Demonstração: Se $\alpha \in \mathcal{A}$ é um elemento não nulo, então $\mathcal{O}_{\mathbb{K}}\alpha \subset \mathcal{A}$ e $\mathcal{O}_{\mathbb{K}}/\mathcal{A}$ pode ser visto como um quociente de $\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{K}}\alpha$. Assim,

$$\#\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{K}}\alpha = \#\mathcal{O}_{\mathbb{K}}/\mathcal{A} \cdot \#\mathcal{A}/\mathcal{O}_{\mathbb{K}}\alpha.$$

Pela Proposição 1.7.1, segue que $\#\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{K}}\alpha$ é finito. Portanto, $\#\mathcal{O}_{\mathbb{K}}/\mathcal{A}$ é finito. ∎

Proposição 1.7.3 *Se $\mathcal{A}$ e $\mathcal{B}$ ideais não nulos de $\mathcal{O}_{\mathbb{K}}$, então $N(\mathcal{AB})$=$N(\mathcal{A})N(\mathcal{B})$.*

Demonstração: Pelo Teorema 1.6.2, temos que $\mathcal{B} = \prod_{i=1}^{n} \mathcal{P}_i^{e_i}$, onde $\mathcal{P}_i \subseteq \mathcal{O}_{\mathbb{K}}$, para $i = 1, \cdots, n$, são ideais primos. Seja $\mathcal{P}_i = \mathcal{M}$, para algum i. Assim, é suficiente mostrar que $N(\mathcal{AM}) = N(\mathcal{A})N(\mathcal{M})$, ou seja,

$$\#\mathcal{O}_{\mathbb{K}}/\mathcal{AM} = \#\mathcal{O}_{\mathbb{K}}/\mathcal{A} \cdot \#\mathcal{O}_{\mathbb{K}}/\mathcal{M}, \tag{1.2}$$

onde $\mathcal{M}$ é ideal maximal de $\mathcal{O}_{\mathbb{K}}$. Como $\mathcal{AM} \subseteq \mathcal{A}$, temos que o homomorfismo sobrejetor $\phi : \mathcal{O}_{\mathbb{K}}/\mathcal{AM} \longrightarrow \mathcal{O}_{\mathbb{K}}/\mathcal{A}$, definido por $\phi(x + \mathcal{AM}) = x + \mathcal{A}$, para $x \in \mathcal{O}_{\mathbb{K}}$, possui $\ker(\phi) = \mathcal{A}/\mathcal{AM}$. Pelo Teorema do Homomorfismo, segue que $\mathcal{O}_{\mathbb{K}}/\mathcal{A} \simeq \dfrac{\mathcal{O}_{\mathbb{K}}/\mathcal{AM}}{\mathcal{A}/\mathcal{AM}}$. Assim,

$$\#\mathcal{O}_{\mathbb{K}}/\mathcal{AM} = \#\mathcal{O}_{\mathbb{K}}/\mathcal{A} \cdot \#\mathcal{A}/\mathcal{AM} \tag{1.3}$$

Pelas equações (1.2) e (1.3) é suficiente mostrar $\#\mathcal{A}/\mathcal{AM} = \#\mathcal{O}_{\mathbb{K}}/\mathcal{M}$. Temos que $\mathcal{A}/\mathcal{AM}$ é um $\mathcal{O}_{\mathbb{K}}$-módulo e portanto $\mathcal{A}/\mathcal{AM}$ é um $\mathcal{O}_{\mathbb{K}}/\mathcal{M}$-módulo. Como $\mathcal{O}_{\mathbb{K}}/\mathcal{M}$ é corpo, segue que $\mathcal{A}/\mathcal{AM}$ é um espaço vetorial sobre $\mathcal{O}_{\mathbb{K}}/\mathcal{M}$ e os subespaços são ideais da forma $\mathcal{I}/\mathcal{AM}$, onde $\mathcal{I}$ é um ideal de $\mathcal{O}_{\mathbb{K}}$ tal que $\mathcal{AM} \subseteq \mathcal{I} \subseteq \mathcal{A}$. Vamos mostrar que não existe $\mathcal{I}$ tal que $\mathcal{AM} \subsetneq \mathcal{I} \subsetneq \mathcal{A}$. De fato, como $\mathcal{AM} \subseteq \mathcal{I}$ segue, pelo Lema 1.6.2, que $\mathcal{I} \mid \mathcal{AM}$. Então existe $\mathcal{C}$ um ideal de $\mathcal{O}_{\mathbb{K}}$ tal que $\mathcal{AM} = \mathcal{IC}$. De modo análogo, se $\mathcal{I} \subseteq \mathcal{A}$ então $\mathcal{A} \mid \mathcal{I}$, e então existe $\mathcal{D}$ um ideal de $\mathcal{O}_{\mathbb{K}}$ tal que $\mathcal{I} = \mathcal{AD}$. Assim, $\mathcal{AM} = \mathcal{ADC}$ e portanto $\mathcal{M} = \mathcal{DC}$. Logo, $\mathcal{M} \subseteq \mathcal{C} \subseteq \mathcal{O}_{\mathbb{K}}$ e $\mathcal{M} \subseteq \mathcal{D} \subseteq \mathcal{O}_{\mathbb{K}}$. Mas $\mathcal{M}$ é maximal, então $\mathcal{D} = \mathcal{M}$ ou $\mathcal{D} = \mathcal{O}_{\mathbb{K}}$. Logo, $\mathcal{I} = \mathcal{AM}$ ou $\mathcal{I} = \mathcal{A}$. Deste modo, os únicos subespaços de $\mathcal{A}/\mathcal{AM}$ são os triviais e assim $\dim_{\mathcal{O}_{\mathbb{K}}/\mathcal{M}}(\mathcal{A}/\mathcal{AM}) = 1$. Portanto, $\#\mathcal{A}/\mathcal{AM} = \#\mathcal{O}_{\mathbb{K}}/\mathcal{M}$. ∎

Proposição 1.7.4 *Sejam $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ corpos de números com anéis de inteiros $\mathcal{O}_{\mathbb{K}}, \mathcal{O}_{\mathbb{L}} e \mathcal{O}_{\mathbb{M}}$ respectivamente. Se $\mathcal{J}$ é um ideal fracionário de $\mathbb{M}$, então $N_{\mathbb{L}|\mathbb{K}}(N_{\mathbb{M}|\mathbb{L}}(\mathcal{J})) = N_{\mathbb{M}|\mathbb{K}}(\mathcal{J})$.*

Demonstração: O resultado vale para o ideal $c\mathcal{O}_{\mathbb{M}}$ pois $N_{\mathbb{L}|\mathbb{K}}(N_{\mathbb{M}|\mathbb{L}}(c\mathcal{O}_{\mathbb{M}}))= N_{\mathbb{L}|\mathbb{K}}(\mathcal{O}_{\mathbb{L}}N_{\mathbb{M}|\mathbb{L}}(c))= \mathcal{O}_{\mathbb{K}}N_{\mathbb{L}|\mathbb{K}}(N_{\mathbb{M}|\mathbb{L}}(c))= \mathcal{O}_{\mathbb{K}}N_{\mathbb{M}|\mathbb{K}}(c))= N_{\mathbb{M}|\mathbb{K}}(c\mathcal{O}_{\mathbb{M}}))$. Agora, se $\mathcal{J}$ é um ideal fracionário não nulo de $\mathbb{M}$ e se h é o número das classes de $\mathbb{M}$ então $(\mathcal{J})^h = c\mathcal{O}_{\mathbb{M}}$ e assim, $N_{\mathbb{L}|\mathbb{K}}(N_{\mathbb{M}|\mathbb{L}}(\mathcal{J}))^h = N_{\mathbb{L}|\mathbb{K}}(N_{\mathbb{M}|\mathbb{L}}(c\mathcal{O}_{\mathbb{M}}))= N_{\mathbb{M}|\mathbb{K}}(c\mathcal{O}_{\mathbb{M}}))= N_{\mathbb{M}|\mathbb{K}}(\mathcal{J}^h) = N_{\mathbb{M}|\mathbb{K}}(\mathcal{J})^h$. Como $\mathcal{O}_{\mathbb{K}}$ é um domínio de Dedekind, segue que $N_{\mathbb{L}|\mathbb{K}}(N_{\mathbb{M}|\mathbb{L}}(\mathcal{J})) = N_{\mathbb{M}|\mathbb{K}}(\mathcal{J})$. ∎

Proposição 1.7.5 *Sejam $\mathbb{Q} \subseteq \mathbb{K}$ uma extensão finita de grau n e $\mathcal{O}_\mathbb{K}$ o anel dos inteiros de $\mathbb{K}$ sobre $\mathbb{Z}$. Então:*
i) Se $\mathcal{P} \subseteq \mathcal{O}_\mathbb{K}$ é um ideal primo então $\mathcal{P} \cap \mathbb{Z} = \langle p \rangle$, onde $p \in \mathbb{Z}$ é primo.
ii) $[\mathcal{O}_\mathbb{K}/\mathcal{P} : \mathbb{Z}_p] \leq n$.

Demonstração: i) Seja $\mathcal{P} \subseteq \mathcal{O}_\mathbb{K}$ um ideal primo. Como $\mathbb{Z} \subseteq \mathcal{O}_\mathbb{K}$ segue pelo Lema 1.5.1, que $\mathcal{P} \cap \mathbb{Z}$ é um ideal primo de $\mathbb{Z}$. Assim, como $\mathbb{Z}$ é um anel principal segue que $\mathcal{P} \cap \mathbb{Z} = \langle p \rangle$, onde $p \in \mathbb{Z}$ é um primo.
ii) Consideremos $\varphi : \mathbb{Z} \xrightarrow{i} \mathcal{O}_\mathbb{K} \xrightarrow{\pi} \mathcal{O}_\mathbb{K}/\mathcal{P}$, onde i é a inclusão e π é a projeção. A função $\varphi = \pi \circ i$ é um homomorfismo e $\ker(\varphi) = \mathbb{Z} \cap \mathcal{P} = \langle p \rangle$. Portanto, pelo Teorema do Homomorfismo, segue que $\mathbb{Z}/\mathcal{P} \cap \mathbb{Z} \simeq Im(\varphi) \subset \mathcal{O}_\mathbb{K}/\mathcal{P}$. Logo, $\mathbb{Z}/\langle p \rangle = \mathbb{Z}_p \subset \mathcal{O}_\mathbb{K}/\mathcal{P}$ é uma extensão de corpos. Se $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de $\mathcal{O}_\mathbb{K}$ como um $\mathbb{Z}$-módulo então $\{(\pi \circ i)\alpha_1, \cdots, (\pi \circ i)\alpha_n\}$ é um conjunto de geradores de $\mathcal{O}_\mathbb{K}/\mathcal{P}$ sobre $\mathbb{Z}_p$, pois se $\bar{\alpha} = \alpha + \mathcal{P} \in \mathcal{O}_\mathbb{K}/\mathcal{P}$ então $\bar{\alpha} = (a_1\alpha_1 + \cdots + a_n\alpha_n) + \mathcal{P} = (a_1 + \langle p \rangle)(\alpha_1 + \mathcal{P}) + \cdots + (a_n + \langle p \rangle)(\alpha_n + \mathcal{P})$. Portanto, $[\mathcal{O}_\mathbb{K}/\mathcal{P} : Z_p] \leq n$. ∎

Definição 1.7.2 *Sejam $\mathbb{K}$ um corpo de números e $\mathcal{O}_\mathbb{K}$ o anel dos inteiros de $\mathbb{K}$. O grau $[\mathcal{O}_\mathbb{K}/\mathcal{P} : \mathbb{Z}_p] = f$ é chamado grau de inércia de $\mathcal{P}$.*

Proposição 1.7.6 *Sejam $\mathbb{K}$ um corpo de números e $\mathcal{O}_\mathbb{K}$ o anel dos inteiros de $\mathbb{K}$. Se $\mathcal{P}$ é um ideal primo não nulo de $\mathcal{O}_\mathbb{K}$, então $N(\mathcal{P}) = p^f$, onde f é o grau de inércia de $\mathcal{P}$.*

Demonstração: Pela Proposição 1.7.5 segue que $\mathcal{O}_\mathbb{K}/\mathcal{P}$ é um espaço vetorial sobre $\mathbb{Z}_p$ de dimensão f. Portanto, $N(\mathcal{P}) = \#(\mathcal{O}_\mathbb{K}/\mathcal{P}) = p^f$. ∎

Proposição 1.7.7 *Sejam $\mathbb{Q} \subseteq \mathbb{K}$ uma extensão finita e $\mathcal{O}_\mathbb{K}$ o anel dos inteiros de $\mathbb{K}$. Então,*
i) $N(\mathcal{A}) \in \mathcal{A}$, onde $\mathcal{A} \subseteq \mathcal{O}_\mathbb{K}$ é um ideal.
ii) Se $\mathcal{A}$ é um ideal não nulo de $\mathcal{O}_\mathbb{K}$ então $N(\mathcal{A}) = 1$ se, e somente se, $\mathcal{A} = \mathcal{O}_\mathbb{K}$.

Demonstração: i) Como $N(\mathcal{A}) = \#\mathcal{O}_\mathbb{K}/\mathcal{A}$, segue que o grupo aditivo de $\mathcal{O}_\mathbb{K}/\mathcal{A}$ tem ordem $m = N(\mathcal{A})$. Assim, $m\bar{1} = \bar{0}$, sendo $\bar{1}$ e $\bar{0}$, respectivamente, a unidade e o zero do anel $\mathcal{O}_\mathbb{K}/\mathcal{A}$. Como, $\bar{m} = m\bar{1} = \bar{0}$ segue que $m + \mathcal{A} = 0 + \mathcal{A}$, e portanto, $m \in \mathcal{A}$. Logo, $N(\mathcal{A}) \in \mathcal{A}$.
ii) Temos que $N(\mathcal{A}) = 1$ se, e somente se, $\#\mathcal{O}_\mathbb{K}/\mathcal{A} = 1$ se, e somente se, $\mathcal{A} = \mathcal{O}_\mathbb{K}$. ∎

1.8 Anéis de frações

Nesta seção apresentamos o conceito de anéis de frações enfocando suas principais propriedades.

Definição 1.8.1 *Sejam A um domínio, $\mathbb{K}$ seu corpo de frações, S um subconjunto de $A-\{0\}$, que é fechado em relação a multiplicação e $1 \in S$. Chamamos de anel de frações de A o conjunto dos elementos de $\mathbb{K}$, que são escritos da forma $\frac{a}{s}$, com $a \in A$ e $s \in S$.*

Notação: $S^{-1}A$

Proposição 1.8.1 *Sejam A um domínio, $\mathbb{K}$ um corpo de frações, $S \subset A-\{0\}$ um subconjunto fechado em relação a multiplicação e $1 \in S$. Então:*
1) $S^{-1}A$ é um anel comutativo.
2) $A \subset S^{-1}A$.
3) Se $S = A - \{0\}$ então $S^{-1}A = \mathbb{K}$.
4) Se $S = \{1\}$ ou S é formado somente pela unidade de A então $S^{-1}A = A$.

Demonstração: 1) Se $x, y \in S^{-1}A$, então $x = \frac{a_1}{s_1}$ e $y = \frac{a_2}{s_2}$, com $a_1, a_2 \in A$ e $s_1 s_2 \in S$. Assim, $xy = \frac{a_1 a_2}{s_1 s_2} = \frac{a_2 a_1}{s_2 s_1} = yx$.
2) Se $x \in A$, então $x = \frac{x}{1}$, com $x \in A$ e $1 \in S$. Assim, $x = \frac{x}{1} \in S^{-1}A$.
3) Temos que $\mathbb{K} = \left\{\frac{a}{b}; a, b \in A \ e \ b \neq 0\right\} = \left\{\frac{a}{b}; a \in A \ e \ b \in A - \{0\}\right\} = \left\{\frac{a}{b}; a \in A \ e \ b \in S\right\} = S^{-1}A$.
4) Se $S = \{1\}$ temos que $S^{-1}A = \left\{\frac{a}{b}; a \in A \ e \ b \in S = \{1\}\right\} = \left\{\frac{a}{1}; a \in A\right\}$=A. Agora, se S é formado somente pela unidade de A então

$$S^{-1}A = \left\{\frac{a}{s}; a \in A \ e \ s \in S\right\} = \left\{as^{-1}; a \in A \ e \ s^{-1} \in S\right\} \subset A.$$

Portanto, $S^{-1}A = A$. ∎

Proposição 1.8.2 *Sejam A um domínio, S um subconjunto de $A - \{0\}$ fechado em relação a multiplicação com $1 \in S$ e $A' = S^{-1}A$.*
i) Se $\mathcal{B}' \subseteq A'$ é um ideal, então $(\mathcal{B}' \cap A)A' = \mathcal{B}'$ e a função $\varphi(\mathcal{B}') = \mathcal{B}' \cap A$ é uma injeção crescente do conjunto dos ideais de A' no conjunto dos ideais de A, com relação a inclusão.
ii) A aplicação $\varphi(\mathcal{P}') = \mathcal{P}' \cap A$ é uma bijeção crescente do conjunto dos ideais primos de A' no conjunto dos ideais primos $\mathcal{P}$ de A tal que $\mathcal{P} \cap S = \emptyset$ e a aplicação inversa é dada por $\phi(\mathcal{P}) = \mathcal{P}A'$.

Demonstração: i) Primeiramente vamos mostrar que $(\mathcal{B}' \cap A)A' = \mathcal{B}'$. Como $\mathcal{B}' \cap A \subseteq \mathcal{B}'$ segue que $(\mathcal{B}' \cap A)A' \subseteq \mathcal{B}'A'$=$\mathcal{B}'$. Por outro lado, seja $x \in \mathcal{B}' \subseteq A'$ então $x = \frac{a}{s}$, com $a \in A$ e $s \in S$. Como $\mathcal{B}'$ é um ideal de A' e $A \subseteq A'$ segue que $sx \in \mathcal{B}'$. Assim, $sx = a \in \mathcal{B}' \cap A$, e

então $x = a\frac{1}{s} \in (\mathcal{B}' \cap A)A'$, ou seja, $\mathcal{B}' \subseteq (\mathcal{B}' \cap A)A'$. Portanto, $\mathcal{B}' = (\mathcal{B}' \cap A)A'$. Também φ é uma injeção crescente, uma vez que se $\varphi(\mathcal{B}_1') = \varphi(\mathcal{B}_2')$ então $\mathcal{B}_1' \cap A = \mathcal{B}_2' \cap A$. Assim,

$$(\mathcal{B}_1' \cap A)A' = (\mathcal{B}_2' \cap A)A'$$

e isto implica que

$$\mathcal{B}_1' = \mathcal{B}_2'.$$

Se $\mathcal{B}_1' \subseteq \mathcal{B}_2'$ então $\mathcal{B}_1' \cap A \subseteq \mathcal{B}_2' \cap A$. Portanto, $\varphi(\mathcal{B}_1') \subseteq \varphi(\mathcal{B}_2')$. Para $ii)$ temos que φ esta bem definida, pois por $i)$ φ é uma injeção crescente e pelo Lema 1.5.1 se $\mathcal{P}' \subset A'$ é um ideal primo e como $A \subset A'$ então $\mathcal{P}' \cap A$ é ideal primo de A. Falta mostrar que $\mathcal{P} \cap S = \emptyset$. Suponha que exista $s \in \mathcal{P} \cap S$. Então $s \in \mathcal{P}$ e $s \in S$. Como $\mathcal{P} \subseteq \mathcal{P}'$ então $s \in \mathcal{P}'$ e $\frac{1}{s} \in A'$ e portanto $1 = s\frac{1}{s} \in \mathcal{P}'A' = \mathcal{P}'$. Assim, $\mathcal{P}' = A'$, o que é um absurdo, pois $\mathcal{P}'$ é ideal primo de A'. Portanto, $\mathcal{P} \cap S = \emptyset$ e φ esta bem definida. Agora, vamos mostrar que $\phi(\mathcal{P}) = \mathcal{P}A'$ está bem definida. Seja $\mathcal{P} \subset A$ um ideal primo tal que $\mathcal{P} \cap S = \emptyset$. Então, $\phi(\mathcal{P}) = \mathcal{P}A' \subset A'$. Temos que $\mathcal{P}A' = \left\{\frac{p}{s} : p \in \mathcal{P} \ e \ s \in S\right\}$, uma vez que se $x \in \mathcal{P}A'$ então

$$x = \sum_{i=1}^{n} p_i \frac{a_i}{s_i} \text{ com } \ p_i \in \mathcal{P}, a_i \in \mathcal{P}A' \text{ e } s_i \in S.$$

Assim,

$$x = \frac{b_1p_1 + \cdots + b_np_n}{s} \text{ com } p_i \in A.$$

Logo, $x = \frac{p}{s}$ com $p \in \mathcal{P}$ e $s \in S$, o que prova nossa afirmação. Agora, sejam $x = \frac{a}{s} \in A'$ e $y = \frac{b}{t} \in A'$ tal que $xy = \frac{ab}{st} \in \mathcal{P}A'$. Assim,

$$\frac{ab}{st} = \frac{p}{u} \text{ com } p \in \mathcal{P} \text{ e } u \in S.$$

Logo, $abu = pst \in \mathcal{P}$. Como $u \in S$ e $u \notin \mathcal{P}$ e como $\mathcal{P}$ é primo segue que $ab \in \mathcal{P}$. Assim, $a \in \mathcal{P}$ ou $b \in \mathcal{P}$, e portanto, $\frac{a}{s} \in \mathcal{P}A'$ ou $\frac{b}{t} \in \mathcal{P}A'$. Portanto, $\mathcal{P}A'$ é ideal primo de A'. Mostremos que $\mathcal{P}A' \cap A = \mathcal{P}$. Como $\mathcal{P} \subseteq A$ e $\mathcal{P} \subseteq \mathcal{P}A'$ segue que $\mathcal{P} \subseteq \mathcal{P}A' \cap A$. Por outro lado, se $x \in \mathcal{P}A' \cap A$ então $x \in \mathcal{P}A'$ e $x \in A$. Assim, $x = \frac{p}{s}$, com $p \in \mathcal{P}$ e $s \in S$, e então $sx \in \mathcal{P}$. Como $s \notin \mathcal{P}$, temos que $x \in \mathcal{P}$, pois $\mathcal{P}$ é ideal primo de A. Portanto, $\mathcal{P}A' \cap A = \mathcal{P}$. Finalmente, temos que $(\varphi \circ \phi)(\mathcal{P}) = \varphi(\phi(\mathcal{P})) = \varphi(\mathcal{P}A') = \mathcal{P}A' \cap A = \mathcal{P}$ e $(\phi \circ \varphi)(\mathcal{P}') = \phi(\varphi(\mathcal{P}')) = \phi(\mathcal{P}' \cap A) = (\mathcal{P}' \cap A)A' = \mathcal{P}'$. Portanto, $\varphi = \phi^{-1}$. ∎

Corolário 1.8.1 *Com as notações da Proposição 1.8.2, se A é um anel noetheriano, então A' é um anel noetheriano.*

Demonstração: Seja a função $\varphi : \{\text{conjunto dos ideais de } A'\} \longrightarrow \{\text{conjunto dos ideais de } A\}$ definida por $\varphi(\mathcal{B}') = \mathcal{B}' \cap A$. Pela Proposição 1.8.2, temos que φ é uma injeção crescente. Se $(\mathcal{B}'_n)_{n>0}$ é uma sequência crescente de ideais de A', então $(\varphi(\mathcal{B}'_n))_{n>0}$ é uma sequência crescente de ideais em A. Como A é noetheriano, então existe $n_0 \in \mathbb{N}$ tal que $\varphi(\mathcal{B}'_n) = \varphi(\mathcal{B}'_{n+1}), \forall n \geq n_0$. Como φ é injetora, temos que $\mathcal{B}'_n = \mathcal{B}'_{n+1}, \forall n \geq n_0$. Assim, $(\mathcal{B}'_n)_{n>0}$ é estacionária. Portanto, A' é noetheriano. ∎

Corolário 1.8.2 *Se A é um domínio de Dedekind, $\mathcal{P} \subset A$ é um ideal primo, S=A-$\mathcal{P}$ e $\mathcal{I}$ é um ideal de A tal que $\mathcal{I} = \prod_{i=1}^{r} \mathcal{P}_i^{e_i}$, onde $\mathcal{P}_i$, $i = 1, \cdots, n$, são ideais primos de A, então a decomposição de $A'\mathcal{I}$ em ideais primos de $A' = S^{-1}A$ é dado por $A'\mathcal{I} = \prod_{\mathcal{P}_i \cap S = \emptyset} (A'\mathcal{P}_i)^{e_i}$.*

Demonstração: Se $\mathcal{P}'$ é um ideal primo não nulo de A', então pela Proposição 1.8.2, segue que $\mathcal{P}' \cap A = \mathcal{P}$ é um ideal primo de A tal que $\mathcal{P} \cap S = \emptyset$. Também $\mathcal{P} \neq 0$, pois $\mathcal{P}' = A'\mathcal{P}$. Assim, $\mathcal{P}$ é um ideal maximal de A. Pela Proposição 1.8.2, segue que $\mathcal{P}'$ é um ideal maximal de A'. Como $\mathcal{I} = \prod_{i=1}^{r} \mathcal{P}_i^{e_i}$ segue que $A'\mathcal{I} = A'\left(\prod_{i=1}^{r} \mathcal{P}_i^{e_i}\right) = \prod_{i=1}^{r} (A'\mathcal{P}_i)^{e_i} = \prod_{\mathcal{P}_i \cap S = \emptyset} (A'\mathcal{P}_i)^{e_i}$. Finalmente, se $\mathcal{P}_i \cap S \neq \emptyset$ então $A'\mathcal{P}_i = A'$ e se $\mathcal{P}_i \cap S = \emptyset$ então $A'\mathcal{P}_i$ é um ideal primo de A', para $i = 1, \cdots, n$. ∎

Proposição 1.8.3 *Se $\mathcal{I}$ é um ideal de um anel A, então $\mathcal{I} = \bigcap_i A'_i\mathcal{I}$, onde $A'_i = S_i^{-1}A$, $S_i = A - \mathcal{P}_i$ e $\mathcal{P}_i$ um ideal maximal de A.*

Demonstração: O resultado é verdadeiro quando A é um corpo, pois os únicos ideais de A são os triviais. Suponha que A não é um corpo. Se $x \in \bigcap_i A'_i\mathcal{I}$, então $x = \frac{a_i}{b_i}$, com $a_i \in \mathcal{I}$, $b_i \in A$ e $b_i \notin \mathcal{P}_i$, para todo i. Seja $\mathcal{J}$ o ideal de A gerado pelos elementos b_i. Como $b_i \notin \mathcal{P}_i$, segue que $\mathcal{J} \nsubseteq \mathcal{P}_i$, para todo ideal maximal $\mathcal{P}_i$. Assim, $\mathcal{J} = A$, pois sabemos que todo ideal de A, diferente de A está contido em um ideal maximal. Assim, 1 pode ser expresso em termos dos geradores de $\mathcal{J} = A$, isto é, existem elementos $c_{i1}, \cdots, c_{im} \in A$ tal que $1 = \sum_{k=1}^{m} c_{ik}b_{ik}$. Assim, $x = \sum_{k=1}^{m} c_{ik}(b_{ik}x) = \sum_{k=1}^{m} c_{ik}a_{ik} \in \mathcal{I}$. Portanto, $\bigcap_i A'_i\mathcal{I} \subset \mathcal{I}$. Como $\mathcal{I} \subset \bigcap_i A'_i\mathcal{I}$ segue que $\mathcal{I} = \bigcap_i A'_i\mathcal{I}$. ∎

Proposição 1.8.4 *Seja B um domínio, $A \subset B$ subanel e $S \subset A$ um subconjunto, com $1 \in S$ e fechado em relação a multiplicação. Se $\mathcal{O}_B$ é o anel dos inteiros de A em B. Então $\mathcal{O}'_B$ é o anel dos inteiros de A' em B'.*

Demonstração: Se $x \in \mathcal{O}_B^{'}$, então $x = \dfrac{b}{s}$ com $b \in \mathcal{O}_B$ e $s \in S$. Como $\mathcal{O}_B$ é inteiro sobre A, então

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0, \tag{1.4}$$

onde $a_i \in A$, $i = 0, 1, \cdots, n-1$, não todos nulos. Dividindo a equação (1.4) por s^n obtemos que

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

Como $\dfrac{a_i}{s} \in A^{'}$ e não são todos nulos, segue que $x = \dfrac{b}{s}$ é inteiro sobre $A^{'}$. Agora vamos mostrar que todo elemento de $B^{'}$ que é inteiro sobre $A^{'}$ pertence $\mathcal{O}_B^{'}$. Para isso, seja $x \in B^{'}$ inteiro sobre $A^{'}$. Então

$$x^n + \frac{a_{n-1}}{s_{n-1}}x^{n-1} + \cdots + \frac{a_0}{s_0} = 0 \tag{1.5}$$

com $\dfrac{a_i}{s_i} \in A^{'}$, $i = 0, 1, \cdots, n-1$, não todos nulos. Multiplicando a equação (1.5) por s^n, onde $s = s_0 s_1 \cdots s_{n-1}$ obtemos que $(sx)^n + a_{n-1}(sx)^{n-1} + \cdots + b_0 = 0$, onde $b_i \in$A, para $i = 0, 1, \cdots, n-1$ não são todos nulos. Logo, $sx \in \mathcal{O}_B$ e assim $sx = b$, com $b \in \mathcal{O}_B$. Portanto, $x = \dfrac{b}{s}$ onde $b \in \mathcal{O}_B$ e $s \in S$. Portanto, $x \in \mathcal{O}_B^{'}$. ∎

Corolário 1.8.3 *Se A é um anel integralmente fechado então $A^{'}$ é integralmente fechado.*

Demonstração: Seja $\mathbb{K}$ o corpo de frações do anel A e seja $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ sobre A. Como A é integralmente fechado, temos que $A = \mathcal{O}_{\mathbb{K}}$, e assim pela Proposição 1.8.4, $A^{'} = \mathcal{O}_{\mathbb{K}}^{'}$. ∎

Teorema 1.8.1 *Se A é um anel de Dedekind, então $A^{'}$ é um anel de Dedekind.*

Demonstração: Temos pelo Corolário 1.8.3, que $A^{'}$ é um anel Noetheriano e integralmente fechado, respectivamente. Então falta mostrar que todo ideal primo não nulo de $A^{'}$ é maximal. Assim, se $\mathcal{P}^{'} \subset A^{'}$ é um ideal primo não nulo então, pelo Lema 1.5.1, segue que $\mathcal{P}^{'} \cap A$ é um ideal primo de A, e portanto maximal. Assim, pela Proposição 1.8.2, segue que se $\mathcal{P}^{'} \subseteq \mathcal{M}^{'} \subseteq A^{'}$ então $\varphi(\mathcal{P}^{'}) \subseteq \varphi(\mathcal{M}^{'}) \subseteq \varphi(A^{'})$. Como $\varphi(\mathcal{P}^{'})$ é maximal então $\varphi(\mathcal{P}^{'}) = \varphi(\mathcal{M}^{'})$ ou $\varphi(\mathcal{M}^{'}) = \varphi(A^{'})$. Logo, $\mathcal{P}^{'} = \mathcal{M}^{'}$ ou $\mathcal{M}^{'} = A^{'}$. Portanto, $\mathcal{P}^{'}$ é maximal. ∎

Proposição 1.8.5 *Se A é um anel de Dedekind e $S \subset A$ um subconjunto tal que $S = A - \mathcal{P}$, onde $\mathcal{P} \subset A$ é um ideal primo então $A^{'}$ é principal, ou seja, existe $p \in A^{'}$ tal que os ideais de $A^{'}$ são da forma $\langle p^n \rangle, n \geq 0$.*

Demonstração: Temos que $\mathcal{P} \subset A$ é o único ideal primo não nulo de A tal que $\mathcal{P} \cap S = \emptyset$, pois se existisse um outro ideal primo $\mathcal{P}_1 \subset A$ tal que $\mathcal{P}_1 \cap S = \emptyset$, teríamos que $\mathcal{P}_1 \subset \mathcal{P}$. Como A é Dedekind, segue que $\mathcal{P}_1 = \mathcal{P}$. Pela Proposição 1.8.2, segue que $\mathcal{P}A' = \mathcal{B}$ é o único ideal primo de A'. Mas A' é Dedekind, então todo ideal de A' é do tipo $\mathcal{B}^n$ com $n \geq 0$. Assim,

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

Se $p \in \mathcal{B} - \mathcal{B}^2$ então $\langle p \rangle$ é ideal de A'. Assim, $\langle p \rangle = \mathcal{B}^{n_0}$, para algum n_0, e $\langle p \rangle \not\subset \mathcal{B}^2$. Logo, $n_0 = 1$, e portanto $\langle p \rangle = \mathcal{B}$. Assim $\langle p^n \rangle = \mathcal{B}^n$. Portanto, A' é principal e todos os seus ideais são da forma $\langle p^n \rangle$, com $n \geq 0$. ∎

Teorema 1.8.2 *Sejam A um domínio, $S \subset A$ um subconjunto tal que $0 \notin S$, $1 \in S$ e fechado no produto. Seja $\mathcal{M}$ um ideal maximal de A tal que $\mathcal{M} \cap S = \emptyset$. Então $A'/\mathcal{M}A' \simeq A/\mathcal{M}$.*

Demonstração: Sendo $\mathcal{M}$ um ideal maximal de A, segue que $\mathcal{M}$ também é um ideal primo de A. Assim, pela Proposição 1.8.2, segue que $\mathcal{M}A'$ é um ideal primo de A'. Seja a aplicação $\varphi : A \xrightarrow{i} A' \xrightarrow{\pi} A'/\mathcal{M}A'$, onde i é a inclusão e π é a projeção. Temos que $\ker(\varphi) = \mathcal{M}A' \cap A = \mathcal{M}$, pois $\varphi(x) = \bar{0}$ se, e somente se $x + \mathcal{M}A' = \bar{0}$ se, e somente se, $x \in \mathcal{M}A'$ e $x \in A$. Portanto, $\ker(\varphi) = \mathcal{M}A' \cap A = \mathcal{M}$, onde a última igualdade segue da Proposição 1.8.2. Falta mostrar que φ é sobrejetora. Para isso, seja $\bar{x} \in A'/\mathcal{M}A'$. Assim, $\bar{x} = x + \mathcal{M}A'$, com $x = \frac{a}{s}, a \in A$ e $s \in S$. Como $\mathcal{M} \cap S = \emptyset$ segue que $s \notin \mathcal{M}$ e como $\mathcal{M}$ é maximal segue que $A/\mathcal{M}$ é um corpo. Logo, $\bar{s} = s + \mathcal{M} \neq 0$ é inversível, ou seja, existe $\bar{b} \in A/\mathcal{M}$ tal que $\bar{s}\bar{b} = \bar{1}$. Assim, $sb - 1 \in \mathcal{M}$. Deste modo, $\frac{a}{s} - ab = \frac{a}{s}(1 - sb) \in \mathcal{M}A'$. Portanto, $\varphi(ab) = ab + \mathcal{M}A' = x + \mathcal{M}A'$ se, e somente se, $x - ab \in \mathcal{M}A'$. Portanto, existe $ab \in A$ tal que $\varphi(ab) = x + \mathcal{M}A'$. Portanto, $A'/\mathcal{M}A' \simeq A/\mathcal{M}$. ∎

Capítulo 2

Ramificação e Discriminante

Neste capítulo introduzimos primeiramente o conceito de ramificação e apresentamos algumas propriedades incluindo o Teorema da Igualdade Fundamental. Também apresentamos o conceito de ramificação em corpos quadráticos. Em seguida, apresentamos o conceito de discriminante e também a relação entre ramificação e discriminante. Na penúltima seção apresentamos o Teorema de Kummer, o qual nos apresenta um método de de decomposição através de polinômios. Finalizando, apresentamos o conceito de reticulado como um subconjunto discreto do $\mathbb{R}^n$ e depois através da Teoria dos Números Algébricos apresentamos um método de gerarmos reticulados. Neste capítulo foram utilizadas as seguintes referências [1], [2], [3], [4], [5], [6] e [7].

2.1 Ramificação

Sejam 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 do inteiros de A em $\mathbb{L}$. Pelo Teorema 1.6.1, Capítulo 1, segue que $\mathcal{O}_{\mathbb{L}}$ é um anel de Dedekind. Apresentamos nesta seção a decomposição de ideais primos não nulos $\mathcal{P}$ de A na extensão $\mathbb{L}$, ou seja, veremos que o ideal estendido $\mathcal{P}\mathcal{O}_{\mathbb{L}}$ de $\mathcal{O}_{\mathbb{L}}$, é expresso de modo único na forma $\mathcal{P}\mathcal{O}_{\mathbb{L}}= \prod_{i=1}^{g} \mathcal{Q}_i^{e_i}$, onde os $\mathcal{Q}_i$ são ideais primos de $\mathcal{O}_{\mathbb{L}}$ e os e_i são elementos de $\mathbb{Z}$, para $i = 1, \cdots, g$.

Proposição 2.1.1 *Os ideais primos $\mathcal{Q}_i$ de $\mathcal{O}_{\mathbb{L}}$ são os únicos ideais primos de $\mathcal{O}_{\mathbb{L}}$ tais que $\mathcal{Q}_i \cap A = \mathcal{P}$, para $i = 1, \cdots, g$.*

Demonstração: Seja $\mathcal{D}$ um ideal primo de $\mathcal{O}_{\mathbb{L}}$. Então $\mathcal{D} \cap A = \mathcal{P}$ se, e somente se, $\mathcal{D} \supset \mathcal{P}\mathcal{O}_{\mathbb{L}}$. De fato, se $\mathcal{D} \cap A = \mathcal{P}$, então $\mathcal{P} \subset \mathcal{D}$ e portanto $\mathcal{P}\mathcal{O}_{\mathbb{L}} \subset \mathcal{D}\mathcal{O}_{\mathbb{L}} = \mathcal{D}$. Por outro lado, se

$\mathcal{D} \supset \mathcal{P}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} \mathcal{Q}_i^{e_i}$, pelo Lema 1.5.2, segue que $\mathcal{D} \supset \mathcal{Q}_i$, para algum i. Como $\mathcal{Q}_i$ é maximal, pois $\mathcal{O}_{\mathbb{L}}$ é Dedekind, segue que $\mathcal{Q}_i = \mathcal{D}$. Como $\mathcal{D} \subset \mathcal{O}_{\mathbb{L}}$ e $A \subset \mathcal{O}_{\mathbb{L}}$, pelo Lema 1.5.1, temos que $\mathcal{D} \cap A$ é um ideal primo de A e também $\mathcal{D} \cap A \subsetneq A$, pois $1 \notin \mathcal{D}$. Agora, como $\mathcal{P} \subset \mathcal{D}$ e $\mathcal{P} \subset A$, segue que $\mathcal{P} \subset A \cap \mathcal{D}$. Como A é Dedekind, segue que $\mathcal{P} = A \cap \mathcal{D}$, pois $\mathcal{P}$ é maximal. Portanto, $\mathcal{P} = A \cap \mathcal{Q}_i$. Assim, $\mathcal{D}$ está na fatoração de $\mathcal{P}\mathcal{O}_{\mathbb{L}}$ se, e somente se, $\mathcal{D} \cap A = \mathcal{P}$. ■

Definição 2.1.1 *Se $\mathcal{P} = A \cap \mathcal{D}$, dizemos que $\mathcal{D}$ está acima de $\mathcal{P}$.*

Lema 2.1.1 *Com as notações anteriores temos que*
1) $A/\mathcal{P}$ e $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i$ são corpos e que $A/\mathcal{P}$ pode ser identificado como um subcorpo de $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i$.
2) Como $\mathcal{O}_{\mathbb{L}}$ é um A-módulo finitamente gerado, então $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i$ é um espaço vetorial de dimensão finita sobre $A/\mathcal{P}$, para $i = 1, \cdots, n$.

Demonstração: 1) Como A e $\mathcal{O}_{\mathbb{L}}$ são anéis de Dedekind, segue que $A/\mathcal{P}$ e $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i$, $i = 1, \cdots, g$, são corpos. Agora, consideramos a aplicação $A \xrightarrow{i} \mathcal{O}_{\mathbb{L}} \xrightarrow{\pi} \mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i$, onde i é a inclusão e π é a projeção. Temos que $\ker(\pi \circ i) = \mathcal{Q}_i \cap A = \mathcal{P}$. Pelo Teorema do Homomorfismo segue que $A/\mathcal{P} \simeq Im(\pi \circ i)$. Portanto, $A/\mathcal{P}$ pode ser identificado como um subcorpo de $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i$.
2) Considerando as operações

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

temos que $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i$ é um espaço vetorial sobre $A/\mathcal{P}$ e que $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i$ tem dimensão finita, pois sendo $\{x_1, \cdots, x_n\}$ os geradores de $\mathcal{O}_{\mathbb{L}}$ sobre A, e $b \in \mathcal{O}_{\mathbb{L}}$, então $b = a_1x_1 + \cdots + a_nx_n$, com $a_i \in A, i = 1, \cdots, n$. Assim, $\bar{b} = \bar{a}_1\bar{x}_1 + \cdots + \bar{a}_n\bar{x}_n$, com $\bar{a}_i = a_i + \mathcal{P}$. Portanto, $\{\bar{x}_1, \cdots, \bar{x}_n\}$ gera $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i$ como um espaço vetorial sobre $A/\mathcal{P}$. ■

Definição 2.1.2 *O grau $f_i = f(\mathcal{Q}_i|\mathcal{P})$ da extensão $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i$ sobre $A/\mathcal{P}$ é chamado de grau de inércia de $\mathcal{O}_{\mathbb{L}}$ sobre A, e o expoente $e_i = e(\mathcal{Q}_i|\mathcal{P})$ é chamado de índice de ramificação de $\mathcal{Q}_i$ sobre A.*

Definição 2.1.3 *Dizemos que $\mathcal{P}$ é:*
*a) **totalmente decomposto em $\mathbb{L}$** (ou em $\mathcal{O}_{\mathbb{L}}$) quando $e(\mathcal{Q}|\mathcal{P}) = f(\mathcal{Q}|\mathcal{P}) = 1$, para todo ideal primo $\mathcal{Q}$ que esta acima de $\mathcal{P}$.*
*b) **inerte em $\mathbb{L}$** (ou em $\mathcal{O}_{\mathbb{L}}$) quando $e(\mathcal{Q}|\mathcal{P}) = 1$ e $f(\mathcal{Q}|\mathcal{P}) = n$, para todo ideal primo $\mathcal{Q}$ que esta acima de $\mathcal{P}$.*

c) ***totalmente ramificado em L*** *(ou em $\mathcal{O}_{\mathbb{L}}$) quando $e(\mathcal{Q}|\mathcal{P}) = n$ e $f(\mathcal{Q}|\mathcal{P}) = 1$, para todo ideal primo $\mathcal{Q}$ que esta acima de $\mathcal{P}$.*
d) ***ramificado em L*** *(ou em $\mathcal{O}_{\mathbb{L}}$) se existir um ideal primo $\mathcal{Q}_i$ de $\mathcal{O}_{\mathbb{L}}$ que esta acima de $\mathcal{P}$ tal que $e_i > 1$ para algum i.*

Lema 2.1.2 *Com as notações acima temos que*
1) $\mathcal{P}\mathcal{O}_{\mathbb{L}} \cap A = \mathcal{P}$
2) $\mathcal{O}_{\mathbb{L}}/\mathcal{P}\mathcal{O}_{\mathbb{L}}$ é um espaço vetorial de dimensão finita sobre $A/\mathcal{P}$.

Demonstração: 1) Como $\mathcal{P} \subset \mathcal{P}\mathcal{O}_{\mathbb{L}}$ e $\mathcal{P} \subset A$, segue que $\mathcal{P} \subset \mathcal{P}\mathcal{O}_{\mathbb{L}} \cap A$. Por outro lado, se

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

então $\mathcal{P}\mathcal{O}_{\mathbb{L}} \subset \mathcal{Q}_i$, para $i = 1, \cdots, g$. Logo, $\mathcal{P}\mathcal{O}_{\mathbb{L}} \cap A \subset \mathcal{Q}_i \cap A = \mathcal{P}$. Para 2) consideramos

$$A \xrightarrow{i} \mathcal{O}_{\mathbb{L}} \xrightarrow{\pi} \mathcal{O}_{\mathbb{L}}/\mathcal{P}\mathcal{O}_{\mathbb{L}},$$

onde i é a inclusão e π é a projeção. Temos que $\ker(\pi \circ i) = \mathcal{P}\mathcal{O}_{\mathbb{L}} \cap A = \mathcal{P}$. Pelo Teorema do Homomorfismo, segue que $A/\mathcal{P} \simeq Im(\pi \circ i)$. Portanto, $A/\mathcal{P}$ pode ser identificado com um subcorpo de $\mathcal{O}_{\mathbb{L}}/\mathcal{P}\mathcal{O}_{\mathbb{L}}$. Como $\mathcal{O}_{\mathbb{L}}$ é um A-módulo finitamente gerado, então analogamente ao item 2) do Lema 2.1.1, provamos que $\mathcal{O}_{\mathbb{L}}/\mathcal{P}\mathcal{O}_{\mathbb{L}}$ é um espaço vetorial de dimensão finita sobre $A/\mathcal{P}$. ∎

Lema 2.1.3 *A sequência de ideais*

$$\mathcal{O}_{\mathbb{L}} \supset \mathcal{Q}_1 \supset \mathcal{Q}_1^2 \supset \cdots \supset \mathcal{Q}_1^{e_1} \supset \mathcal{Q}_1^{e_1}\mathcal{Q}_2 \supset \cdots \supset \mathcal{Q}_1^{e_1}\mathcal{Q}_2^{e_2} \supset \cdots \supset \mathcal{Q}_1^{e_1} \cdots \mathcal{Q}_g^{e_g} = \mathcal{P}\mathcal{O}_{\mathbb{L}}$$

é maximal.

Demonstração: Dois elementos desta sequência são da forma $\mathcal{Q}$ e $\mathcal{Q}\mathcal{Q}_i$, onde $\mathcal{Q}$ é o produto de ideais $\mathcal{Q}_j$. Se existir $\mathcal{D}$ tal que $\mathcal{Q}\mathcal{Q}_i \subset \mathcal{D} \subset \mathcal{Q}$ segue pelo Lema 1.6.2 que $\mathcal{D}$ divide $\mathcal{Q}\mathcal{Q}_i$. Assim, existe $\mathcal{C}_1 \subset \mathcal{O}_{\mathbb{L}}$ tal que $\mathcal{Q}\mathcal{Q}_i = \mathcal{D}\mathcal{C}_1$. De modo análogo, $\mathcal{Q}$ divide $\mathcal{D}$, ou seja, existe $\mathcal{C}_2 \subset \mathcal{O}_{\mathbb{L}}$ tal que $\mathcal{D} = \mathcal{Q}\mathcal{C}_2$. Logo, $\mathcal{Q}_i \subseteq \mathcal{C}_1 \subseteq \mathcal{O}_{\mathbb{L}}$ e $\mathcal{Q}_i \subseteq \mathcal{C}_2 \subseteq \mathcal{O}_{\mathbb{L}}$. Como $\mathcal{Q}_i$ é maximal, segue que $\mathcal{Q}_i = \mathcal{C}_2$ ou $\mathcal{C}_2 = \mathcal{O}_{\mathbb{L}}$. Se $\mathcal{Q}_i = \mathcal{C}_2$ então $\mathcal{D} = \mathcal{Q}\mathcal{Q}_i$, e se $\mathcal{C}_2 = \mathcal{O}_{\mathbb{L}}$ então $\mathcal{D} = \mathcal{Q}$. Portanto, não existe ideal não trivial entre $\mathcal{Q}\mathcal{Q}_i$ e $\mathcal{Q}$. ∎

Teorema 2.1.1 *(Teorema da Igualdade Fundamental)* $\sum_{i=1}^{g} e_i f_i = [\mathcal{O}_{\mathbb{L}}/\mathcal{P}\mathcal{O}_{\mathbb{L}} : A/\mathcal{P}] = n.$

Demonstração: Vamos provar a primeira igualdade. Pela demonstração do Lema 2.1.1, temos que $\mathcal{Q}/\mathcal{Q}\mathcal{Q}_i$ é um espaço vetorial sobre $\mathcal{O}_\mathbb{L}/\mathcal{Q}_i$, e pelo Lema 2.1.3 temos que seus subespaços são os triviais. Assim, $\dim_{\mathcal{O}_\mathbb{L}/\mathcal{Q}_i} \mathcal{Q}/\mathcal{Q}\mathcal{Q}_i = 1$ e $\#\mathcal{O}_\mathbb{L}/\mathcal{Q}_i = \#\mathcal{Q}/\mathcal{Q}\mathcal{Q}_i$. Como $[\mathcal{O}_\mathbb{L}/\mathcal{Q}_i : A/\mathcal{P}] = f_i$ e $[\mathcal{Q}/\mathcal{Q}\mathcal{Q}_i : \mathcal{O}_\mathbb{L}/\mathcal{Q}_i] = 1$ temos que $[\mathcal{Q}/\mathcal{Q}\mathcal{Q}_i : A/\mathcal{P}] = f_i$. Dado um índice i, observemos que existem exatamente e_i elementos consecutivos na sequência dos ideais com o quociente da forma $\mathcal{Q}/\mathcal{Q}\mathcal{Q}_i$, ou seja, de dimensão f_i sobre $A/\mathcal{P}$. A dimensão total de $[\mathcal{O}_\mathbb{L}/\mathcal{P}\mathcal{O}_\mathbb{L} : A/\mathcal{P}]$ é igual a soma das dimensões dos quocientes, ou seja,

$$[\mathcal{O}_\mathbb{L}/\mathcal{P}\mathcal{O}_\mathbb{L} : A/\mathcal{P}] = e_1 f_1 + \cdots + e_g f_g = \sum_{i=1}^{g} e_i f_i.$$

Agora vamos provar a segunda igualdade. Se A é principal, pelo Corolário 1.2.3 temos que $\mathcal{O}_\mathbb{L}$ é um A-módulo livre de posto n. Se $\{x_1, \cdots, x_n\}$ é uma base de $\mathcal{O}_\mathbb{L}$ sobre A, temos que $\{x_1 + \mathcal{P}\mathcal{O}_\mathbb{L}, \cdots, x_n + \mathcal{P}\mathcal{O}_\mathbb{L}\}$ é uma base de $\mathcal{O}_\mathbb{L}/\mathcal{P}\mathcal{O}_\mathbb{L}$ sobre $A/\mathcal{P}$. De fato, se $\bar{b} \in \mathcal{O}_\mathbb{L}/\mathcal{P}\mathcal{O}_\mathbb{L}$ temos que $\bar{b} = b + \mathcal{P}\mathcal{O}_\mathbb{L}$, e então

$$\begin{aligned}(a_1x_1 + \cdots + a_nx_n) + \mathcal{P}\mathcal{O}_\mathbb{L} &= (a_1x_1 + \mathcal{P}\mathcal{O}_\mathbb{L}) + \cdots + (a_nx_n + \mathcal{P}\mathcal{O}_\mathbb{L}) \\ &= (a_1 + \mathcal{P})(x_1 + \mathcal{P}\mathcal{O}_\mathbb{L}) + \cdots + (a_n + \mathcal{P})(x_n + \mathcal{P}\mathcal{O}_\mathbb{L}) \\ &= \quad \bar{a_1}\bar{x_1} + \cdots + \bar{a_n}\bar{x_n},\end{aligned}$$

com $\bar{a_i} \in A/\mathcal{P}$, $i = 1, \cdots, n$. Agora, se $\bar{a_1}\bar{x_1} + \cdots + \bar{a_n}\bar{x_n} = \bar{0}$ então

$$a_1x_1 + \cdots + a_nx_n = \sum_{j=1}^{s} b_jp_j, \text{ com } b_j \in \mathcal{O}_\mathbb{L} \text{ e } p_j \in \mathcal{P}, j = 1, \cdots, s.$$

Como $\{x_1, \cdots, x_n\}$ gera $\mathcal{O}_\mathbb{L}$ sobre A, segue que $b_j = \sum_{i=1}^{n} c_{ij}x_i$, com $c_{ij} \in A$, para $j = 1, \cdots, n$. Então

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

Como $\{x_1, \cdots, x_n\}$ é linearmente independente, segue que $a_i = \sum_{j=1}^{s} c_{ij}p_j \in \mathcal{P}$, ou seja, $\bar{a}_i = \bar{0}$, para $i = 1, \cdots, n$. A demonstração para o caso geral é feita por redução ao caso anterior. Temos que A é um anel de Dedekind. Se $\mathcal{P}$ é um ideal primo não nulo de A e se $S = A - \mathcal{P}$, temos pela Proposição 1.8.5, que $S^{-1}A$ é um anel principal e pela Proposição 1.8.4, que $S^{-1}\mathcal{O}_\mathbb{L}$ é anel dos inteiros de $\mathbb{L}$ sobre $S^{-1}A$ e $S^{-1}\mathcal{O}_\mathbb{L}$ é um $S^{-1}A$-módulo livre. Daí, pelo caso anterior, temos que $[S^{-1}\mathcal{O}_\mathbb{L}/S^{-1}\mathcal{O}_\mathbb{L}\mathcal{P} : S^{-1}A/S^{-1}A\mathcal{P}] = n$. Considerando a fatoração do ideal $\mathcal{P}S^{-1}\mathcal{O}_\mathbb{L} = \prod_{i=1}^{g}(S^{-1}\mathcal{O}_\mathbb{L}\mathcal{Q}_i)^{e_i}$ e como $\mathcal{Q}_i \cap A = \mathcal{P}$, $\mathcal{Q}_i \cap S = \emptyset$ e $S^{-1}\mathcal{O}_\mathbb{L}\mathcal{Q}_i$ são ideais primos não nulos de

$S^{-1}\mathcal{O}_{\mathbb{L}}$, temos pela primeira parte que

$$\left[S^{-1}\mathcal{O}_{\mathbb{L}}/\mathcal{P}S^{-1}\mathcal{O}_{\mathbb{L}} : S^{-1}A/\mathcal{P}S^{-1}A\right] = \sum_{i=1}^{g} e_i \left[S^{-1}\mathcal{O}_{\mathbb{L}}/S^{-1}\mathcal{O}_{\mathbb{L}}\mathcal{Q}_i : S^{-1}A/\mathcal{P}S^{-1}A\right].$$

Porém pelo Teorema 1.8.2, temos que $S^{-1}A/\mathcal{P}S^{-1}A \simeq A/\mathcal{P}$ e $S^{-1}\mathcal{O}_{\mathbb{L}}/S^{-1}\mathcal{O}_{\mathbb{L}}\mathcal{Q}_i \simeq \mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i$. Portanto, $n = [S^{-1}\mathcal{O}_{\mathbb{L}}/S^{-1}\mathcal{O}_{\mathbb{L}}\mathcal{Q}_i : S^{-1}A/\mathcal{P}S^{-1}A] = \sum_{i=1}^{g} e_i f_i$. ∎

Lema 2.1.4 *Se $\mathcal{A}_1, \mathcal{A}_2$ são ideais de um anel A e $\mathcal{A}_1 + \mathcal{A}_2 = A$ então $\mathcal{A}_1\mathcal{A}_2 = \mathcal{A}_1 \cap \mathcal{A}_2$.*

Demonstração: Temos que $\mathcal{A}_1\mathcal{A}_2 \subset \mathcal{A}_1$ e $\mathcal{A}_1\mathcal{A}_2 \subset \mathcal{A}_2$ e assim $\mathcal{A}_1\mathcal{A}_2 \subset \mathcal{A}_1 \cap \mathcal{A}_2$. Agora, suponhamos que $x \in \mathcal{A}_1 \cap \mathcal{A}_2$. Por hipótese, $\mathcal{A}_1 + \mathcal{A}_2 = A$, assim, existem elementos $a_1 \in \mathcal{A}_1$, $a_2 \in \mathcal{A}_2$ tal que $1 = a_1 + a_2$. Logo, $x = a_1x + a_2x$ é a soma de dois elementos de $\mathcal{A}_1\mathcal{A}_2$. Assim, $\mathcal{A}_1 \cap \mathcal{A}_2 \subset \mathcal{A}_1\mathcal{A}_2$. Portanto, $\mathcal{A}_1\mathcal{A}_2 = \mathcal{A}_1 \cap \mathcal{A}_2$. ∎

Lema 2.1.5 *Sejam A um anel e $\{\mathcal{A}_1, \cdots, \mathcal{A}_n\}$ um conjunto finito de ideais de A, tais que $\mathcal{A}_i + \mathcal{A}_j = A$ para $i \neq j$. Então $A/\prod_{i=1}^{n} \mathcal{A}_i \simeq \prod_{i=1}^{n} A/\mathcal{A}_i$.*

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

$$\varphi : A \longrightarrow A/\mathcal{A}_1 \times A/\mathcal{A}_2,$$

definida por $\varphi(a) = (a + \mathcal{A}_1, a + \mathcal{A}_2)$, com $a \in A$. Assim $\ker(\varphi) = \mathcal{A}_1 \cap \mathcal{A}_2$, uma vez que, $\varphi(x) = (\bar{0}, \bar{\bar{0}})$ se, e somente se, $(x + \mathcal{A}_1, x + \mathcal{A}_2) = (\bar{0}, \bar{\bar{0}})$ se, e somente se, $x + \mathcal{A}_1 = \bar{0}$ e $x + \mathcal{A}_2 = \bar{\bar{0}}$ se, e somente se $x \in \mathcal{A}_1$ e $x \in \mathcal{A}_2$. Então $x \in \mathcal{A}_1 \cap \mathcal{A}_2$. Para a sobrejetora, devemos encontrar $x, y, z \in A$ tal que $(y + \mathcal{A}_1, z + \mathcal{A}_2) = (x + \mathcal{A}_1, x + \mathcal{A}_2) = \varphi(x)$. Como $\mathcal{A}_1 + \mathcal{A}_2 = A$, existem elementos $a_1 \in \mathcal{A}_1$, $a_2 \in \mathcal{A}_2$ tais que $1 = a_1 + a_2$. Seja, $x = a_1z + a_2y$. Como $a_2 \equiv 1 (modulo\ \mathcal{A}_1)$ e $a_1 \equiv 1 (modulo\ \mathcal{A}_2)$ temos que $x \equiv y (modulo\ \mathcal{A}_1)$ e $x \equiv z (modulo\ \mathcal{A}_2)$ o que implica, $x + \mathcal{A}_1 = y + \mathcal{A}_1$ e $x + \mathcal{A}_2 = z + \mathcal{A}_2$, ou seja φ é sobrejetora. Portanto, pelo Teorema do Homomorfismo temos $A/\mathcal{A}_1 \cap \mathcal{A}_2 \simeq A/\mathcal{A}_1 \times A/\mathcal{A}_2$, e pelo Lema 2.1.4, temos que

$$A/\mathcal{A}_1\mathcal{A}_2 \simeq A/\mathcal{A}_1 \times A/\mathcal{A}_2.$$

Agora, supomos que o resultado é verdadeiro para $\forall k < n$. Fazendo $\mathcal{B} = \mathcal{A}_2 \cdots \mathcal{A}_n$, temos que $\mathcal{A}_1 + \mathcal{B} = A$. Como $\mathcal{A}_1 + \mathcal{A}_i = A$, para $i \geq 2$ temos que existem elementos $c_i \in \mathcal{A}_1$ e $a_i \in \mathcal{A}_i$ tais que $c_i + a_i = 1$. Assim, $1 = \prod_{i=2}^{n} c_i + a_i = c + a_2 + \cdots + a_n$, onde c é a soma dos termos que contém no mínimo um c_i como fator. Logo, $c \in \mathcal{A}_1$. Como $\mathcal{A}_2 \cdots \mathcal{A}_n \in \mathcal{B}$, segue que $\mathcal{A}_1 + \mathcal{B} = A$. Pelo caso $n = 2$, segue que $A/\mathcal{A}_1\mathcal{B} \simeq A/\mathcal{A}_1 \times A/\mathcal{B}$, e por hipótese de indução temos que $A/\prod_{i=1}^{n} \mathcal{A}_i \simeq \prod_{i=1}^{n} A/\mathcal{A}_i$. ∎

Proposição 2.1.2 *Com as notações anteriores, temos que* $\mathcal{O}_{\mathbb{L}}/\mathcal{P}\mathcal{O}_{\mathbb{L}} \simeq \prod_{i=1}^{g} \mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i^{e_i}$.

Demonstração: Temos que $\mathcal{Q}_i$ é o único ideal maximal de $\mathcal{O}_{\mathbb{L}}$ que contém $\mathcal{Q}_i^{e_i}$, pois se existir $\mathcal{M}$ um ideal maximal, tal que $\mathcal{M} \supset \mathcal{Q}_i^{e_i}$, temos pelo Lema 1.5.2 que $\mathcal{M} \supset \mathcal{Q}_i$, para algum i. Como $\mathcal{Q}_i$ é maximal segue que $\mathcal{M} = \mathcal{Q}_i$. Vamos mostrar que $\mathcal{Q}_i^{e_i} + \mathcal{Q}_j^{e_j} = \mathcal{O}_{\mathbb{L}}$, para $i \neq j$. Se $\mathcal{Q}_i^{e_i} + \mathcal{Q}_j^{e_j} \subsetneq \mathcal{O}_{\mathbb{L}}$, então existe um ideal maximal $\mathcal{M}$ de $\mathcal{O}_{\mathbb{L}}$, tal que $\mathcal{Q}_i^{e_i} + \mathcal{Q}_j^{e_j} \subset \mathcal{M} \subset \mathcal{O}_{\mathbb{L}}$. Como $\mathcal{Q}_i^{e_i} \subset \mathcal{Q}_i^{e_i} + \mathcal{Q}_j^{e_j}$, segue que $\mathcal{Q}_i^{e_i} \subset \mathcal{M}$, ou seja, $\mathcal{Q}_i \subset \mathcal{M}$, e como $\mathcal{Q}_i$ é maximal, temos que $\mathcal{Q}_i = \mathcal{M}$. De modo análogo, como $\mathcal{Q}_j^{e_j} \subset \mathcal{Q}_i^{e_i} + \mathcal{Q}_j^{e_j}$, segue que $\mathcal{Q}_j^{e_j} \subset \mathcal{M}$, ou seja, $\mathcal{Q}_j \subset \mathcal{M}$ e como $\mathcal{Q}_j$ é maximal, segue que $\mathcal{Q}_j = \mathcal{M}$. Assim, $\mathcal{Q}_i = \mathcal{Q}_j$, o que é um absurdo. Portanto, $\mathcal{Q}_i^{e_i} + \mathcal{Q}_j^{e_j} = \mathcal{O}_{\mathbb{L}}$. Então pelo Lema 2.1.5, segue que $\mathcal{O}_{\mathbb{L}}/\mathcal{P}\mathcal{O}_{\mathbb{L}} \simeq \prod_{i=1}^{g} \mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i^{e_i}$. ∎

Teorema 2.1.2 *Sejam* $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{L}_1$ *corpos de números, com respectivos anéis de inteiros* $\mathcal{O}_{\mathbb{K}} \subseteq \mathcal{O}_{\mathbb{L}} \subseteq \mathcal{O}_{\mathbb{L}_1}$. *Seja* $\mathcal{I}$ *um ideal primo de* $\mathcal{O}_{\mathbb{L}_1}$, $\mathcal{Q} = \mathcal{I} \cap \mathcal{O}_{\mathbb{L}}$ *e* $\mathcal{P} = \mathcal{Q} \cap \mathcal{O}_{\mathbb{K}}$. *Então*

$$e(\mathcal{I}|\mathcal{Q})e(\mathcal{Q}|\mathcal{P}) = e(\mathcal{I}|\mathcal{P}) \ \ e \ \ f(\mathcal{I}|\mathcal{Q})f(\mathcal{Q}|\mathcal{P}) = f(\mathcal{I}|\mathcal{P}).$$

Demonstração: Considere $f(\mathcal{I}|\mathcal{Q}) = [\mathcal{O}_{\mathbb{L}_1}/\mathcal{I} : \mathcal{O}_{\mathbb{L}}/\mathcal{Q}]$, $f(\mathcal{Q}|\mathcal{P}) = [\mathcal{O}_{\mathbb{L}}/\mathcal{Q} : \mathcal{O}_{\mathbb{K}}/\mathcal{P}]$ e $f(\mathcal{I}|\mathcal{P}) = [\mathcal{O}_{\mathbb{L}_1}/\mathcal{I} : \mathcal{O}_{\mathbb{K}}/\mathcal{P}]$. Assim, pelo Teorema da Multiplicidade de Graus, temos que

$$f(\mathcal{I}|\mathcal{Q})f(\mathcal{Q}|\mathcal{P}) = [\mathcal{O}_{\mathbb{L}_1}/\mathcal{I} : \mathcal{O}_{\mathbb{L}}/\mathcal{Q}][\mathcal{O}_{\mathbb{L}}/\mathcal{Q} : \mathcal{O}_{\mathbb{K}}/\mathcal{P}] = [\mathcal{O}_{\mathbb{L}_1}/\mathcal{I} : \mathcal{O}_{\mathbb{K}}/\mathcal{P}] = f(\mathcal{I}|\mathcal{P}).$$

Para mostrar a outra igualdade, considere $e = e(\mathcal{Q}|\mathcal{P})$, $e' = e(\mathcal{I}|\mathcal{Q})$ e $e'' = e(\mathcal{I}|\mathcal{P})$. Seja $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \mathcal{Q}^e \cdot \mathcal{J}$, onde $\mathcal{Q}, \mathcal{J}$ são ideais primos de $\mathcal{O}_{\mathbb{L}}$. Como $\mathcal{Q}^e$ divide $\mathcal{P}\mathcal{O}_{\mathbb{L}}$ e $\mathcal{Q}^{e+1}$ não divide $\mathcal{P}\mathcal{O}_{\mathbb{L}}$, segue que $\mathcal{Q}$ não divide $\mathcal{J}$. Analogamente, $\mathcal{O}_{\mathbb{L}_1}\mathcal{Q} = \mathcal{I}^{e'} \cdot \mathcal{J}'$, onde $\mathcal{I}$ não divide $\mathcal{J}'$. Assim,

$$\mathcal{O}_{\mathbb{L}_1}\mathcal{P} = \mathcal{O}_{\mathbb{L}_1}(\mathcal{P}\mathcal{O}_{\mathbb{L}}) = \mathcal{O}_{\mathbb{L}_1}(\mathcal{Q}^e\mathcal{J}) = (\mathcal{O}_{\mathbb{L}_1}\mathcal{Q})^e(\mathcal{O}_{\mathbb{L}_1}\mathcal{J}) = \mathcal{I}^{e'e}\mathcal{J}'^e(\mathcal{O}_{\mathbb{L}_1}\mathcal{J})$$

e $\mathcal{I}$ não divide $\mathcal{O}_{\mathbb{L}_1}\mathcal{J}$, pois caso contrário, $\mathcal{Q} = \mathcal{I} \cap \mathcal{O}_{\mathbb{L}} \supseteq \mathcal{O}_{\mathbb{L}_1}\mathcal{J} \supseteq \mathcal{J}$, contrariando que $\mathcal{Q}$ não divide $\mathcal{J}$. Assim, $e'e$ é a maior potência exata de $\mathcal{I}$, que divide $\mathcal{O}_{\mathbb{L}_1}\mathcal{P}$. Portanto, $e'' = e'e$. ∎

Lema 2.1.6 *Seja* A *um domínio de Dedekind. Sejam* $\mathcal{P}_1, \cdots, \mathcal{P}_r$, *ideais primos distintos e não nulos de* A, *e sejam* $x_1, \cdots, x_r \in A$ *e* $e_1, \cdots, e_r$ *inteiros positivos. Então existe um elemento* $x \in A$ *tal que* $x - x_i \in \mathcal{P}_i^{e_i}$ *e* $x - x_i \notin \mathcal{P}_i^{e_i+1}$, *para* $i = 1, \cdots, r$.

Demonstração: Para $i = 1, \cdots, r$ temos que $\mathcal{P}_i^{e_i} \supsetneq \mathcal{P}_i^{e_i+1}$. Então existe um elemento $a_i \in \mathcal{P}_i^{e_i}$, $a_i \notin \mathcal{P}_i^{e_i+1}$. Pela Proposição 2.1.2, existe $x \in A$ tal que $x - (x_i + a_i) \in \mathcal{P}_i^{e_i+1}$, para $i = 1, \cdots, r$. Então $x - x_i = [x - (x_i + a_i)] + a_i \in \mathcal{P}_i^{e_i}$, mas $x - x_i \notin \mathcal{P}_i^{e_i+1}$, pois $a_i \notin \mathcal{P}_i^{e_i+1}$. ∎

Lema 2.1.7 *Sejam A um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{K} \subseteq \mathbb{L}$ uma extensão de Galois finita de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros de A em $\mathbb{L}$. Se $\mathcal{Q}_1$ e $\mathcal{Q}_2$ são ideais primos de $\mathcal{O}_{\mathbb{L}}$ tais que $\mathcal{Q}_1 \cap A = \mathcal{Q}_2 \cap A \neq 0$, então existe um $\mathbb{K}$-automorfismo σ de $\mathbb{L}$ tal que $\sigma(\mathcal{Q}_1) = \mathcal{Q}_2$.*

Demonstração: Seja $G = \{\sigma_1, \cdots, \sigma_n\}$ o grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$. Se $\sigma_i(\mathcal{Q}_1) \neq \mathcal{Q}_2$, para todo $i = 1, \cdots, n$, pelo Lema 2.1.6, existe $x \in \mathcal{O}_{\mathbb{L}}$ tal que $x \notin \sigma_i(\mathcal{Q}_1)$, para $i = 1, \cdots, n$, e $x \in \mathcal{Q}_2$. Seja $a = \prod_{i=1}^{n} \sigma_i(x)$. Assim, $a \in \mathcal{Q}_2 \cap A$, e $a \notin \mathcal{Q}_1$, pois $\sigma_i(x) \notin \mathcal{Q}_1$, para $i = 1, \cdots, n$, o que é uma contradição. Portanto, existe $\sigma \in G$ tal que $\sigma(\mathcal{Q}_1) = \mathcal{Q}_2$. ∎

Teorema 2.1.3 *Sejam A um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{K} \subseteq \mathbb{L}$ uma extensão de Galois finita de grau n, e $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros de A em $\mathbb{L}$ e $\mathcal{P}$ um ideal primo de A. Se $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} \mathcal{Q}_i^{e_i}$ e $[\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i : A/\mathcal{P}] = f_i$ então $e_1 = e_2 = \cdots = e_g$, $f_1 = f_2 = \cdots = f_g$ e os corpos $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i$, $i = 1, \cdots, g$, são isomorfos.*

Demonstração: Pelo Lema 2.1.7, para cada $i = 1, \cdots, g$, existe $\sigma \in G$ tal que $\sigma(\mathcal{Q}_1) = \mathcal{Q}_i$. Assim, $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \sigma(\mathcal{P}\mathcal{O}_{\mathbb{L}}) = \prod_{i=1}^{g} \sigma(\mathcal{Q}_i)^{e_i}$. Pela unicidade da fatoração de $\mathcal{P}\mathcal{O}_{\mathbb{L}}$ segue $e_i = e$ para cada $i = 1, \cdots, g$. Finalmente, como $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i = \mathcal{O}_{\mathbb{L}}/\sigma(\mathcal{Q}_1) \simeq \mathcal{O}_{\mathbb{L}}/\mathcal{Q}_1$ segue que $f_1 = f_i$ para $i = 1, \cdots, g$. ∎

Corolário 2.1.1 *Com as hipóteses do Teorema 2.1.3, temos que $efg = n$, onde n é o grau da extensão $\mathbb{L}$ sobre $\mathbb{K}$.*

Demonstração: Pelo Teorema 2.1.1, temos que $\sum_{i=1}^{g} e_i f_i = n$. Pelo Teorema 2.1.3, temos que $e_i = e$ e $f_i = f$, para todo $i = 1, \cdots, g$. Portanto, $efg = n$. ∎

Proposição 2.1.3 *Se A é um domínio de Dedekind que possui somente um número finito de ideais primos então A é principal.*

Demonstração: Pelo Teorema 1.6.2, todo ideal não nulo de A é um produto finito de ideais primos não nulos de A. Assim, é suficente mostrar que estes ideais primos são principais. Sejam $\mathcal{P}_1, \cdots, \mathcal{P}_r$ os ideais primos não nulos de A. Pela Lema 2.1.6, para $h = 1, \cdots, r$, existe $y_h \in A$ tal que $y_h \in \mathcal{P}_h$, $y_h \notin \mathcal{P}_h^2$ e $y_h \notin \mathcal{P}_j$, para $j \neq h$, onde consideramos $x_1 = \cdots = x_r = 0$, $e_h = 1$, e $e_j = 0$, para $j \neq h$. Assim, $\mathcal{P}_h$ divide Ay_h, $\mathcal{P}_h^2$ não divide Ay_h e $\mathcal{P}_j$ não divide Ay_h, para $j \neq h$. Então a decomposição de Ay_h em ideais primos é $Ay_h = \mathcal{P}_h$. Portanto, cada ideal $\mathcal{P}_h$ é principal. ∎

2.2 Ramificação em corpos quadráticos

Nesta seção, apresentamos especificamente a ramificação nos corpos quadráticos. Deste modo, sejam $d \in \mathbb{Z}$ livre de quadrados, $\mathbb{L} = \mathbb{Q}(\sqrt{d})$, $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros de $\mathbb{L}$ e p um número primo. Seja $p\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} \mathcal{Q}_i^{e_i}$ a decomposição em $\mathbb{L}$ do ideal $p\mathcal{O}_{\mathbb{L}}$ como um produto de ideais primos de $\mathcal{O}_{\mathbb{L}}$. Pelo Teorema 2.1.1, segue que $\sum_{i=1}^{g} e_i f_i = 2$. Assim, $g \leq 2$ e temos os seguintes casos:

a) Se $g = 2$, $e_1 = e_2 = 1$, $f_1 = f_2 = 1$, então p se decompõe em $\mathbb{L}$, ou seja, $p\mathcal{O}_{\mathbb{L}} = \mathcal{Q}_1\mathcal{Q}_2$, onde $\mathcal{Q}_1, \mathcal{Q}_2$ são ideais primos de $\mathcal{O}_{\mathbb{L}}$ acima de $p\mathbb{Z}$.

b) Se $g = 1$, $e_1 = 1$, $f_1 = 2$, então p é inerte em $\mathbb{L}$, ou seja, $p\mathcal{O}_{\mathbb{L}} = \mathcal{Q}$, onde $\mathcal{Q}$ é um ideal primo de $\mathcal{O}_{\mathbb{L}}$ acima de $p\mathbb{Z}$.

c) Se $g = 1$, $e_1 = 2$, $f_1 = 1$, então p ramifica em $\mathbb{L}$, ou seja, $p\mathcal{O}_{\mathbb{L}} = \mathcal{Q}^2$, onde $\mathcal{Q}$ é um ideal primo de $\mathcal{O}_{\mathbb{L}}$ acima de $p\mathbb{Z}$.

Definição 2.2.1 *Dados um número primo ímpar p e um inteiro d relativamente primo com p, dizemos que d é um resíduo quadrático módulo p, se existir $a \in \mathbb{Z}$ tal que $d \equiv a^2 (modulo\ p)$, isto é, se a classe de restos de d módulo p for um quadrado em $\mathbb{Z}_p$, caso contrário, d não é resíduo quadrático módulo p.*

Exemplo 2.2.1 *Se $p = 5$ então $d = 19$ é um resíduo quadrático módulo 5, pois existe $a = 2$ tal que $19 \equiv 2^2 (modulo\ 5)$. Se $p = 7$ então $d = 19$ não é resíduo quadrático módulo 7, pois não existe a tal que $19 \equiv a^2 (modulo\ 7)$.*

Teorema 2.2.1 *Seja $\mathbb{L} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, onde d é um inteiro livre de quadrados.*
i) Os primos ímpares p, onde d é um resíduo quadrático módulo p, decompõem em $\mathbb{L}$.
ii) Os primos ímpares p, onde d não é um resíduo quadrático módulo p, são inertes em $\mathbb{L}$.
iii) Os primos ímpares divisores de d ramificam em $\mathbb{L}$.

Demonstração: Se p é ímpar, temos que $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\sqrt{d}]$ ou $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Agora, se

$$\alpha = a + b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right],$$

com b ímpar, então

$$\alpha \equiv a + (b+p)\left(\frac{1+\sqrt{d}}{2}\right) (modulo p).$$

Assim, $\alpha' = a + (b+p)\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}[\sqrt{d}]$, e $\alpha \equiv \alpha'(modulo p)]$, e portanto $\mathcal{O}_{\mathbb{L}}/p\mathcal{O}_{\mathbb{L}}$ é isomorfo a $\mathbb{Z}[\sqrt{d}]/p\mathcal{O}_{\mathbb{L}}$. Por outro lado, temos que $\mathbb{Z}[x]/\langle x^2 - d\rangle$ é isomorfo a $\mathbb{Z}[\sqrt{d}]$, e portanto,

$$\mathcal{O}_{\mathbb{L}}/p\mathcal{O}_{\mathbb{L}} \simeq \mathbb{Z}[x]/\langle p, x^2 - \bar{d}\rangle \simeq \mathbb{Z}_p[x]/\langle x^2 - \bar{d}\rangle,$$

onde $\bar{d}$ é a classe de resíduo de d módulo p.

i) Se $d \equiv x^2(modulo\ p)$, então $x^2 - \bar{d}$ em $\mathbb{Z}_p[x]$, fatora-se como $x^2 - \bar{d} = (x - \sqrt{d})(x + \sqrt{d})$, onde $h_1(x) = x - \sqrt{d}$ e $h_2(x) = x + \sqrt{d}$ são polinômios irredutíveis distintos tais que $\langle h_1 h_2\rangle = \langle h_1\rangle \cap \langle h_2\rangle$ e $\langle h_1 + h_2\rangle = \mathbb{Z}_p[x]$. Assim,

$$\mathcal{O}_{\mathbb{L}}/p\mathcal{O}_{\mathbb{L}} = \mathbb{Z}_p[x]/\langle x^2 - d\rangle \simeq \mathbb{Z}_p[x]/\langle x - \sqrt{d}\rangle \times \mathbb{Z}_p[x]/\langle x + \sqrt{d}\rangle$$

e como $\mathbb{Z}_p[x]/\langle x - \sqrt{d}\rangle$ e $\mathbb{Z}_p[x]/\langle x + \sqrt{d}\rangle$ são corpos, segue que $p\mathcal{O}_{\mathbb{L}} = \mathcal{Q}_1\mathcal{Q}_2$, com $\mathcal{Q}_1$ e $\mathcal{Q}_2$ primos, ou seja, p se decompõe.

ii) Se $d \not\equiv x^2(modulo\ p)$, então $x^2 - \bar{d}$ é irredutível em $\mathbb{Z}_p[x]$, e $\mathcal{O}_{\mathbb{L}}/p\mathcal{O}_{\mathbb{L}}$ é isomorfo a um corpo. Assim, $p\mathcal{O}_{\mathbb{L}}$ permanece primo, ou seja, p é inerte em $\mathbb{L}$.

iii) Se p é um divisor de d temos que $x^2 - \bar{d}$ é um quadrado de um polinômio irredutível. Assim, $\mathcal{O}_{\mathbb{L}}/p\mathcal{O}_{\mathbb{L}} \simeq \mathbb{Z}_p[x]/\langle h^2\rangle$ e o elemento $h + \langle h^2\rangle$ é não nulo e nilpotente. Então p se ramifica. ■

Exemplo 2.2.2 *Seja $\mathbb{L} = \mathbb{Q}(\sqrt{10})$. Como 5 divide 10, temos pelo Teorema 2.2.1, que 5 ramifica em $\mathbb{L}$. Assim, $e = 2$ e $f = 1$. Agora, se p=3 então 10 é resíduo quadrático módulo 3, logo 3 decompõe. Assim, $e = 1$ e $f = 1$. Se p=7, temos que 10 não é resíduo quadrático módulo 7, então 7 é inerte.*

Teorema 2.2.2 *Seja $\mathbb{L} = \mathbb{Q}(\sqrt{d})$, um corpo quadrático, onde d é um inteiro livre de quadrados. Então:*

i) Se $d \equiv 1(modulo\ 8)$ então 2 se decompõe em $\mathbb{L}$.

ii) Se $d \equiv 5(modulo\ 8)$ então 2 é inerte em $\mathbb{L}$.

iii) Se $d \equiv 2(modulo\ 4)$ ou $d \equiv 3(modulo\ 4)$ então 2 ramifica em $\mathbb{L}$.

Demonstração: Se $d \equiv 1(modulo\ 4)$ então $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right]$ e o polinômio minimal de $\dfrac{1+\sqrt{d}}{2}$ é $x^2 - x - \dfrac{d-1}{4}$. Assim, $\mathcal{O}_{\mathbb{L}}$ é isomorfo a $\mathbb{Z}[x]/\langle x^2 - x - a\rangle$, onde $a = \dfrac{d-1}{4}$, e portanto,

$$\mathbb{Z}/2\mathcal{O}_{\mathbb{L}} \simeq \mathbb{Z}_2[x]/\langle x^2 - x - \bar{a}\rangle.$$

Logo, para $i)$ temos que se $d \equiv 1(modulo\ 8)$, então $2k = \dfrac{d-1}{4}, k \in \mathbb{Z}$. Assim, $a \equiv 0(modulo\ 2)$ e $x^2 - x - \bar{a} \equiv x^2 + x \equiv x(x+1)(modulo\ 2)$. Portanto, $\mathcal{O}_{\mathbb{L}}/2\mathcal{O}_{\mathbb{L}}$ é o produto de dois corpos,

ou seja, 2 decompõe em $\mathbb{L}$. Para $ii)$ se $d \equiv 5(modulo\ 8)$, então $2k = \dfrac{d-1-4}{4}, k \in \mathbb{Z}$. Assim, $a \equiv 1(modulo\ 2)$ e $x^2 - x - \bar{a} \equiv x^2 + x + \bar{1}(modulo\ 2)$. Como $x^2 + x + \bar{1}$ é irredutível, segue que 2 permanece primo em $\mathbb{L}$. Agora, para $iii)$ se $d \equiv 2$ ou $d \equiv 3(modulo\ 4)$, então $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\sqrt{d}]$ e $\mathcal{O}_{\mathbb{L}}/2\mathcal{O}_{\mathbb{L}}$ é isomorfo e $\mathbb{Z}_p[x]/\langle x^2 - \bar{d}\rangle$. Neste caso, $x^2 - \bar{d} = x^2$ ou $x^2 - \bar{1} = (x^2-1)^2$, e ambos os casos é um quadrado. Assim, $\mathbb{Z}_p[x]/\langle x^2 - \bar{d}\rangle$ possui um elemento nilpotente não nulo. Então 2 ramifica em $\mathbb{L}$. ∎

Exemplo 2.2.3 *Se $\mathbb{L} = \mathbb{Q}(\sqrt{17})$, segue pelo Teorema 2.2.2 que 2 se decompõe em $\mathbb{L}$. Se $\mathbb{L} = \mathbb{Q}(\sqrt{21})$, então 2 é inerte em $\mathbb{L}$ e se $\mathbb{L} = \mathbb{Q}(\sqrt{6})$ então 2 ramifica em $\mathbb{L}$.*

2.3 Discriminante

Nesta seção, apresentamos o conceito de discriminante e enfocamos suas principais propriedades.

Definição 2.3.1 *Sejam $A \subseteq B$ anéis tal que B é um A-módulo livre de posto n. Seja $\{\alpha_1, \cdots, \alpha_n\} \subset B$. Definimos o discriminante do conjunto $\{\alpha_1, \cdots, \alpha_n\}$ por*

$$D(\alpha_1, \cdots, \alpha_n) = det(Tr_{B|A}(\alpha_i\alpha_j)).$$

Exemplo 2.3.1 *Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{11})$ um corpo de números e $\{1, \sqrt{11}\} \subset \mathbb{K}$. Assim,*

$$D(1, \sqrt{11}) = \begin{vmatrix} Tr_{\mathbb{K}|\mathbb{Q}}(1) & Tr_{\mathbb{K}|\mathbb{Q}}(\sqrt{11}) \\ Tr_{\mathbb{K}|\mathbb{Q}}(\sqrt{11}) & Tr_{\mathbb{K}|\mathbb{Q}}(\sqrt{11})^2 \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 22 \end{vmatrix} = 44.$$

Proposição 2.3.1 *Sejam $A \subseteq B$ anéis tal que B é um A-módulo livre de posto n. Se $\{y_1, \cdots, y_n\}$ é um conjunto de elementos de B, tais que $y_i = \sum_{j=1}^{n} a_{ij}\alpha_j$ com $a_{ij} \in A$, para $i = 1, \cdots, n$, então $D(y_1, \cdots, y_n) = (det(a_{ij}))^2 D(\alpha_1, \cdots, \alpha_n)$.*

Demonstração: Sejam $y_p = \sum_{i=1}^{n} a_{pi}\alpha_i$ e $y_q = \sum_{j=1}^{n} a_{qj}\alpha_j$. Assim, $y_p y_q = \sum_{j,i=1}^{n} a_{pi}a_{qj}\alpha_i\alpha_j$. Logo, $D(y_1, \cdots, y_n) = det(Tr_{B|A}(y_p y_q))$. Mas $Tr_{B|A}(y_p y_q) = \sum_{i=1}^{n} a_{pi}a_{qj}Tr_{B|A}(\alpha_i\alpha_j)$. Na forma matricial, temos

$$(Tr_{B|A}(y_p y_q)) = (a_{pi})(Tr_{B|A}(\alpha_i\alpha_j))(a_{qj})^t.$$

Assim,

$$\begin{aligned} D(y_1, \cdots, y_n) &= det(Tr_{B|A}(y_p y_q)) = det((a_{pi})(Tr_{B|A}(\alpha_i\alpha_j))(a_{qj})) \\ &= det(a_{pi})det(Tr_{B|A}(\alpha_i\alpha_j))det(a_{qj}) = (det(a_{i,j}))^2 D(\alpha_1, \cdots, \alpha_n). \end{aligned}$$ ∎

Exemplo 2.3.2 *Pelo Exemplo* 2.3.1*, vimos que o* $D(1,\sqrt{11})$ *de* $\mathbb{Q}(\sqrt{11})$ *é igual a 44. Agora, considerando outra base de* $\mathbb{K}$*, por exemplo* $\{2-\sqrt{11}, 1+\sqrt{11}\}$ *segue pela Proposição* 2.3.1*, que*

$$D(2-\sqrt{11}, 1+\sqrt{11}) = \det\begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}^2 D(1,\sqrt{11}) = (3)^2 44.$$

Definição 2.3.2 *Sejam* $A \subseteq B$ *anéis tal que* B *é um* A*-módulo livre de posto finito* n*. Chamamos de discriminante de* B *sobre* A *o ideal de* A*, dado por* $\mathcal{D}_{B|A} = \langle D(\alpha_1, \cdots, \alpha_n)\rangle$*, onde* $\{\alpha_1, \cdots, \alpha_n\}$ *é uma base de* B *sobre* A*.*

Proposição 2.3.2 *Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$*, onde* $d \in \mathbb{Z}$ *é livre de quadrados. Se* $d \equiv 2(modulo\ 4)$ *ou* $d \equiv 3(modulo\ 4)$ *então o discriminante de* $\mathcal{O}_{\mathbb{K}}$*, onde* $\mathcal{O}_{\mathbb{K}}$ *é o anel dos inteiros de* $\mathbb{K}$ *sobre* $\mathbb{Z}$*, é* $4d$*.*

Demonstração: Pelo Teorema 1.3.1, se $d \equiv 2(modulo\ 4)$ ou $d \equiv 3(modulo\ 4)$ então $\{1, \sqrt{d}\}$ é uma base do anel dos inteiros de $\mathbb{K}$. Assim, pela Definição 2.3.1 temos que

$$D(1,\sqrt{d}) = \begin{vmatrix} Tr(1) & Tr(\sqrt{d}) \\ Tr(\sqrt{d}) & Tr(\sqrt{d})^2 \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 2d \end{vmatrix} = 4d.$$

Portanto, o discriminante da base $\{1, \sqrt{d}\}$ do anel dos inteiros de $\mathbb{K}$ é $4d$. ∎

Proposição 2.3.3 *Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$*, onde* $d \in \mathbb{Z}$ *é livre de quadrados. Se* $d \equiv 1(modulo\ 4)$ *então o discriminante de* $\mathcal{O}_{\mathbb{K}}$*, onde* $\mathcal{O}_{\mathbb{K}}$ *é o anel dos inteiros de* $\mathbb{K}$ *sobre* $\mathbb{Z}$*, é* d*.*

Demonstração: Pelo Teorema 1.3.1, se $d \equiv 1(modulo\ 4)$ então $\left\{1, \dfrac{1+\sqrt{d}}{2}\right\}$ é uma base do anel dos inteiros $\mathbb{K}$. Assim,

$$D\left(1, \frac{1+\sqrt{d}}{2}\right) = \begin{vmatrix} Tr(1) & Tr\left(\dfrac{1+\sqrt{d}}{2}\right) \\ Tr\left(\dfrac{1+\sqrt{d}}{2}\right) & Tr\left(\dfrac{1+\sqrt{d}}{2}\right)^2 \end{vmatrix} = \begin{vmatrix} 2 & 1 \\ 1 & \dfrac{1+d}{2} \end{vmatrix} = 1+d-1 = d.$$

Portanto, o discriminante da base $\left\{1, \dfrac{1+\sqrt{d}}{2}\right\}$ do anel dos inteiros de $\mathbb{K}$ é d. ∎

Exemplo 2.3.3 *Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ *um corpo de números. Como* $5 \equiv 1(modulo\ 4)$*, temos pelo Teorema 1.3.1, que* $\left\{1, \dfrac{1}{2} + \dfrac{\sqrt{5}}{2}\right\}$ *é uma base de* $\mathbb{K}$*. Assim, pela Proposição 2.3.3, temos que*

$$D\left(1, \frac{1+\sqrt{5}}{2}\right) = \begin{vmatrix} Tr(1) & Tr\left(\dfrac{1+\sqrt{5}}{2}\right) \\ Tr\left(\dfrac{1+\sqrt{5}}{2}\right) & Tr\left(\dfrac{1+\sqrt{5}}{2}\right)^2 \end{vmatrix} = \begin{vmatrix} 2 & 1 \\ 1 & \dfrac{1+5}{2} \end{vmatrix} = 1+5-1 = 5.$$

Proposição 2.3.4 *Sejam $A \subseteq B$ anéis tal que B é um A-módulo livre de posto finito n. Suponhamos que $\mathcal{D}_{B|A}$ contém um elemento que não é um divisor de zero. Então $\{\alpha_1, \cdots, \alpha_n\} \subset B$ é uma base de B sobre A se, e somente se, $D(\alpha_1, \cdots, \alpha_n)$ gera $\mathcal{D}_{B|A}$.*

Demonstração: Se $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de B sobre A, pela Proposição 2.3.1, temos que $D(\alpha_1, \cdots, \alpha_n)$ gera $\mathcal{D}_{B|A}$. Por outro lado, suponhamos que $d = D(\alpha_1, \cdots, \alpha_n)$ gera $\mathcal{D}_{B|A}$. Seja $\{e_1, \cdots, e_n\}$ uma base de B sobre A. Sejam $d' = D(e_1, \cdots, e_n)$ e $\alpha_i = \sum_{j=1}^{n} a_{ij}e_j$, com $a_{ij} \in A$, $1 \leq i, j \leq n$. Pela Proposição 2.3.1 segue que $d = \det(a_{ij})^2 d'$. Por hipótese, $Ad = Ad' = \mathcal{D}_{B|A}$, ou seja, $d' = bd$, $b \in A$. Logo,

$$d - \det(a_{ij})^2 db = (1 - \det(a_{ij})^2 b)d = 0.$$

Temos que d não é um divisor de zero, pois caso contrário, como d gera $\mathcal{D}_{B|A}$ teríamos que todo elemento de $\mathcal{D}_{B|A}$ seria um divisor de zero, o que não ocorre. Logo, $1 - det(a_{ij})^2 b = 0$ e assim, $b \det(a_{ij}) \det(a_{ij}) = 1$. Logo, $\det(a_{ij})$ é inversível e portanto $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de B sobre A. ∎

Lema 2.3.1 *(Lema de Dedekind) Sejam G um grupo, $\mathbb{K}$ um corpo, e $\sigma_1, \cdots, \sigma_n$ homomorfismos distintos de G no grupo multiplicativo $\mathbb{K}^*$. Então $\{\sigma_1, \cdots, \sigma_n\}$ são linearmente independentes sobre $\mathbb{K}$.*

Demonstração: Suponhamos que $\sigma_1, \cdots, \sigma_n$ são linearmente dependentes. Seja $\sum_{i=1}^{r} a_i\sigma_i = 0$, com $a_i \in \mathbb{K}$, tal que o número r dos $a_i's$ não nulos seja o menor possível. Como σ_1 e σ_2 são distintos, então existe $z \in G$ tal que $\sigma_1(z) \neq \sigma_2(z)$. Além disso, para todo $x \in G$, temos que

$$a_1\sigma_1(x) + a_2\sigma_2(x) + \cdots + a_r\sigma_r(x) = 0. \tag{2.1}$$

Como os $\sigma_i's$ são homomorfismos, tem-se que a expressão é válida para todo $x \in G$. Assim, para xz temos

$$a_1\sigma_1(x)\sigma_1(z) + a_2\sigma_2(x)\sigma_2(z) + \cdots + a_r\sigma_r(x)\sigma_r(z) = 0. \tag{2.2}$$

Multiplicando a Equação (2.1) por $\sigma_1(z)$ e subtraindo da Equação (2.2) obtemos,

$$a_2(\sigma_1(z) - \sigma_2(z))\sigma_2(x) + \cdots + a_r(\sigma_1(z) - \sigma_r(z))\sigma_r(x) = 0.$$

Com isso vale para todo $x \in G$ e r foi escolhido como o menor possível, segue que $a_2(\sigma_1(z) - \sigma_2(z)) = 0$, ou seja $\sigma_1(z) = \sigma_2(z)$, para todo $z \in G$, uma vez que $a_2 \neq 0$, o que contradiz a hipótese de que os homomorfismos são distintos. ∎

Proposição 2.3.5 *Sejam $\mathbb{K} \subseteq \mathbb{L}$ corpos e $\sigma_1, \cdots, \sigma_n$, $\mathbb{K}$-isomorfismo de $\mathbb{L}$. Se $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, então*

$$D(\alpha_1, \cdots, \alpha_n) = det(\sigma_i(\alpha_j))^2 \neq 0.$$

Demonstração: Temos que $D(\alpha_1, \cdots, \alpha_n) = \det(Tr(\alpha_i\alpha_j))$. Como o traço de $\alpha_i\alpha_j$ é a soma de seus conjugados, segue que

$$\begin{aligned} D(\alpha_1, \cdots, \alpha_n) &= \det(Tr(\alpha_i\alpha_j)) = \det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j)\right) \\ &= \det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)\right) = \det(\sigma_i(\alpha_j))^2, \end{aligned}$$

uma vez que

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

Falta mostrar que $\det(\sigma_i(\alpha_j)) \neq 0$. Se $\det(\sigma_i(\alpha_j)) = 0$, então existem $a_1, \cdots, a_n \in \mathbb{C}$, não todos nulos, tal que $\sum_{i=1}^{n} a_i\sigma_i(\alpha_j) = 0$, para $j = 1, \cdots, n$. Seja $\alpha \in \mathbb{L}$. Assim, $\alpha = \sum_{i=1}^{n} b_i\alpha_i$, onde $b_i \in \mathbb{K}$, $i = 1, \cdots, n$. Por linearidade, $\sum_{i=1}^{n} a_i\sigma_i(\alpha) = 0$, $\forall \alpha \in \mathbb{L}$. Assim, $\sum_{i=1}^{n} a_i\sigma_i = 0$, o que contradiz o Lema 2.3.1. Portanto, $\det(\sigma_i(\alpha_j))^2 \neq 0$. ∎

Exemplo 2.3.4 *Seja $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3})$. Assim, existem dois $\mathbb{Q}-$isomorfismos, σ_1, σ_2, onde $\sigma_1(a + b\sqrt{3}) = a + b\sqrt{3}$ e $\sigma_2(a + b\sqrt{3}) = a - b\sqrt{3}$. Como $\{1, \sqrt{3}\}$ é uma base de $\mathbb{Q}(\sqrt{3})$ sobre $\mathbb{Q}$ segue que*

$$D(1, \sqrt{3}) = \begin{vmatrix} 1 & 1 \\ \sqrt{3} & -\sqrt{3} \end{vmatrix}^2 = (-2\sqrt{3})^2 = 12.$$

Proposição 2.3.6 *Sejam $A \subseteq B$ anéis tal que B é um A-módulo livre de posto n e A um domínio. Se $\{x_1, \cdots, x_n\}$ e $\{x_1', \cdots, x_n'\}$ são bases do A-módulo B, então $D_{B|A}(x_1, \cdots, x_n) = D_{B|A}(x_1', \cdots, x_n') = 0$ ou $D_{B|A}(x_1, \cdots, x_n)$ e $D_{B|A}(x_1', \cdots, x_n')$ são elementos associados.*

Demonstração: Por hipótese, existem elementos $a_{ij} \in A$ tais que $x_j' = \sum_{i=1}^{n} a_{ij}x_i$, para todo $j = 1, \cdots, n$. Então pela Proposição 2.3.1, temos que

$$D_{B|A}(x_1', \cdots, x_n') = [\det(a_{ij})]^2 D_{B|A}(x_1, \cdots, x_n).$$

Como (a_{ij}) é uma matriz inversível, segue que $\det(a_{ij})$ é uma unidade do anel A. Assim ambos determinantes são iguais a ou ambos são elementos associados. ∎

Proposição 2.3.7 *Sejam $\mathbb{K}$ um corpo de números, $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros e $\{x_1 \cdots, x_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{Q}$ contida em $\mathcal{O}_{\mathbb{K}}$. Se $D(x_1, \cdots, x_n)$ for livre de quadrados, então $\{x_1 \cdots, x_n\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$.*

Demonstração: Se $\{e_1 \cdots, e_n\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$, então $x_i = \sum_{j=1}^{n} a_{ij}e_j$, com $a_{ij} \in \mathbb{Z}$. Assim, pela Proposição 2.3.1, $D(x_1 \cdots, x_n) = \det(a_{ij})^2 D(e_1 \cdots, e_n)$. Como $D(x_1 \cdots, x_n)$ é livre de quadrados segue que $\det(a_{ij}) = \pm 1$. Portanto, $\{x_1 \cdots, x_n\}$ é uma base do anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$.

∎

Exemplo 2.3.5 *Pelo Exemplo 2.3.3, temos que $D\left(1, \frac{1+\sqrt{5}}{2}\right) = 5$. Assim, pelo Proposição 2.3.7 temos que $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$.*

Definição 2.3.3 *Sejam $\mathbb{K}$ um corpo de números e $\mathcal{O}_{\mathbb{K}}$ o seu anel dos inteiros. Uma base do $\mathbb{Z}$-módulo livre $\mathcal{O}_{\mathbb{K}}$ de posto $[\mathbb{K} : \mathbb{Q}]$, é chamada de base integral e seu discriminante é chamado de discriminante absoluto.*

Definição 2.3.4 *O discriminante em $\mathbb{K}$ sobre $\mathbb{Q}$, de qualquer base integral é chamado discriminante do corpo $\mathbb{K}$, e é denotado por $\delta_{\mathbb{L}|\mathbb{Q}}$.*

Proposição 2.3.8 *Sejam $\mathbb{K}$ 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, $D(1, \alpha, \cdots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N(f'(\alpha))$, onde $f'(x)$ é a derivada de $f(x)$.*

Demonstração: Como $\mathbb{K} \subseteq \mathbb{K}[\alpha]$ é uma extensão finita de grau n, segue que $\{1, \alpha, \cdots, \alpha^{n-1}\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Assim, pela Proposição 2.3.5, segue que $D(1, \alpha, \cdots, \alpha^{n-1}) = \det(\sigma_i(\alpha^j))^2 \neq 0$, onde σ_i, $1 \leq i \leq n$, são $\mathbb{K}$-isomorfismos de $\mathbb{K}[\alpha]$. Observemos que $\det(\sigma_i(\alpha^j))$ é um determinante de Vandermonde. Logo, $\det(\sigma_i(\alpha^j)) = \prod_{1 \leq i < j \leq n} (\alpha^j - \alpha^i)$. Assim,

$$D(1, \alpha, \cdots, \alpha^{n-1}) = \prod_{1 \leq i < j \leq n} (\alpha^j - \alpha^i)^2,$$

onde $\alpha, \cdots, \alpha^n$ são conjugados de α. Temos que $f(x) = \prod_{i=1}^{n}(x - \alpha^i)$ é o polinômio minimal de α sobre $\mathbb{K}$ e $f'(x) = \sum_{i=1}^{n} \prod_{i=1, i\neq j}^{n} (x - \alpha^i)$. Logo,

$$f'(\alpha) = \prod_{i=1}^{n}(\alpha^j - \alpha^i).$$

Assim,

$$\prod_{j=1}^{n} f'(\alpha) = \prod_{j=1}^{n}\prod_{i=1}^{n}(\alpha^j - \alpha^i) = \prod_{i=1, i\neq j}^{n} (\alpha^j - \alpha^i). \tag{2.3}$$

Observemos que $N(f'(\alpha)) = \prod_{i=1}^{n} \sigma_i(f'(\alpha))$=$\prod_{i=1}^{n} f'(\alpha^j)$, onde os $f'(\alpha^j)$ são os conjugados de $f'(\alpha)$. Também como cada fator $\alpha^j - \alpha^i$, para $i < j$, aparece duas vezes, uma como $\alpha^j - \alpha^i$ e a outra $\alpha^i - \alpha^j$, segue que o produto desses fatores é $-(\alpha^j - \alpha^i)^2$. Assim,

$$\prod_{i=1, i\neq j}^{n} (\alpha^j - \alpha^i) = \prod_{i=1, i\neq j}^{n} -(\alpha^j - \alpha^i)^2 = (-1)^s \prod_{1\leq i<j\leq n}^{n} (\alpha^j - \alpha^i)^2,$$

onde s é o número de pares (i, j) com $1 \leq i < j \leq n$, e é dado por $s = \frac{1}{2}n(n-1)$. Pela Equação (2.3) obtemos que $N(f'(\alpha)) = D(1, \alpha, \cdots, \alpha^{n-1})(-1)^s$. Portanto,

$$D(1, \alpha, \cdots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N(f'(\alpha)).$$ ■

Exemplo 2.3.6 *Sejam $\mathbb{L} = \mathbb{Q}(\sqrt{2})$ e $f(x) = x^2 - 2$ o polinômio minimal de $\sqrt{2}$ sobre $\mathbb{Q}$. Então $D(1, \sqrt{2}) = (-1)^{\frac{1}{2}2} N(f'(\sqrt{2})) = 8$, onde $f'(\sqrt{2}) = 2\sqrt{2}$ e $N(2\sqrt{2}) = 8$.*

Definição 2.3.5 *Seja $\mathbb{K}$ um corpo. Seja $m(x) \in \mathbb{K}[x]$ um polinômio mônico de grau n, com raízes $\alpha_1, \cdots, \alpha_n$. O discriminante de m é definido por*

$$D(m) = \prod_{i<j}(\alpha_j - \alpha_i)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i\neq j}(\alpha_j - \alpha_i) = \prod_{i=1}^{n} \prod_{j=i+1}^{n} (\alpha_j - \alpha_i)^2,$$

onde α_i, α_j são raízes de m.

Exemplo 2.3.7 *Seja $m(x) = x^2 + ax + b \in \mathbb{Q}[x]$. As raízes de $m(x)$ são $\alpha_1 = \dfrac{-a + \sqrt{a^2 - 4b}}{2}$ e $\alpha_2 = \dfrac{-a - \sqrt{a^2 - 4b}}{2}$. Assim,*

$$D(x^2 + ax + b) = (\alpha_2 - \alpha_1)^2 = a^2 - 4b.$$

Seja $m(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$. Fazendo uma mudança de variável temos $m(x) = x^3 + b_1x + c_1$. Assim, temos que

$$D(x^3 + b_1x + c_1) = -4b_1^3 - 27c_1^2.$$

Proposição 2.3.9 *Sejam p um número primo ímpar e ξ uma raiz p-ésima primitiva da unidade. Então* $D(1, \xi, \cdots, \xi^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}$.

Demonstração: Pelo Teorema 1.4.2, temos que $\{1, \xi, \cdots, \xi^{p-2}\}$ é uma base inteira e temos que $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ é o polinômio ciclotômico. Pela Proposição 2.3.8, temos que $D(1, \xi, \cdots, \xi^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} N(f'(\xi))$. Como p é ímpar, temos que o primeiro fator se resume a $(-1)^{\frac{(p-1)}{2}}$. Se $f(t) = \dfrac{t^p - 1}{t - 1}$ temos que

$$f'(t) = \frac{(t-1)pt^{p-1} - (t^p - 1)}{(t-1)^2} \ \ e \ \ f'(\xi) = \frac{-p\xi^{p-1}}{1 - \xi}.$$

Assim, $N(f'(\xi)) = \dfrac{N(p)N(\xi)^{p-1}}{N(1-\xi)} = \dfrac{-p^{p-1}1^{p-1}}{p} = p^{p-2}$. Portanto, $D(1, \xi, \cdots, \xi^{p-2}) = \pm p^{p-2}$. ∎

Observação 2.3.1 *Quando $n = p^r$, onde r é um número inteiro maior que 1 e p é um número primo temos que* $\dfrac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = x^{(p-1)p^{r-1}} + x^{(p-2)p^{r-1}} + \cdots + x^{p^{r-1}} + 1$ *é o polinômio p^r-ésimo polinômio ciclotômico. Temos que o p^r-ésimo polinômio ciclotômico tem grau $(p-1)p^{r-1}$ e seu termo independente é igual a 1. Logo, pela definição de norma, obtemos que*

$$N_{\mathbb{Q}(\xi_{p^r})/\mathbb{Q}(\xi_{p^r}^t)} = (-1)^{(p-1)p^{r-1}}, \text{ onde } t = 0, \cdots, p^{r-1} \text{ e } mdc(t, p^r) = 1. \tag{2.4}$$

Proposição 2.3.10 *Sejam p um número primo ímpar e ξ uma raiz p^r-ésima primitiva da unidade. Então o discriminante de $\mathbb{Q}(\xi_{p^r})$ sobre $\mathbb{Q}$ é* $D(1, \xi_{p^r}, \cdots, \xi_{p^r}^{\varphi(p^r)-1}) = \pm p^{p^{r-1}(r(p-1)-1)}$.

Demonstração: Pela Proposição 2.3.8, temos que $D(1, \xi_{p^r}, \cdots, \xi_{p^r}^{\varphi(p^r)-1}) = \pm N_{\mathbb{Q}(\xi_{p^r})/\mathbb{Q}}(f'(\xi_{p^r}))$. Derivando ambos os lados de $f(x) = \dfrac{x^{p^r} - 1}{x^{p^{r-1}} - 1}$, temos que

$$f'(x) = \frac{p^r x^{p^r - 1}(x^{p^{r-1}} - 1) - (x^{p^r} - 1)p^{r-1}x^{p^{r-1}-1}}{(x^{p^{r-1}} - 1)^2}, \tag{2.5}$$

e substituindo x por ξ_{p^r} na Equação (2.5) temos que

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

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

$$N_{\mathbb{Q}(\xi_{p^r})/\mathbb{Q}}(f'(\xi_{p^r})) = \frac{N_{\mathbb{Q}(\xi_{p^r})/\mathbb{Q}}(-p^r)}{N_{\mathbb{Q}(\xi_{p^r})/\mathbb{Q}}(1 - \xi_p) N_{\mathbb{Q}(\xi_{p^r})/\mathbb{Q}}(\xi_{p^r})}.$$

Da Equação (2.4) temos que $N_{\mathbb{Q}(\xi_{p^r})/\mathbb{Q}}(\xi_{p^r}) = \pm 1$. Também $N_{\mathbb{Q}(\xi_{p^r})/\mathbb{Q}}(-p^r) = (-p^r)^{(p-1)p^{r-1}}$ e $N_{\mathbb{Q}(\xi_{p^r})/\mathbb{Q}}(1 - \xi_p) = N_{\mathcal{Q}(\xi_p)/\mathcal{Q}} N_{\mathcal{Q}(\xi_{p^r})/\mathcal{Q}(\xi_p)}(1 - \xi_p) = (N_{\mathcal{Q}(\xi_p)/\mathcal{Q}}(1 - \xi_p))^{p^{r-1}} = p^{p^{r-1}}$. Portanto, $D(1, \xi_{p^r}, \cdots, \xi_{p^r}^{\varphi(p^r)-1}) = \dfrac{\pm p^{r(p-1)p^{r-1}}}{p^{p^{r-1}}} = \pm p^{p^{r-1}(r(p-1)-1)}$. ∎

2.4 Ramificação e discriminante

Sejam 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 do inteiros de A em $\mathbb{L}$. Esta seção tem como objetivo relacionar os conceitos de ramificação e discriminante, onde provamos que os ideais primos de A ramificam se, e somente se, estes ideais contém o discriminante.

Lema 2.4.1 *Sejam A um anel e $\mathcal{O}_{\mathbb{L}1}, \cdots, \mathcal{O}_{\mathbb{L}g}$ anéis contendo A, tais que sejam A-módulos livres finitamente gerados, e seja $\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} \mathcal{O}_{\mathbb{L}i}$ como um produto de anéis. Então,*

$$\mathcal{D}_{\mathcal{O}_{\mathbb{L}}/A} = \prod_{i=1}^{q} \mathcal{D}_{\mathcal{O}_{\mathbb{L}i}/A}.$$

Demonstração: Faremos a prova por indução sobre g. Para o caso $g = 2$, considere $\{x_1, \cdots, x_n\}$ uma base de $\mathcal{O}_{\mathbb{L}1}$ sobre A e $\{y_1, \cdots, y_m\}$ uma base de $\mathcal{O}_{\mathbb{L}2}$ sobre A. Com a identificação natural de $\mathcal{O}_{\mathbb{L}1}$ com $\mathcal{O}_{\mathbb{L}1} \times \{0\}$ e $\mathcal{O}_{\mathbb{L}2}$ com $\{0\} \times \mathcal{O}_{\mathbb{L}2}$, podemos considerar $\{x_1, \cdots, x_n, y_1, \cdots, y_m\}$ uma base de $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{L}1} \times \mathcal{O}_{\mathbb{L}2}$. Como $x_i = (x_i, 0)$ e $y_i = (0, y_i)$ segue que $x_i y_i = 0$ e assim $Tr(x_i y_i) = 0$. Logo,

$$\begin{aligned} D(x_1, \cdots, x_n, y_1, \cdots, y_m) &= \det \begin{pmatrix} Tr(x_i x_j) & 0 \\ 0 & Tr(y_i y_j) \end{pmatrix} \\ &= \det(Tr(x_i x_j)) \det(Tr(y_i y_j)) = D(x_1, \cdots, x_n) D(y_1, \cdots, y_m). \end{aligned}$$

Portanto, $\mathcal{D}_{\mathcal{O}_{\mathbb{L}}/A} = \mathcal{D}_{\mathcal{O}_{\mathbb{L}_1}/A} \mathcal{D}_{\mathcal{O}_{\mathbb{L}_2}/A} = \prod_{i=1}^{2} \mathcal{D}_{\mathcal{O}_{\mathbb{L}i}/A}$. Por hipótese de indução, suponhamos verdadeiro, para $g-1$, ou seja, se $\mathcal{G} = \prod_{i=1}^{g-1} \mathcal{O}_{\mathbb{L}i}$, então $\mathcal{D}_{\mathcal{G}/A} = \prod_{i=1}^{g-1} \mathcal{D}_{\mathcal{O}_{\mathbb{L}i}/A}$. Logo, $\mathcal{O}_{\mathbb{L}} = \mathcal{G} \times \mathcal{O}_{\mathbb{L}g}$, onde $\mathcal{G}$ é identificado com $\mathcal{G} \times \{0\}$ e $\mathcal{O}_{\mathbb{L}g}$ é identificado com $\{0\} \times \mathcal{O}_{\mathbb{L}g}$. Usando o caso $g = 2$, temos que $\mathcal{D}_{\mathcal{O}_{\mathbb{L}}/A} = \mathcal{D}_{\mathcal{G}/A} \mathcal{D}_{\mathcal{O}_{\mathbb{L}g}/A} = \prod_{i=1}^{g-1} \mathcal{D}_{\mathcal{O}_{\mathbb{L}i}/A} \mathcal{D}_{\mathcal{O}_{\mathbb{L}g}/A} = \prod_{i=1}^{g} \mathcal{D}_{\mathcal{O}_{\mathbb{L}i}/A}$, por hipótese de indução. ∎

Observação 2.4.1 *Com as mesmas hipóteses do Lema 2.4.1, prova-se analogamente que se $x \in \mathcal{O}_{\mathbb{L}}$ então $m_{\mathcal{O}_{\mathbb{L}}|A}(x) = \prod_{i=1}^{g} m_{\mathcal{O}_{\mathbb{L}i}/A}(\pi_i(x))$, $N_{\mathcal{O}_{\mathbb{L}}|A}(x) = \prod_{i=1}^{g} N_{\mathcal{O}_{\mathbb{L}i}/A}(\pi_i(x))$ e $Tr_{\mathcal{O}_{\mathbb{L}}|A}(x) = \prod_{i=1}^{g} Tr_{\mathcal{O}_{\mathbb{L}i}/A}(\pi_i(x))$, onde $\pi_i(x)$ é definida como $\pi_i : \mathcal{O}_{\mathbb{L}}/\mathcal{P}\mathcal{O}_{\mathbb{L}} \longrightarrow \mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i^{e_i}$ a i-ésima projeção induzida do isomorfismo natural $\mathcal{O}_{\mathbb{L}}/\mathcal{P}\mathcal{O}_{\mathbb{L}} \simeq \prod_{i=1}^{g} \mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i^{e_i}$.*

Proposição 2.4.1 *Sejam $A \subseteq \mathcal{O}_{\mathbb{L}}$ anéis e $\mathcal{P}$ um ideal primo de A. Sejam $S = A - \mathcal{P}$, $A' = S^{-1}A$ e $\mathcal{O}'_{\mathbb{L}} = S^{-1}\mathcal{O}_{\mathbb{L}}$. Então para todo $x \in \mathcal{O}_{\mathbb{L}}$ temos que $m_{\mathcal{O}'_{\mathbb{L}}|A'}(x) = m_{\mathcal{O}_{\mathbb{L}}|A}(x)$, $Tr_{\mathcal{O}'_{\mathbb{L}}|A'}(x) = Tr_{\mathcal{O}_{\mathbb{L}}|A}(x)$ e $N_{\mathcal{O}'_{\mathbb{L}}|A'}(x) = N_{\mathcal{O}_{\mathbb{L}}|A}(x)$.*

Demonstração: Sejam $\theta_x : \mathcal{O}_{\mathbb{L}} \longrightarrow \mathcal{O}_{\mathbb{L}}$ e $\theta'_x : \mathcal{O}'_{\mathbb{L}} \longrightarrow \mathcal{O}'_{\mathbb{L}}$ os homomorfismos definidos por $\theta_x(y) = xy$, onde $x, y \in \mathcal{O}_{\mathbb{L}}$ e $\theta'_x(y) = xy$, onde $x, y \in \mathcal{O}'_{\mathbb{L}}$. Sejam $M(\theta_x)$ e $M(\theta'_x)$ as matrizes correpondentes com relação a base $\{z_1, \cdots, z_n\}$. Assim, temos que as matrizes coincidem. Portanto, os polinômios característicos, os traços e as normas do elemento x em $\mathcal{O}_{\mathbb{L}}|A$ e em $\mathcal{O}'_{\mathbb{L}}|A'$ coincidem. ∎

Lema 2.4.2 *Sejam $A \subseteq \mathcal{O}_{\mathbb{L}}$ anéis e $\mathcal{A}$ um ideal de A. Se $\mathcal{O}_{\mathbb{L}}$ é um A-módulo livre com base $\{x_1, \cdots, x_n\}$, então $\{\overline{x}_1, \cdots, \overline{x}_n\}$ é uma base de $\mathcal{O}_{\mathbb{L}}/\mathcal{A}\mathcal{O}_{\mathbb{L}}$ sobre $A/\mathcal{A}$ e*

$$D(\overline{x}_1, \cdots, \overline{x}_n) = \overline{D(x_1, \cdots, x_n)}.$$

Demonstração: Pela demonstração do Teorema 2.1.1 segue que $\{\bar{x}_1, \cdots, \bar{x}_n\}$ é uma base de $\mathcal{O}_{\mathbb{L}}/\mathcal{A}\mathcal{O}_{\mathbb{L}}$ sobre $A/\mathcal{A}$. Agora, para $x \in \mathcal{O}_{\mathbb{L}}$ seja $\theta_x : \mathcal{O}_{\mathbb{L}} \longrightarrow \mathcal{O}_{\mathbb{L}}$ o endomorfismo definido por $\theta_x(a) = ax$, $a \in \mathcal{O}_{\mathbb{L}}$, com $M = (a_{ij})$, onde $a_{ij} \in A$, a sua matriz. Considere o endomorfismo $\theta_{\bar{x}} : \mathcal{O}_{\mathbb{L}}/\mathcal{A}\mathcal{O}_{\mathbb{L}} \longrightarrow \mathcal{O}_{\mathbb{L}}/\mathcal{A}\mathcal{O}_{\mathbb{L}}$ definido por $\theta_{\bar{x}}(\bar{a}) = \bar{a}\bar{x}$. Temos que a matriz de $\theta_{\bar{x}}$ é $M = \overline{(a_{ij})}$, com $a_{ij} \in A/\mathcal{A}$, pois

$$\begin{aligned}
\theta_{\bar{x}}(\bar{x}_1) &= \theta_x(x_1) + \mathcal{A}\mathcal{O}_{\mathbb{L}} = xx_1 + \mathcal{A}\mathcal{O}_{\mathbb{L}} = (a_{11}x_1 + \cdots + a_{1n}x_n) + \mathcal{A}\mathcal{O}_{\mathbb{L}} \\
&= (a_{11}x_1 + \mathcal{A}\mathcal{O}_{\mathbb{L}}) + \cdots + (a_{1n}x_n + \mathcal{A}\mathcal{O}_{\mathbb{L}}) = \overline{a_{11}x_1} + \cdots + \overline{a_{1n}x_1}
\end{aligned}$$

$$\vdots$$

$$\begin{aligned}
\theta_{\bar{x}}(\bar{x}_n) &= \theta_x(x_n) + \mathcal{A}\mathcal{O}_{\mathbb{L}} = xx_n + \mathcal{A}\mathcal{O}_{\mathbb{L}} = (a_{n1}x_1 + \cdots + a_{nn}x_n) + \mathcal{A}\mathcal{O}_{\mathbb{L}} \\
&= (a_{n1}x_1 + \mathcal{A}\mathcal{O}_{\mathbb{L}}) + \cdots + (a_{nn}x_n + \mathcal{A}\mathcal{O}_{\mathbb{L}}) = \overline{a_{n1}x_1} + \cdots + \overline{a_{nn}x_1}.
\end{aligned}$$

Como $Tr_{\mathcal{O}_{\mathbb{L}}|A}(x) = \sum_{i=1}^{n} a_{ii}$ temos que $Tr_{\mathcal{O}_{\mathbb{L}}|A}(\bar{x}) = \sum_{i=1}^{n} \overline{a_{ii}} = \overline{\sum_{i=1}^{n} a_{ii}} = \overline{Tr_{\mathcal{O}_{\mathbb{L}}|A}(x)}$. Portanto, $\det(Tr_{\mathcal{O}_{\mathbb{L}}|A}(\overline{x_i x_j})) = \det(\overline{Tr_{\mathcal{O}_{\mathbb{L}}|A}(x_i x_j)})$, ou seja, $D(\overline{x}_1, \cdots, \overline{x}_n) = \overline{D(x_1, \cdots, x_n)}$. ∎

Definição 2.4.1 *Seja A um anel. Dizemos que $a \in A$ é nilpotente se $a^n = 0$, para algum $n > 0$. Dizemos que A é um anel reduzido se o único elemento nilpotente de A é o zero.*

Lema 2.4.3 *Se A é um anel Noetheriano reduzido, então o ideal nulo de A é uma intersecção finita de ideais primos não nulos de A.*

Demonstração: Pela Lema 1.5.3, temos que todo ideal de um anel noetheriano contém um produto de ideais primos. Portanto, $\langle 0\rangle = \prod_{i=1}^{g} \mathcal{P}_i^{e_i}$. Vamos mostrar que $\langle 0\rangle = \bigcap_{i=1}^{g} \mathcal{P}_i^{e_i}$. Temos que $\langle 0\rangle \subseteq \mathcal{P}_1 \cap \cdots \cap \mathcal{P}_g$. Por outro lado, se $x \in \mathcal{P}_1 \cap \cdots \cap \mathcal{P}_g$, então $x^{e_1+e_2+\cdots+e_g} \in \mathcal{P}_1^{e_1} \cdots \mathcal{P}_g^{e_g} = \langle 0\rangle$. Como A é reduzido, segue que $x = 0$. Portanto, $\langle 0\rangle = \bigcap_{i=1}^{g} \mathcal{P}_i^{e_i}$. ∎

Definição 2.4.2 *Um espaço vetorial V sobre um corpo $\mathbb{K}$, é uma $\mathbb{K}$-álgebra se existe uma multiplicação:*

• $V \times V \longrightarrow V$ *definida por* $(a, b) \longmapsto ab$

satisfazendo,

1. $a(b+c)=ab+ac$, $\forall a, b, c \in V$,
2. $a(\alpha b)=(\alpha a)b=\alpha(ab)$, $\forall \alpha \in \mathbb{K}$ *e* $a, b \in V$,
3. $a(bc)=(ab)c$, $\forall a, b, c \in V$,
4. $\exists 1_V \in V$; $a1_V = a = 1_V a$, $\forall a \in V$.

Observação 2.4.2 *Se $ab = ba$, $\forall a, b \in V$, dizemos que a $\mathbb{K}$-álgebra é comutativa.*

Lema 2.4.4 *Sejam $\mathbb{K}$ um corpo e $\mathbb{L}$ uma $\mathbb{K}$-álgebra comutativa de dimensão finita. Então $\mathbb{L}$ é reduzido se, e somente se, $\mathcal{D}_{\mathbb{L}|\mathbb{K}} \neq \{0\}$.*

Demonstração: Se $\mathbb{L}$ é reduzido, pelo Lema 2.4.3, segue que $\langle 0\rangle = \bigcap_{i=1}^{g} \mathcal{Q}_i$, onde os $\mathcal{Q}_i$ são ideais primos de $\mathbb{L}$ distintos. Assim, $\mathbb{L}/\mathcal{Q}_i$ é um domínio e uma $\mathbb{K}$-álgebra de dimensão finita. Logo, $\mathbb{L}/\mathcal{Q}_i$ é uma extensão algébrica sobre $\mathbb{K}$, ou seja, $\mathbb{L}/\mathcal{Q}_i$ é inteiro sobre $\mathbb{K}$. Como $\mathbb{K}$ é corpo, temos pela Proposição 1.1.3, que $\mathbb{L}/\mathcal{Q}_i$ é corpo. Portanto os ideais $\mathcal{Q}_i$ são maximais e consequêntemente $\mathcal{Q}_i + \mathcal{Q}_j = \mathbb{L}$, para $i \neq j$. Pelo Lema 2.1.5, segue que

$$\prod_{i=1}^{g} \mathbb{L}/\mathcal{Q}_i = \mathbb{L}/\prod_{i=1}^{g} \mathcal{Q}_i = \mathbb{L}/\langle 0\rangle = \mathbb{L},$$

e pelo Lema 2.4.1, temos que $\mathcal{D}_{\mathbb{L}|\mathbb{K}} = \prod_{i=1}^{g} \mathcal{D}_{(\mathbb{L}/\mathcal{Q}_i)/\mathbb{K}}$. Pela Proposição 2.3.5, temos que o discriminante $\mathcal{D}_{(\mathbb{L}/\mathcal{Q}_i)/\mathbb{K}} \neq \langle 0\rangle$ o que implica que $\mathcal{D}_{\mathbb{L}|\mathbb{K}} \neq \langle 0\rangle$. Reciprocamente, suponha que $\mathbb{L}$ não é reduzido. Assim, existe $x \in \mathbb{L}$, $x \neq 0$, x nilpotente. Seja $\{x_1, \cdots, x_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$ com $x = x_1$. Então xx_j é nilpotente, para todo $j = 1, \cdots, n$. Logo, se definirmos $\theta_{xx_j} : \mathbb{L} \longrightarrow \mathbb{L}$, onde $\theta_{xx_j}(a) = axx_j$, para $a \in \mathbb{L}$, temos que θ_{xx_j} possui os autovalores todos nulos, e portanto

$Tr_{\mathbb{L}|\mathbb{K}}(xx_j) = 0$. Logo, a matriz traço $(Tr_{\mathbb{L}|\mathbb{K}}(x_ix_j))$ tem uma linha nula o que implica que $D(x_1, \cdots, x_n) = 0$ e assim $\mathcal{D}_{\mathbb{L}|\mathbb{K}} = \{0\}$, o que é um absurdo. ∎

Teorema 2.4.1 *Seja $\mathbb{K} \subseteq \mathbb{L}$ corpos de números. Sejam $\mathcal{O}_\mathbb{K}$ e $\mathcal{O}_\mathbb{L}$ os anéis dos inteiros de $\mathbb{K}$ e $\mathbb{L}$, respectivamente, e $\mathcal{P}$ um ideal primo de $\mathcal{O}_\mathbb{K}$. Então $\mathcal{P}$ ramifica se, e somente se, $\mathcal{O}_\mathbb{L}/\mathcal{P}\mathcal{O}_\mathbb{L}$ não é reduzido.*

Demonstração: Suponhamos que $\mathcal{P}$ ramifica. Seja $\mathcal{P}\mathcal{O}_\mathbb{L} = \prod_{i=1}^{g} \mathcal{Q}_i^{e_i}$, onde $\mathcal{Q}_i \cap \mathcal{O}_\mathbb{K} = \mathcal{P}$, para $i = 1, \cdots, g$. Como $\mathcal{P}$ ramifica, existe $k \in \mathbb{N}$ tal que $e_k > 1$. Temos que $\mathcal{P}\mathcal{O}_\mathbb{L} \subsetneq \mathcal{Q}_j$, para todo $j = 1, \cdots, g$, pois se $\mathcal{P}\mathcal{O}_\mathbb{L} = \mathcal{Q}_j$ teríamos que $e_j = 1$, o que é contra a hipótese. Assim, para cada $j = 1, \cdots, g$, seja $a_j \in \mathcal{Q}_j - \mathcal{P}\mathcal{O}_\mathbb{L}$. Seja $\bar{x} = a_1 \cdots a_g + \mathcal{P}\mathcal{O}_\mathbb{L} \neq \bar{0}$. Se $r = e_1 \cdots e_g$, então

$$\bar{x}^r = (a_1 \cdots a_g)^r + \mathcal{P}\mathcal{O}_\mathbb{L} = a_1^r \cdots a_k^r \cdots a_g^r + \mathcal{P}\mathcal{O}_\mathbb{L} = \bar{0}.$$

Portanto, $\mathcal{O}_\mathbb{L}/\mathcal{P}\mathcal{O}_\mathbb{L}$ não é reduzido. Reciprocamente, como $\mathcal{P}\mathcal{O}_\mathbb{L} = \prod_{i=1}^{g} \mathcal{Q}_i^{e_i}$, segue que $\mathcal{O}_\mathbb{L}/\mathcal{P}\mathcal{O}_\mathbb{L} \simeq \prod_{i=1}^{g} \mathcal{O}_\mathbb{L}/\mathcal{Q}_i^{e_i}$ e sendo $\mathcal{O}_\mathbb{L}/\mathcal{P}\mathcal{O}_\mathbb{L}$ não reduzido existe $\bar{x} = (x_1 + \mathcal{Q}_1^{e_1}, x_2 + \mathcal{Q}_2^{e_2}, \cdots, x_g + \mathcal{Q}_g^{e_g}) \neq \bar{0}$ nilpotente. Assim, existe j_0 tal que $x_{j_0} \notin \mathcal{Q}_{j_0}^{e_{j_0}}$ e existe $n \in \mathbb{N}$ tal que $\bar{x}^n = \bar{0}$. Portanto, $x_i^n \in \mathcal{Q}_i^{e_i}$, para $i = 1, \cdots, g$. Se $e_{j_0} = 1$ e $x_{j_0}^n \in \mathcal{Q}_{j_0}$ então $x_{j_0} \in \mathcal{Q}_{j_0}$ o que é uma contradição. Portanto, $e_{j_0} > 1$. ∎

Corolário 2.4.1 *Com as hipóteses do Teorema 2.4.1, $\mathcal{P}$ ramifica se, e somente se, $\mathcal{D}_{(\mathcal{O}_\mathbb{L}/\mathcal{P}\mathcal{O}_\mathbb{L})|(\mathcal{O}_\mathbb{K}/\mathcal{P})} = \{0\}$.*

Demonstração: Temos, pelo Teorema 2.4.1, que $\mathcal{P}$ ramifica se, e somente se, $\mathcal{O}_\mathbb{L}/\mathcal{P}\mathcal{O}_\mathbb{L}$ não é reduzido, e pelo Lema 2.4.4, segue que $\mathcal{O}_\mathbb{L}/\mathcal{P}\mathcal{O}_\mathbb{L}$ não é reduzido se, e somente se, $\mathcal{D}_{(\mathcal{O}_\mathbb{L}/\mathcal{P}\mathcal{O}_\mathbb{L})|(\mathcal{O}_\mathbb{K}/\mathcal{P})} = \{0\}$. ∎

Teorema 2.4.2 *Sejam $\mathbb{K} \subseteq \mathbb{L}$ corpos de números. Sejam $\mathcal{O}_\mathbb{K}$ e $\mathcal{O}_\mathbb{L}$ os anéis dos inteiros de $\mathbb{K}$ e $\mathbb{L}$, respectivamente, e $\mathcal{P}$ um ideal primo de $\mathcal{O}_\mathbb{K}$. Então $\mathcal{P}$ ramifica se, e somente se, $\mathcal{P} \supset \mathcal{D}_{\mathcal{O}_\mathbb{L}|\mathcal{O}_\mathbb{K}}$.*

Demonstração: Suponhamos que o ideal primo $\mathcal{P} \subset \mathcal{O}_\mathbb{K}$ ramifica. Sejam $S = \mathcal{O}_\mathbb{K} - \mathcal{P}$, $\mathcal{O}'_\mathbb{K} = S^{-1}\mathcal{O}_\mathbb{K}$, $\mathcal{O}'_\mathbb{L} = S^{-1}\mathcal{O}_\mathbb{L}$ e $\mathcal{P}' = \mathcal{P}\mathcal{O}'_\mathbb{K}$. Pela Proposição 1.8.5, temos que $\mathcal{O}'_\mathbb{K}$ é principal e assim pelo Corolário 1.2.3, temos que $\mathcal{O}'_\mathbb{L}$ é um $\mathcal{O}'_\mathbb{K}$-módulo livre. Pelo Teorema 1.8.2, temos que $\mathcal{O}_\mathbb{K}/\mathcal{P} \simeq \mathcal{O}'_\mathbb{K}/\mathcal{P}'$ e $\mathcal{O}_\mathbb{L}/\mathcal{P}\mathcal{O}_\mathbb{L} \simeq \mathcal{O}'_\mathbb{L}/\mathcal{P}'\mathcal{O}'_\mathbb{L}$. Seja $\{e_1, \cdots, e_n\}$ uma base de $\mathcal{O}'_\mathbb{L}$ sobre $\mathcal{O}'_\mathbb{K}$. Pelo Corolário 2.4.1, temos que $\mathcal{D}_{(\mathcal{O}_\mathbb{L}/\mathcal{P}\mathcal{O}_\mathbb{L})|(\mathcal{O}_\mathbb{K}/\mathcal{P})} = \{0\}$. Assim, $\bar{0} = \overline{D(e_1, \cdots, e_n)} \in \mathcal{O}_\mathbb{K}/\mathcal{P} = \mathcal{O}'_\mathbb{K}/\mathcal{P}'$,

e portanto $D(e_1, \cdots, e_n) \in \mathcal{P}'$. Agora, se $\{x_1, \cdots, x_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ contida em $\mathcal{O}_\mathbb{L}$, então $x_i = \sum_{j=1}^{n} a_{ij}e_j$, com $a_{ij} \in \mathcal{O}'_\mathbb{K}, i = 1, \cdots, n$, pois $\mathcal{O}_\mathbb{L} \subset \mathcal{O}'_\mathbb{L}$. Logo, $D(x_1, \cdots, x_n) \in \mathcal{O}_\mathbb{K}$ e $D(x_1, \cdots, x_n) = \det(a_{ij})^2 D(e_1, \cdots, e_n) \in \mathcal{O}'_\mathbb{K}\mathcal{P}' \subset \mathcal{P}'$. Assim, $D(x_1, \cdots, x_n) \in \mathcal{O}_\mathbb{K} \cap \mathcal{P}' = \mathcal{P}$. Portanto, $\mathcal{D}_{\mathcal{O}_\mathbb{L}|\mathcal{O}_\mathbb{K}} = \langle D(x_1, \cdots, x_n)\rangle \subset \mathcal{P}$. Reciprocamente, se $\mathcal{D}_{\mathcal{O}_\mathbb{L}|\mathcal{O}_\mathbb{K}} \subset \mathcal{P}$ e se $\{e_1, \cdots, e_n\}$ é uma base de $\mathcal{O}'_\mathbb{L}$ sobre $\mathcal{O}'_\mathbb{K}$, então para $i = 1, \cdots, n$, temos que $e_i = \frac{y_i}{s}$, com $y_i \in \mathcal{O}_\mathbb{L}$ e $s \in S$. Assim,

$$\begin{aligned} D(e_1, \cdots, e_n) &= \det(Tr_{\mathbb{L}|\mathbb{K}}(e_ie_j)) = \det\left(Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{y_iy_j}{s^2}\right)\right) \\ &= \frac{1}{s^{2n}}\det(Tr_{\mathbb{L}|\mathbb{K}}(y_iy_j)) = s^{-2n}D(y_1, \cdots, y_n) \in A'\mathcal{D}_{\mathcal{O}_\mathbb{L}|\mathcal{O}_\mathbb{K}} \subseteq \mathcal{O}'_\mathbb{K}\mathcal{P} = \mathcal{P}', \end{aligned}$$

ou seja, $D(e_1, \cdots, e_n) \in \mathcal{P}'$. Assim, $\overline{D(e_1, \cdots, e_n)} = \bar{0}$ em $\mathcal{O}_\mathbb{K}/\mathcal{P}'$ e portanto, $\mathcal{D}_{(\mathcal{O}_\mathbb{L}/\mathcal{P}\mathcal{O}_\mathbb{L})/(\mathcal{O}_\mathbb{K}|\mathcal{P})} = \{0\}$. Pelo Corolário 2.4.1, segue que $\mathcal{P}$ ramifica. ∎

Corolário 2.4.2 *Com as hipóteses do Teorema 2.4.2, temos que existe somente um número finito de ideais primos de $\mathcal{O}_\mathbb{K}$ que ramifica em $\mathcal{O}_\mathbb{L}$.*

Demonstração: Pelo Teorema 2.4.2 temos que o ideal primo $\mathcal{P}$ ramifica se, e somente se, $\mathcal{P} \supset \mathcal{D}_{\mathcal{O}_\mathbb{K}|\mathcal{O}_\mathbb{L}} = \prod_{i=1}^{g} \mathcal{P}_i^{e_i}$. Além disso, os $\mathcal{P}_i$, para $i = 1, \cdots, g$, são os únicos ideais primos de $\mathcal{O}_\mathbb{K}$ que contém $\mathcal{D}_{\mathcal{O}_\mathbb{K}|\mathcal{O}_\mathbb{L}}$, uma vez que se $\mathcal{M}$ é um ideal primo de $\mathcal{O}_\mathbb{K}$ tal que $\mathcal{M} \supset \mathcal{D}_{\mathcal{O}_\mathbb{K}|\mathcal{O}_\mathbb{L}} = \prod_{i=1}^{g} \mathcal{P}_i^{e_i}$, pelo Lema 1.5.2 segue que $\mathcal{M} \supset \mathcal{P}_i$, para algum $i = 1, \cdots, g$. Como $\mathcal{P}_i$ é ideal maximal segue que $\mathcal{M} = \mathcal{P}_i$. ∎

Exemplo 2.4.1 *Sejam $\mathbb{K} = \mathbb{Q}$ e $\mathbb{L} = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados.*
a) Se $d \equiv 2$ ou $3(\text{modulo } 4)$ então $\mathbb{Z}[\sqrt{d}]$ é o anel dos inteiros de $\mathbb{K}$ e $D(1, \sqrt{d}) = 4d$. Assim, os primos que se ramificam em $\mathbb{K}$ é o 2 e os divisores de d.
b) Se $d \equiv 1(\text{modulo } 4)$ então $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ é o anel dos inteiros de $\mathbb{K}$ e $D\left(1, \frac{1+\sqrt{d}}{2}\right) = d$. Assim, os primos que ramificam em $\mathbb{K}$ são os divisores de d.

Proposição 2.4.2 *Seja ξ uma raiz n-ésima primitiva da unidade. Se p não divide n então p não ramifica.*

Demonstração: Seja $f(x)$ o polinômio minimal de ξ e $[\mathbb{Q}[\xi] : \mathbb{Q}] = m$. Temos que o polinômio $f(x) \mid (x^n - 1)$, ou seja, $x^n - 1 = f(x)g(x)$, com $g(x) \in \mathbb{Q}[x]$. Além disso, pela Proposição 2.3.8, temos que $D(1, \cdots, \xi^{m-1}) = \pm N(f'(\xi))$. Como $nx^{n-1} = f'(x)g(x) + f(x)g'(x)$, segue

que, $n\xi^{n-1} = f'(\xi)g(\xi)$, uma vez que $f(\xi) = 0$. Como ξ é uma raiz da unidade, temos que, $N(\xi) = \pm 1$. Então $\pm n^m = N(f'(\xi))N(g(\xi))$ e assim, $N(f'(\xi)) \mid n^m$. Como ξ é inteiro sobre $\mathbb{Z}$, segue que o discriminante absoluto divide $D(1, \cdots, \xi^{m-1})$, e então também divide $\pm n^m$. Portanto, pelo Teorema 2.4.2, p ramifica se, e somente se, $p \mid n^m$. ∎

Exemplo 2.4.2 *Pela Proposição 2.3.9, temos que* $D(1, \xi, \cdots, \xi^{p-2}) = \pm p^{p-2}$. *Assim,* p *é o único primo que ramifica em* $\mathbb{Q}(\xi_p)$.

2.5 Teorema de Kummer

Sejam A um domínio de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita e separável de $\mathbb{K}$ de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros de $\mathbb{L}$ sobre A. Se $\mathcal{P}$ é um ideal primo não nulo de A, pelos Teoremas 1.6.2 e 2.1.1 temos que $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} \mathcal{Q}_i^{e_i}$, onde $\sum_{i=1}^{g} e_i f_i = n$ com o grau $[\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i : A/\mathcal{P}] = f_i, i = 1, \cdots, g$. Nesta seção, apresentamos devido a Kummer, que tal decomposição pode ser explicitamente indicada a partir da fatoração do polinômio minimal $m_{\alpha|\mathbb{K}}(x)$ módulo $\mathcal{P}A[x]$, onde α é um elemento de $\mathcal{O}_{\mathbb{L}}$ tal que $\mathcal{O}_{\mathbb{L}} = A[\alpha]$. Para os próximos resultados usamos as notações $f(x) = \sum_{i=1}^{g} a_i x^i \in A[x]$ e $\bar{f}(x) = \sum_{i=1}^{g} (a_i + \mathcal{P})x^i \in (A/\mathcal{P})[x]$.

Teorema 2.5.1 *Sejam* $\mathcal{O}_{\mathbb{L}} = A[\alpha]$, *onde* $\alpha \in \mathcal{O}_{\mathbb{L}}$, *e* $m_{\alpha|\mathbb{K}}(x)$ *o polinômio minimal de* α *sobre* $\mathbb{K}$. *Sejam* $m_1(x), ..., m_g(x)$ *polinômios mônicos em* $A[x]$ *tal que* $\overline{m}(x) = \overline{m_1(x)^{e_1}} \cdots \overline{m_g(x)^{e_g}}$ *é a fatoração de* $\overline{m}(x)$ *em polinômios irredutíveis distintos em* $(A/\mathcal{P})[x]$. *Então existem ideais primos distintos* $\mathcal{Q}_1, \cdots, \mathcal{Q}_g$ *de* $\mathcal{O}_{\mathbb{L}}$ *acima de* $\mathcal{P}$ *tal que* $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i = A/\mathcal{P}(\overline{\alpha_i})$, *onde* $\overline{\alpha_i}$ *é uma raiz de* $\overline{m}_i(x)$, *e assim* $f(\mathcal{Q}_i|\mathcal{P}) = gr(\overline{m_i})$, *para* $i = 1, \cdots, g$.

Demonstração: Para cada $i = 1, \cdots, g$ seja $\overline{\alpha_i}$ uma raiz de $\overline{m_i}(x)$ num fecho algébrico de $A/\mathcal{P}$. Logo, $\overline{m_i}(x)$ é o polinômio minimal de $\overline{\alpha_i}$ sobre $A/\mathcal{P}$. O homomorfismo λ_i de $A[x]$ sobre $(A/\mathcal{P})[\overline{\alpha_i}]$, definido por $f(x) \longmapsto \bar{f}(\overline{\alpha_i})$, $f(x) \in A[x]$ induz um homomorfismo $\bar{\lambda}_i$ de $A[x]/\langle m \rangle$ sobre $(A/\mathcal{P})[\overline{\alpha_i}]$, uma vez que $\lambda_i(m(x)) = 0$. Por outro lado, o homomorfismo φ de $A[x]$ sobre $A[\alpha]$, definido por $f \longmapsto f(\alpha)$, tem como núcleo o ideal principal $\langle m(x) \rangle$ de $A[x]$. Assim, φ induz um isomorfismo $\bar{\varphi} : A[x]/\langle m(x) \rangle \longrightarrow A[\alpha]$. Como $\bar{\lambda}_i$ e $\bar{\varphi}^{-1}$ são homomorfismos, segue que $u_i = \bar{\lambda}_i \circ \bar{\varphi}^{-1}$ é um homomorfismo sobrejetor de $A[\alpha]$ sobre $(A/\mathcal{P})[\overline{\alpha_i}]$. Assim, $u_i(f(\alpha)) = \bar{f}(\overline{\alpha_i})$, para todo $f \in A[x]$. Assim, $\mathcal{O}_{\mathbb{L}}/\ker(u_i) \simeq (A/\mathcal{P})[\overline{\alpha_i}]$. Como $(A/\mathcal{P})[\overline{\alpha_i}]$ é um corpo segue que $\ker(u_i)$ é um ideal maximal $\mathcal{Q}_i$ de $\mathcal{O}_{\mathbb{L}}$. Como $\mathcal{P} \subseteq \mathcal{Q}_i \cap A \neq A$ e da maximilidade de $\mathcal{P}$, segue que $\mathcal{P} = \mathcal{Q}_i \cap A$. Temos que, como a restrição de u_i a A, $(u_i)_{|A} : A \longrightarrow (A/\mathcal{P})[\overline{\alpha_i}]$, coincide

com o homomorfismo canônico de A sobre $(A/\mathcal{P})[\overline{\alpha_i}]$, segue que $\bar{u}_i$ é um $A/\mathcal{P}$-isomorfismo de $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i$ sobre $(A/\mathcal{P})[\overline{\alpha_i}]$. Logo, $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i = (A/\mathcal{P})[\widetilde{\alpha}_i]$, para uma certa raiz $\widetilde{\alpha}_i \in \mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i$ de $\overline{m_i}(x)$. Portanto, $f(\mathcal{Q}_i|\mathcal{P}) = \mathrm{gr}(\overline{m_i})$. Como $u_i(m_j(\alpha)) = 0 \neq u_i(m_i(\alpha))$, para $i \neq j$, segue que $\mathcal{Q}_i$ são distintos dois a dois. ∎

Teorema 2.5.2 *Com as hipóteses do Teorema 2.5.1 temos que* $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} \mathcal{Q}_i^{e_i}$, *onde* $\mathcal{Q}_i = \mathcal{P}\mathcal{O}_{\mathbb{L}} + m_i(\alpha)\mathcal{O}_{\mathbb{L}}$ *são ideais primos de* $\mathcal{O}_{\mathbb{L}}$ *acima de* $\mathcal{P}$ *e* $e(\mathcal{Q}_i|\mathcal{P}) = e_i$, *para* $i = 1, \cdots, g$.

Demonstração: Temos que $\mathcal{P}\mathcal{O}_{\mathbb{L}} + m_i(\alpha)\mathcal{O}_{\mathbb{L}} \subseteq \mathcal{Q}_i$, para $i = 1, \cdots, g$. Por outro lado, seja $\beta \in \mathcal{Q}_i$. Como $\mathcal{Q}_i \in \mathcal{O}_{\mathbb{L}} = A[\alpha]$ temos que $\beta = g(\alpha)$, com $g \in A[x]$. Como $\bar{g}(\overline{\alpha_i}) = u_i(g(\alpha)) = 0$ e como $\overline{m}_i(x)$ é o polinômio minimal de $\overline{\alpha_i}$ sobre $A/\mathcal{P}$, segue que existe $h \in A[x]$ tal que $\bar{g}(x) = \overline{m_i}(x)\cdot\bar{h}(x)$. Logo, $g(x) - m_i(x)h(x)$ tem seus coeficientes em $\mathcal{P}$, e $\beta = (g - m_i h)(\alpha) + m_i(\alpha)h(\alpha) \in \mathcal{P}\mathcal{O}_{\mathbb{L}} + m_i(\alpha)\mathcal{O}_{\mathbb{L}}$. Finalmente, temos que $\mathcal{Q}_1^{e_1}\cdots\mathcal{Q}_g^{e_g} \subseteq \mathcal{P}\mathcal{O}_{\mathbb{L}}$, pois $(\mathcal{A}+\mathcal{O}_{\mathbb{L}})\cdot(\mathcal{A}+\mathcal{C}) \subseteq \mathcal{A}+\mathcal{B}\mathcal{C}$, para quaisquer ideais $\mathcal{A}, \mathcal{B}, \mathcal{C}$ de $\mathcal{O}_{\mathbb{L}}$, e que

$$\mathcal{Q}_1^{e_1}\cdots\mathcal{Q}_g^{e_g} \subseteq (\mathcal{P}\mathcal{O}_{\mathbb{L}} + m_1(\alpha)^{e_1}\mathcal{O}_{\mathbb{L}})(\mathcal{P}\mathcal{O}_{\mathbb{L}} + m_2(\alpha)^{e_2}\mathcal{O}_{\mathbb{L}})\cdots(\mathcal{P}\mathcal{O}_{\mathbb{L}} + m_n(\alpha)^{e_n}\mathcal{O}_{\mathbb{L}}) \subset \mathcal{P}\mathcal{O}_{\mathbb{L}} + \gamma\mathcal{O}_{\mathbb{L}},$$

onde $\gamma = m_1(\alpha)^{e_1}\cdots m_g(\alpha)^{e_g}$. Como o polinômio $m_1(x)^{e_1}\cdots m_g(x)^{e_g} - m(x)$ tem seus coeficientes em $\mathcal{P}$ e $m(\alpha) = 0$ temos que $\gamma = (m_1(x)^{e_1}\cdots m_g(x)^{e_g} - m(x))(\alpha) \in \mathcal{P}\mathcal{O}_{\mathbb{L}}$. Assim, $\mathcal{Q}_1^{e_1}\cdots\mathcal{Q}_g^{e_g} \subset \mathcal{P}\mathcal{O}_{\mathbb{L}}$, ou seja, $\mathcal{Q}_1^{e_1}\cdots\mathcal{Q}_g^{e_g}$ é um múltiplo de $\mathcal{P}\mathcal{O}_{\mathbb{L}}$. Logo, $\mathcal{Q}_1^{e_1}\cdots\mathcal{Q}_g^{e_g}$ são os únicos ideais primos de $\mathcal{O}_{\mathbb{L}}$ que estão acima de $\mathcal{P}$ e que $e(\mathcal{Q}_i|\mathcal{P}) \leq e_i$. Portanto,

$$\sum_{i=1}^{g} e(\mathcal{Q}_i|\mathcal{P})f(\mathcal{Q}_i|\mathcal{P}) \leq \sum_{i=1}^{g} e_i gr(\overline{m_i}) = gr(\overline{m}) = n.$$

Pelo Teorema 2.1.1, temos que $\sum_{i=1}^{g} e(\mathcal{Q}_i|\mathcal{P})f(\mathcal{Q}_i|\mathcal{P}) = \sum_{i=1}^{g} e_i gr(\overline{m_i}) = n$. Portanto, $e(\mathcal{Q}_i|\mathcal{P}) = e_i$, para $i = 1, \cdots, g$ e $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \mathcal{Q}_1^{e_1}\cdots\mathcal{Q}_g^{e_g}$. ∎

Observação 2.5.1 *O Teorema de Kummer foi dividido nos Teoremas 2.5.1 e 2.5.2.*

Corolário 2.5.1 *Com as hipóteses do Teorema 2.5.1, temos que:*

a) $\mathcal{P}$ *decompõe em* $\mathbb{L}$ *se, e somente se,* $\overline{m}(x)$ *fatora em* $(A/\mathcal{P})[x]$ *em fatores lineares distintos* $x - (a_i + \mathcal{P})$, *para* $i = 1, \cdots, n$. *Neste caso,* $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \mathcal{Q}_1\cdots\mathcal{Q}_n$, *onde* $\mathcal{Q}_j = \mathcal{P}\mathcal{O}_{\mathbb{L}} + (\alpha - a_i)\mathcal{O}_{\mathbb{L}}$ *são ideais primos distintos de* $\mathcal{O}_{\mathbb{L}}$, *para* $i = 1, \cdots, n$.

b) $\mathcal{P}$ *é inerte em* $\mathbb{L}$ *se, e somente se,* $\overline{m}(x)$ *é irredutível em* $(A/\mathcal{P})[x]$. *Neste caso,* $\mathcal{P}\mathcal{O}_{\mathbb{L}}$ *é um ideal primo de* $\mathcal{O}_{\mathbb{L}}$.

c) $\mathcal{P}$ *é totalmente ramificado em* $\mathbb{L}$ *se, e somente se,* $\overline{m}(x)$ *é uma potência n-ésima em* $(A/\mathcal{P})[x]$, *isto é,* $\overline{m}(x) = (x - (a + \mathcal{P}))^n$, *para algum* $a \in A$. *Neste caso,* $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \mathcal{Q}^n$, *onde* $\mathcal{Q} = \mathcal{P}\mathcal{O}_{\mathbb{L}} + (\alpha - a)\mathcal{O}_{\mathbb{L}}$ *é um ideal de* $\mathcal{O}_{\mathbb{L}}$.

Demonstração: a) Como $\mathcal{P}$ decompõe em $\mathbb{L}$, segue que

$$g = n \text{ e } e(\mathcal{Q}_i|\mathcal{P}) = f(\mathcal{Q}_i|\mathcal{P}) = 1$$

para todo ideal primo $\mathcal{Q}_i$ de $\mathcal{O}_{\mathbb{L}}$ que esta acima de $\mathcal{P}$. Assim, pelo Teorema 2.5.1, temos que $gr(\overline{m_i}) = 1$, para $i = 1, \cdots, n$. Logo, $\overline{m_i}(x) = (x - (a_i + \mathcal{P}))$, para $i = 1, \cdots, n$. Pelo Teorema 2.5.2, temos que $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \mathcal{Q}_1 \cdots \mathcal{Q}_n$, onde $\mathcal{Q}_i = \mathcal{P}\mathcal{O}_{\mathbb{L}} + (\alpha - a_i)\mathcal{O}_{\mathbb{L}}$ são ideais primos de $\mathcal{O}_{\mathbb{L}}$. Por outro lado, se $m(x)$ fatora em $(A/\mathcal{P})[x]$ em fatores lineares distintos $x - (a_i + \mathcal{P})$, para $i = 1, \cdots, n$, então pelo Teorema 2.5.1, segue que $f(\mathcal{Q}_i|\mathcal{P}) = gr(\overline{m_i}) = 1$. Logo, pelo Teorema 2.1.1, temos que $e_i = 1$, para $i = 1, \cdots, n$. Assim, pelo Teorema 2.5.2 temos que $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \mathcal{Q}_1 \cdots \mathcal{Q}_n$. Portanto, $\mathcal{P}$ decompõe em $\mathbb{L}$.
b) Se $\mathcal{P}$ é inerte em $\mathbb{L}$, temos que

$$g = n,\ e(\mathcal{Q}_1|\mathcal{P}) = 1 \text{ e } f(\mathcal{Q}_1|\mathcal{P}) = n,$$

onde $\mathcal{Q}_1$ é um ideal primo de $\mathcal{O}_{\mathbb{L}}$ que esta acima de $\mathcal{P}$. Pelo Teorema 2.5.1 temos que, $gr(\overline{m_1}) = n$. Assim, $\overline{m}_1(x)$ é irredutível em $(A/\mathcal{P})[x]$. Por outro lado, se $\overline{m}_1(x)$ é irredutível em $(A/\mathcal{P})[x]$, pelo Teorema 2.5.1, segue que $f(\mathcal{Q}_1|\mathcal{P}) = n$. Pelo Teorema 2.1.1, temos que $e_1 = 1$. Assim, pelo Teorema 2.5.2, temos que $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \mathcal{Q}_1$. Portanto, $\mathcal{P}$ é inerte em $\mathbb{L}$.
c) Se $\mathcal{P}$ é totalmente ramificado em $\mathbb{L}$, temos que

$$g = n, e(\mathcal{Q}_i|\mathcal{P}) = n \text{ e } f(\mathcal{Q}_i|\mathcal{P}) = 1,$$

onde $\mathcal{Q}_i$ são ideais primos de $\mathcal{O}_{\mathbb{L}}$ que esta acima de $\mathcal{P}$, para $i = 1, \cdots, n$. Assim, pelo Teorema 2.5.1, temos que gr $(\overline{m_i}) = 1$, $i = 1, \cdots, n$. Logo, $\overline{m}_i(x) = (x - (a_i + \mathcal{P}))$, para $i = 1, \cdots, n$, e $\overline{m}(x) = (x - (a + \mathcal{P}))^n$. Pelo Teorema 2.5.2, segue que $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \mathcal{Q}_1^n$, onde $\mathcal{Q}_1 = \mathcal{P}\mathcal{O}_{\mathbb{L}} + (\alpha - a)\mathcal{O}_{\mathbb{L}}$ é um ideal primo de $\mathcal{O}_{\mathbb{L}}$. Por outro lado, $\overline{m}(x)$ é uma potência n-ésima em $(A/\mathcal{P})[x]$, e então pelo Teorema 2.5.1 temos que $f(\mathcal{Q}_1|\mathcal{P}) = gr(\overline{m}_1) = 1$. Pelo Teorema 2.1.1, temos que $e_1 = n$. Assim, pelo Teorema 2.5.2, segue que $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \mathcal{Q}_1^n$. Portanto, $\mathcal{P}$ é totalmente ramificado em $\mathbb{L}$.■

Exemplo 2.5.1 *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\alpha)$. Pelo Teorema 1.3.1 temos que o anel dos inteiros de $\mathbb{K}$ é $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{-1}]$. Para $\mathcal{P} = \langle 3 \rangle$, temos que*

$$x^2 + 1 = m_{\alpha|\mathbb{Q}}(x)$$

é irredutível módulo $3\mathbb{Z}[x]$. Assim, pelo Corolário 2.5.1, temos que $\langle 3 \rangle$ é totalmente inerte, ou seja,

$$3\mathcal{O}_{\mathbb{K}} = \mathcal{Q},$$

onde $\mathcal{Q}$ é um ideal primo de $\mathcal{O}_{\mathbb{K}}$, com $e(\mathcal{Q}|\mathcal{P}) = 1$, e pelo Teorema 2.5.1, temos que $f(\mathcal{Q}|\mathcal{P}) = 2$. Se $\mathcal{P} = \langle 5 \rangle$, temos que

$$x^2 + 1 = m_{\alpha|\mathbb{Q}}(x) = (x+2)(x+3)$$

módulo $5\mathbb{Z}[x]$. Assim, pelo Corolário 2.5.1, temos que $\langle 5 \rangle$ é totalmente decomposto, ou seja,

$$5\mathcal{O}_{\mathbb{K}} = \mathcal{Q}_1\mathcal{Q}_2,$$

onde $\mathcal{Q}_1 = \langle 5, \alpha + 2 \rangle, \mathcal{Q}_2 = \langle 5, \alpha + 3 \rangle$ são ideais primos de $\mathcal{O}_{\mathbb{L}}$ com $e(\mathcal{Q}_1|\mathcal{P})e(\mathcal{Q}_2|\mathcal{P}) = 1$ e $f(\mathcal{Q}_1|\mathcal{P})f(\mathcal{Q}_2|\mathcal{P}) = 1$.

Exemplo 2.5.2 *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{10})$. Pelo Teorema 1.3.1, temos que o anel dos inteiros de $\mathbb{Q}(\sqrt{10})$ é $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}(\sqrt{10})$. Para $\mathcal{P} = \langle 2 \rangle$, temos que*

$$x^2 - 10 = m_{\sqrt{10}|\mathbb{Q}}(x) = x^2$$

módulo $2\mathbb{Z}[x]$. Então $\langle 2 \rangle \mathcal{O}_{\mathbb{L}} = \mathcal{P}^2$, onde $\mathcal{P} = \langle 2, 10 \rangle$. Assim, $e(\mathcal{P}|\langle 2 \rangle) = 2$. Portanto, $\mathcal{P} = \langle 2 \rangle$ é totalmente ramificado em $\mathbb{Q}(\sqrt{10})$. Para $\mathcal{P} = \langle 3 \rangle$ um ideal primo de $\mathbb{Z}$ temos que

$$x^2 - 10 = m_{\sqrt{10}|\mathbb{Q}}(x) = (x+1)(x-1)$$

módulo $3\mathbb{Z}[x]$, e então $\langle 3 \rangle \mathcal{O}_{\mathbb{L}} = \langle 3, 1 + \sqrt{10} \rangle \langle 3, 1 - \sqrt{10} \rangle = \mathcal{P}\mathcal{P}'$. Assim, $e(\mathcal{P}|\langle 3 \rangle) = e(\mathcal{P}'|\langle 3 \rangle) = 1$ e $f(\mathcal{P}|\langle 3 \rangle) = f(\mathcal{P}'|\langle 3 \rangle) = 1$. Portanto, $\mathcal{P} = \langle 3 \rangle$ é totalmente decomposto em $\mathbb{Q}(\sqrt{10})$.

Corolário 2.5.2 *Com as hipóteses do Teorema 2.5.1, temos que $\mathcal{P}$ ramifica em $\mathbb{L}$ se, e somente se, o polinômio $\overline{m_{\alpha|\mathbb{K}}}(x) \in (A/\mathcal{P})[x]$ é inseparável.*

Demonstração: Seja $m(x) = m_{\alpha|\mathbb{K}}(x)$. Pelo Teorema 2.5.1, $\mathcal{P}$ ramifica em $\mathbb{L}$ se, e somente se, na fatoração $\overline{m}(x) = \overline{m_1^{e_1}}(x) \cdots \overline{m_g^{e_g}}(x)$, tivermos que $e_i > 1$ ou $\overline{m_i^{e_i}}$ for inseparável para algum $i = 1, \cdots, g$. Mas isto ocorre se, e somente se, $\bar{m}(x)$ for inseparável. ∎

Corolário 2.5.3 *Com as hipóteses do Teorema 2.5.1, temos que o polinômio $\overline{m_{\alpha|\mathbb{K}}}(x) \in (A/\mathcal{P})[x]$ é inseparável se, e somente se, $D(m_{\alpha|\mathbb{K}}) \in \mathcal{P}$.*

Demonstração: Seja $m(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Temos que $D_{\mathbb{L}|\mathbb{K}}(m) = C(a_1, \cdots, a_n)$, onde $C \in \mathbb{Z}[x_1, \cdots, x_n]$. Assim,

$$D_{\mathbb{L}|\mathbb{K}}(\bar{m}) = C(a_1 + \mathcal{P}, \cdots, a_n + \mathcal{P}) = C(a_1, \cdots, a_n) + \mathcal{P}.$$

Portanto, o polinômio $\bar{m}(x)$ é inseparável se, e somente se, $D_{\mathbb{L}|\mathbb{K}}(\bar{m}) = \bar{0}$ se, e somente se, $C(a_1, \cdots, a_n) \in \mathcal{P}$. ∎

Corolário 2.5.4 *Com as hipóteses do Teorema 2.5.1, temos que* $D(m_{\alpha|\mathbb{K}}) \in \mathcal{P}$ *se, e somente se,* $\mathcal{P}$ *divide* $\mathcal{D}_{\mathcal{O}_{\mathbb{L}}|A}$.

Demonstração: Temos que $\mathcal{D}_{\mathcal{O}_{\mathbb{L}}|A} = \langle D(1, \alpha, \cdots, \alpha^{n-1})\rangle$, onde $\{1, \alpha, \cdots, \alpha^{n-1}\}$ é uma base de $\mathcal{O}_{\mathbb{L}}$ sobre A. Mas $D(1, \alpha, \cdots, \alpha^{n-1}) = D(m) \in \mathcal{P}$ se, e somente se, $\mathcal{P}$ divide $D(1, \alpha, \cdots, \alpha^{n-1})$ se, e somente se, $\mathcal{P}$ divide $\mathcal{D}_{\mathcal{O}_{\mathbb{L}}|A}$. ■

Como a existência de um elemento α tal que $\mathcal{O}_{\mathbb{L}} = A[\alpha]$ nem sempre é satisfeira, mostraremos, que esta hipótese pode ser substituída usando anéis de frações. Mais precisamente, escolhendo um elemento primitivo $\gamma \in \mathcal{O}_{\mathbb{L}}$ da extensão $\mathbb{K} \subseteq \mathbb{L}$, relacionaremos a decomposição de $\mathcal{P}$ em $\mathbb{L}$ com a fatoração módulo $\mathcal{P}A[x]$ do polinômio minimal $m_{\gamma|\mathbb{K}}(x)$, para quase todos os ideais primos não nulos $\mathcal{P}$ de A. Para isto, basta excluir os ideais $\mathcal{P}$ tais que $D(m_{\gamma|\mathbb{K}}) \in \mathcal{P}$.

Corolário 2.5.5 *Sejam* $\gamma \in \mathcal{O}_{\mathbb{L}}$ *tal que* $\mathbb{L} = \mathbb{K}[\gamma]$, $\mathcal{P}$ *um ideal primo não nulo de* A *tal que* $D(m_{\gamma|\mathbb{K}}) \notin \mathcal{P}$ *e S=A-*$\mathcal{P}$. *Então*
a) $\{1, \gamma, \cdots, \gamma^{n-1}\}$ *é uma base do* A'*-módulo* $\mathcal{O}'_{\mathbb{L}}$.
b) O polinômio $\overline{m}_{\gamma|\mathbb{K}}(x) \in (A/\mathcal{P})[x]$ *é separável.*
c) Se $m_1(x), \cdots, m_g(x)$ *são polinômios mônicos em* $A[x]$ *tal que* $\overline{m}_{\gamma|\mathbb{K}}(x) = \bar{m}_1(x) \cdots \bar{m}_g(x)$ *seja a fatoração de* $\overline{m}_{\gamma|\mathbb{K}}(x)$ *em polinômios irredutíveis em* $(A/\mathcal{P})[x]$, *então os Teorema 2.5.1 e 2.5.2, são válidos com* $e_1 = \cdots = e_g = 1$ *e* γ *em lugar de* α.

Demonstração: a) Pela Proposição 1.8.4, temos que $\mathcal{O}'_{\mathbb{L}}$ é o anel dos inteiros de A' e pela Proposição 1.8.5, A' é principal. Logo, pelo Corolário 1.2.3, $\mathcal{O}'_{\mathbb{L}}$ considerado como um A'-módulo possui uma base $\{\beta_1, \cdots, \beta_n\}$. Como $\gamma \in \mathcal{O}_{\mathbb{L}}$, temos que $\gamma^{i-1} = \sum_{j=1}^{n} a_{ij}\beta_j$, $i = 1, \cdots, n$. Pela Proposição 2.3.1, temos que

$$D(m_{\gamma|\mathbb{K}}) = D(1, \gamma, \cdots, \gamma^{n-1}) = \det(a_{ij})^2 D(\beta_1, \cdots, \beta_n).$$

Como $D(m_{\gamma|\mathbb{K}}) \in A - \mathcal{P} \subseteq A' - (\mathcal{P}A')$ é inversível em A', segue que $\det(a_{ij})$ também é inversível. Assim, $\{1, \gamma, \cdots, \gamma^{n-1}\}$ é uma base do A'- módulo $\mathcal{O}'_{\mathbb{L}}$.
b) Como $D(m_{\gamma|\mathbb{K}}) \notin \mathcal{P}$, segue pelo Teorema 2.4.2, que $\mathcal{P}$ não ramifica em $\mathbb{K}$, e assim temos pelo Corolário 2.5.2, que $m_{\gamma|\mathbb{K}}(x)$ módulo $\mathcal{P}A'$ é um polinômio separável em $(A'/\mathcal{P}A')[x]$. Pelo Teorema 1.8.2, temos que $A'/\mathcal{P}A' \simeq A/\mathcal{P}$. Assim, podemos identificar $(A'/\mathcal{P}A')[x] \simeq (A/\mathcal{P})[x]$. Logo, o polinômio $\overline{m}_{\gamma|\mathbb{K}}(x)$ é separável em $(A/\mathcal{P})[x]$.
c) Pela demonstração da Proposição 1.8.2 temos que se $\mathcal{Q} \subseteq \mathcal{O}_{\mathbb{L}}$ então

$$\mathcal{Q}\mathcal{O}'_{\mathbb{L}} \cap \mathcal{O}_{\mathbb{L}} = \mathcal{Q}. \tag{2.6}$$

Pelo Teorema 2.5.2 temos que $\mathcal{P}\mathcal{O}_{\mathbb{L}}^{'} = \mathcal{D}_1 \cdots \mathcal{D}_r$, onde os ideais primos $\mathcal{D}_i$ de $\mathcal{O}_{\mathbb{L}}^{'}$, distintos e acima de $\mathcal{P}A^{'}$ são da forma $\mathcal{D}_i = \mathcal{P}\mathcal{O}_{\mathbb{L}}^{'} + m_i(\gamma)\mathcal{O}_{\mathbb{L}}^{'} = (\mathcal{P}\mathcal{O}_{\mathbb{L}} + m_i(\gamma)\mathcal{O}_{\mathbb{L}})\mathcal{O}_{\mathbb{L}}^{'}$. Pela demonstração do Teorema 2.1.1, temos que $\mathcal{D}_i = \mathcal{Q}_i\mathcal{O}_{\mathbb{L}}^{'}$ e $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \mathcal{Q}_1 \cdots \mathcal{Q}_r$ onde $\mathcal{Q}_1, \cdots, \mathcal{Q}_r$, são os únicos ideais primos de $\mathcal{O}_{\mathbb{L}}$ acima $\mathcal{P}$. Pela equação (2.6), temos que $\mathcal{Q}_i = \mathcal{D}_i \cap \mathcal{O}_{\mathbb{L}} = (\mathcal{P} + m_i(\gamma)\mathcal{O}_{\mathbb{L}})\mathcal{O}_{\mathbb{L}}{}' \cap \mathcal{O}_{\mathbb{L}}$ $= \mathcal{P}\mathcal{O}_{\mathbb{L}} + m_i(\gamma)\mathcal{O}_{\mathbb{L}}$. Pelo Teorema 2.5.1, temos que $\mathcal{O}_{\mathbb{L}}^{'}/\mathcal{D}_i = (A^{'}/\mathcal{P}A^{'})\bar{\gamma}_i$, onde $\bar{\gamma}_i$ é uma raiz de $\bar{m}_i(x)$ e pelo Teorema 2.1.1, temos que $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i = (A/\mathcal{P})(\bar{\gamma}_i)$ e $e_1 = \cdots = e_r = 1$. ∎

Teorema 2.5.3 *Sejam $\mathcal{P}$ um ideal primo de A e $\mathbb{L} = \mathbb{K}[\gamma]$, onde $\gamma \in \mathcal{O}_{\mathbb{L}}$ é uma raiz de um polinômio $m(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$ tal que $a_{n-1}, \cdots, a_0 \in \mathcal{P}$ e $a_0 \notin \mathcal{P}^2$. Então $m(x)$ é irredutível em $\mathbb{K}[X]$, $n = [\mathbb{L} : \mathbb{K}]$ e $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \mathcal{Q}^n$, onde $\mathcal{Q} = \mathcal{P}\mathcal{O}_{\mathbb{L}} + \gamma\mathcal{O}_{\mathbb{L}}$ é um ideal primo de $\mathcal{O}_{\mathbb{L}}$. Neste caso, $\mathcal{P}$ é totalmente ramificado em $\mathbb{L}$.*

Demonstração: Seja $\mathcal{Q}$ um ideal primo de $\mathcal{O}_{\mathbb{L}}$ tal que $\mathcal{Q} \cap A = \mathcal{P}$ e $e = e(\mathcal{Q}|\mathcal{P})$. Como $a_0 \notin \mathcal{P}^2$, $a_0 \in \mathcal{P}$ e $\langle a_0 \rangle$ é ideal de A, segue que $a_0 A = \mathcal{P}\mathcal{I}$, onde $\mathcal{I}$ é um ideal de A não divisível por $\mathcal{P}$. Temos que $a_0\mathcal{O}_{\mathbb{L}} = \mathcal{Q}^e\mathcal{A}$, onde $\mathcal{A}$ é um ideal de $\mathcal{O}_{\mathbb{L}}$ não divisível por $\mathcal{Q}$. Como $\gamma^n + a_{n-1}\gamma^{n-1} + \cdots + a_0 = 0$, temos que

$$\gamma^n = -(a_{n-1}\gamma^{n-1} + \cdots + a_0) \in \mathcal{P}\mathcal{O}_{\mathbb{L}} \subseteq \mathcal{Q}.$$

Logo $\gamma \in \mathcal{Q}$, e assim $\gamma^n \in \mathcal{Q}^n$ e $\{a_{n-1}\gamma^{n-1}, \cdots, a_1\gamma\} \subseteq (\mathcal{P}\mathcal{O}_{\mathbb{L}})\mathcal{Q} \subseteq \mathcal{Q}^{e+1}$. Como $\mathcal{Q}^{e+1}$ não divide $a_0\mathcal{O}_{\mathbb{L}}$ temos que $\gamma^n + a_{n-1}\gamma^{n-1} + \cdots + a_1\gamma = -a_0 \notin \mathcal{Q}^{e+1}$. Assim, $\gamma^n \notin \mathcal{Q}^{e+1}$ e portanto, $n \leq e$. Sendo m um múltiplo em $\mathbb{K}[x]$ do polinômio $m_{\gamma|K}(x)$, temos que

$$[\mathbb{L} : \mathbb{K}] = gr(m_{\gamma|\mathbb{K}}) \leq gr(m) = n \leq e.$$

Pelo Teorema 2.1.1, segue que $[\mathbb{L} : \mathbb{K}] = n$ e que $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \mathcal{Q}^n$. Como $\mathcal{Q}^n = \mathcal{P}\mathcal{O}_{\mathbb{L}} \subseteq \mathcal{P}\mathcal{O}_{\mathbb{L}} + \gamma\mathcal{O}_{\mathbb{L}} \subseteq \mathcal{Q}$ segue que $\mathcal{P}\mathcal{O}_{\mathbb{L}} + \gamma\mathcal{O}_{\mathbb{L}} = \mathcal{Q}^m$, para algum $m = 1, \cdots, n$. Temos que $m = 1$, pois caso contrário $\gamma \in \mathcal{Q}^2$, e assim, $\gamma^n \in \mathcal{Q}^{2n} \subseteq \mathcal{Q}^{e+1}$, o que é um absurdo. ∎

Proposição 2.5.1 *Sejam $\mathcal{P}$ um ideal primo não nulo de A, totalmente ramificado em $\mathbb{L}$, $\mathcal{Q}$ o único ideal primo de $\mathcal{O}_{\mathbb{L}}$ tal que $\mathcal{Q} \cap A = \mathcal{P}$ e S=A-$\mathcal{P}$. Então $\mathcal{P}A^{'}$ é totalmente ramificado em $\mathbb{L}$, onde $\mathcal{Q}\mathcal{O}_{\mathbb{L}}^{'}$ é o único ideal de $\mathcal{O}_{\mathbb{L}}^{'}$ tal que $\mathcal{Q}\mathcal{O}_{\mathbb{L}}^{'} \cap A = \mathcal{P}A^{'}$.*

Demonstração: Pela Proposição 1.8.5, temos que $(\mathcal{P}A^{'})\mathcal{O}_{\mathbb{L}}^{'} = \prod_{i=1}^{g}(\mathcal{Q}\mathcal{O}_{\mathbb{L}}^{'})^{e_i}$. Como $\mathcal{P}$ é totalmente ramificado, temos que $e(\mathcal{Q}_1 : \mathcal{P}) = n$ e $f(\mathcal{Q}_1 : \mathcal{P}) = 1$. Pelo Teorema 1.8.2, segue que $\mathcal{O}_{\mathbb{L}}^{'}/\mathcal{Q}_1\mathcal{O}_{\mathbb{L}}^{'} \simeq \mathcal{O}_{\mathbb{L}}/\mathcal{Q}_1\mathcal{O}_{\mathbb{L}}$ e $A^{'}/\mathcal{P}A^{'} \simeq A/\mathcal{P}$. Assim, $e(\mathcal{Q}_1\mathcal{O}_{\mathbb{L}}^{'} : \mathcal{P}A^{'}) = n$ e $f(\mathcal{Q}_1\mathcal{O}_{\mathbb{L}}^{'} : \mathcal{P}A^{'}) = 1$. Portanto, $\mathcal{P}A^{'}$ é totalmente ramificado em $\mathbb{L}$. ∎

2.6 Reticulados

Nesta seção, apresentamos o conceito de reticulados no $\mathbb{R}^n$ enfocando algumas propriedades.

Definição 2.6.1 *1) Um subgrupo $H \subset \mathbb{R}^n$ é discreto se $H \cap K$ é finito, para todo subconjunto compacto $K \subset \mathbb{R}^n$.*
2) Um subgrupo discreto $H \subset \mathbb{R}^n$ gerado como um $\mathbb{Z}$-módulo por n vetores linearmente independente sobre $\mathbb{R}$ é chamado um reticulado do $\mathbb{R}^n$.
3) Fazendo $v_i = (v_{i1}, \cdots, v_{in}) \in \mathbb{R}^n$, para $i = 1, \cdots, m$, a matriz

$$M = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{pmatrix}$$

é chamada matriz geradora do reticulado. A matriz $G = MM^t$ é chamada matriz de Gram do reticulado, onde t denota a transposta da matriz t.
4) Se $\{e_1, \cdots, e_n\}$ é uma base de um reticulado de H, definimos

$$P_e = \left\{ x \in R^n : x = \sum_{i=1}^{n} \lambda_i e_i, 0 \leq \lambda_i < 1 \right\}$$

como região fundamental de H.
5) O volume da região fundamental é o módulo do determinante da matriz G. O volume da região fundamental, independe da base, pois a matriz mudança de base é invertível, com entradas inteiras. Assim, o volume do reticulado é definido como sendo o volume de uma região fundamental.

Lema 2.6.1 *O conjunto dos pontos de um reticulado H no $\mathbb{R}^n$ é discreto.*

Demonstração: Consideremos uma base $\{e_1, \cdots, e_n\}$ do reticulado H. Temos que $< x, e_2 >= 0, ..., < x, e_n >= 0$ fornece um sistema de $n-1$ equações lineares homogêneas em n incógnitas. Como cada sistema tem uma solução não nula, segue que existe um vetor x ortogonal aos vetores $e_2, ..., e_n$. Se $< x, e_1 >= 0$, então o vetor x poderia ser ortogonal a todos os vetores do $\mathbb{R}^n$, o que é impossível. Assim, $< x, e_1 > \neq 0$. O vetor $f_1 = [1/ < x, e_1 >]/x$ pode ser ortogonal a todos os vetores $e_2, ..., e_n$, e $< f_1, e_1 >= 1$. Desta maneira, para todo $1 \leq i \leq n$, podemos escolher um vetor f_i, tal que $< f_i, e_i >= 1$ e $< f_j, e_i >= 0$, para $j \neq i$. Agora, seja que o vetor

$z = a_1 z_1 + \cdots + a_n z_n$ de H pertence a uma bola $U(r)$, isto é, $||z|| < r$. Como $a_k =< z, f_k >$, pela inequação de Cauchy-Schwartz temos,

$$||a_k|| = || < z, f_k > || \leq ||z||||f_k|| < r||f_k||,$$

onde $r||f_k||$ não depende de z. Assim, existe um número finito de possibilidades para a_k e o conjunto de todos $z \in H$ para $||z|| < r$ é finito. ■

Exemplos de Reticulados importantes

Reticulado n-dimensional A_n: Para todo $n \geq 1$, $A_n = \{(x_0, x_1, \ldots, x_n) \in \mathbb{Z}^{n+1};\ x_0 + x_1 + \cdots + x_n = 0\}$ é um reticulado. Por definição, temos que A_n está contido no hiperplano $\sum_i x_i = 0$ no $\mathbb{R}^{n+1}$, possui uma matriz geradora B, dada por:

$$B = \begin{bmatrix} -1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & -1 & 1 & \cdots & 0 & 0 \\ . & . & . & . & \cdots & . & . \\ 0 & 0 & 0 & 0 & \cdots & -1 & 1 \end{bmatrix},$$

onde $detA_n = det(BB^t) = n + 1$.

Reticulado D_n, para $n \geq 3$: Temos que $D_n = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : x_1 + \cdots + x_n \text{ é par}\}$ é um reticulado. Sua matriz geradora é dada por;

$$B = \begin{bmatrix} -1 & -1 & 0 & \cdots & 0 & 0 \\ 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & \cdots & 0 & 0 \\ . & . & . & \cdots & . & . \\ 0 & 0 & 0 & \cdots & 1 & -1 \end{bmatrix}$$

onde $detD_n = 4$.

Reticulado 8-dimensional E_8: Temos que o sistema de coordenadas pares de E_8 consiste dos pontos $\{(x_1, \cdots, x_8) : \forall\, x_i \in \mathbb{Z} \text{ ou } \forall\, x_i \in \mathbb{Z} + \frac{1}{2}, \sum x_i \equiv 0 (modulo 2)\}$. O sistema de coordenadas ímpares é obtido mudando o sinal de qualquer coordenada: os pontos são $\{(x_1, \cdots, x_8) : \forall\, x_i \in \mathbb{Z} \text{ ou } \forall\, x_i \in \mathbb{Z} + \frac{1}{2}, \sum x_i \equiv 2x_8 (mod 2)\}$. A matriz geradora de E_8 é dada por

$$B = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{bmatrix},$$

e $detB = 1$.

Reticulado 6-dimensional E_6: Os vetores em E_8 perpendiculares a qualquer A_2 subreticulado V em E_8 formam o reticulado E_6, isto é, $E_6 = \{x \in E_8 : x \cdot v = 0, \forall\, v \in V\}$. A matriz geradora de E_6 é dada por

$$B = \begin{bmatrix} 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{bmatrix},$$

e o seu determinante é $detB = 3$.

Teorema 2.6.1 *Sejam $H \subset \mathbb{R}^n$ um reticulado e $S \subset \mathbb{R}^n$ um subconjunto integrável tal que $v(S) > v(H)$. Então existem $x, y \in S$, $x \neq y$ tal que $x - y \in H$.*

Demonstração: Sejam $v = \{v_1, \cdots, v_n\}$ uma $\mathbb{Z}$-base de H e P_v a sua região fundamental. Assim, $S = \dot{\bigcup}_{h \in H} S \cap (h + P_v)$ é uma união disjunta. Como o volume é invariante por translação, temos que

$$v(S) = \sum_{h \in H} v(S \cap (h + P_v)) = \sum_{h \in H} v((-h + S) \cap P_v).$$

Os conjuntos $(-h + S) \cap P_v$, $h \in H$, não podem ser disjuntos, pois caso contrário, teríamos que $v(P_v) = v(H) \geq \sum_{h \in H} v((-h + S) \cap P_v) = v(S)$, o que é contra hipótese. Portanto, existem $h_1, h_2 \in H$, tais que

$$((-h_1 + S) \cap P_e) \cap ((-h_2 + S) \cap P_e) \neq \emptyset.$$

Logo, existem $x, y \in S$ tais que $x - h_1 = y - h_2$. Portanto, $x - y = h_1 - h_2 \in H$. ∎

Teorema 2.6.2 *Sejam H um reticulado no $\mathbb{R}^n$ e $S \subset \mathbb{R}^n$ um subconjunto integrável convexo e simétrico em relação a origem. Se $v(S) > v(H)2^n$ então $S \cap (H - \{0\}) \neq \emptyset$.*

Demonstração: Como $v\left(\frac{1}{2}S\right) = 2^{-n}v(S) > v(H)$, segue do Teorema 2.6.1 que os conjuntos $\frac{1}{2}S + z$ não são disjuntas dois a dois, isto é, existem $z_1, z_2 \in H$, $z_1 \neq z_2$ e $c_1, c_2 \in S$, tais que $\frac{1}{2}c_1 + z_1 = \frac{1}{2}c_2 + z_2$. Como S é simétrico e convexo, temos que

$$-c_1 \in S \text{ e } z_1 - z_2 = \frac{1}{2}c_2 + (1 - \frac{1}{2})c_1 \in S \cap (H - \{0\}).$$ ∎

Teorema 2.6.3 *Sejam H um reticulado no $\mathbb{R}^n$, $S \subset \mathbb{R}^n$ um subconjunto integrável convexo e simétrico em relação a origem. Se $v(S) \geq v(H)2^n$ e S é compacto, então $S \cap (H - \{0\}) \neq \emptyset$.*

Demonstração: Seja o conjunto $(1 + \epsilon)S$, para $\epsilon > 0$. Então $(1 + \epsilon)S$ é compacto, convexo e simétrico, e $v((1 + \epsilon)S) > 2^n v(H)$. Pelo Teorema 2.6.2, segue que $(1 + \epsilon)S \cap H - \{0\} \neq \emptyset$. Como H é discreto segue que $(1+\epsilon)S \cap H - \{0\}$ é finito, e portanto, é compacto. Agora, temos que se $\epsilon_1 < \epsilon_2$, então $(1 + \epsilon_1)S \subset (1 + \epsilon_2)S$, uma vez que se $(1 + \epsilon_1)x \in (1 + \epsilon_1)S$, com $x \in S$, então $(1 + \epsilon_1)x = (1 + \epsilon_2)y \in S$, com $y \in S$ se, e somente se, $y = \left(\frac{1 + \epsilon_1}{1 + \epsilon_2}\right) x$, ou seja, $y = rx$, para algum $0 < r < 1$. Assim, é suficiente mostrar que $rx \in S$. Como S é convexo, temos que, $(1 - t)(-x) + tx \in S$, com $0 \leq t \leq 1$. Em particular, se $t = \frac{r + 1}{2} < 1$, temos

$$\left(1 - \frac{r + 1}{2}\right)(-x) + \frac{r + 1}{2}x = rx \in S.$$

Assim, concluímos que $(1 + \epsilon_1)S \subset (1 + \epsilon_2)S$, para todo $\epsilon_2 > \epsilon_1$. Pelo Teorema dos Intervalos Encaixantes, segue que $\bigcap_{\epsilon>0}((1+\epsilon)S) \cap (H - \{0\}) \neq \emptyset$. Assim, existe $x \in H - \{0\}$ e $x \in (1+\epsilon)S$, para todo $\epsilon > 0$. Finalmente, temos que $(x_n) = \left(\frac{x}{1 + \frac{1}{n}}\right)$ é uma sequência convergente de S, e como S é compacto, segue que (x_n) converge para $x \in S$. Portanto, $S \cap H - \{0\} \neq \emptyset$. ∎

2.7 Reticulados via corpos de números

Nesta seção apresentamos uma maneira de obtermos reticulados através da Teoria Algébricas dos Números, através da imersão de um corpo de números $\mathbb{K}$ no $\mathbb{R}^n$, de modo que a imagem de ideais no anel dos inteiros $\mathcal{O}_{\mathbb{K}}$, correspondam a reticulados neste espaço.

Recordamos que dada uma extensão $\mathbb{K}$ de $\mathbb{Q}$ de grau n existem n monomorfismos distintos $\sigma_j : \mathbb{K} \longrightarrow \mathbb{C}$, uma vez que o polinômio minimal de um elemento primitivo de $\mathbb{K}$ sobre $\mathbb{Q}$ tem somente n raízes em $\mathbb{C}$. Se $\sigma_j(\mathbb{K}) \subset \mathbb{R}$, dizemos que σ_j é real, e caso contrário, dizemos que σ_j é imaginário. Quando todos os monomorfismos são reais dizemos que $\mathbb{K}$ é um corpo totalmente real e quando são todos imaginários dizemos que $\mathbb{K}$ é um corpo totalmente imaginário. Se $\alpha : \mathbb{C} \longrightarrow \mathbb{C}$ é a conjugação complexa, então para todo $j = 1, \cdots, n$, temos que $\alpha \circ \sigma_j = \sigma_k$, com $1 \leq k \leq n$, e que $\sigma_k = \sigma_j$ se, e somente se, $\sigma_j(\mathbb{K}) \subset \mathbb{R}$. Assim, usando r_1 para denotar o número de índices tal que $\sigma_j(K) \subset \mathbb{R}$, podemos ordenar os monomorfismos $\sigma_1, \cdots, \sigma_n$ de tal modo que $\sigma_1, \cdots, \sigma_{r_1}$ sejam os monomorfismos reais e $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$, para $j = 1, \cdots, r_2$, são os monomorfismos imaginários. Então $n - r_1$ é um número par, e assim podemos escrever $r_1 + 2r_2 = n$. Para cada $x \in \mathbb{K}$, temos que o homomorfismo $\sigma_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{R}^n$ definido por

$$\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \cdots, \sigma_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$$

é um homomorfismo injetivo de anéis, chamado homomorfismo canônico de $\mathbb{K}$ em $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$. Geralmente identificamos $\mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$ com $\mathbb{R}^n$, e este homomorfismo pode também ser visto como

$$\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \cdots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_2+1}(x), \cdots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)),$$

onde $\Re(x)$ representa a parte real e $\Im(x)$ representa a parte imaginária de x.

Proposição 2.7.1 *Seja $\mathbb{K}$ um corpo de números de grau n. Se $\mathbb{M} \subset \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n, com base $\{\alpha_1, \cdots, \alpha_n\}$, então $\sigma(M) \subset \mathbb{R}^n$ é um reticulado, com volume*

$$v(\sigma(M)) = 2^{-r_2} |\det(\sigma_i(\alpha_j))|.$$

Demonstração: Para cada j fixo, as coordenadas de $\sigma(\alpha_j)$ com respeito a base canônica do $\mathbb{R}^n$ são dadas por

$$(\sigma_1(\alpha_j), \sigma_2(\alpha_j), \cdots, \sigma_{r_1}(\alpha_j), \Re\sigma_{r_1+1}(\alpha_j), \Im\sigma_{r_1+1}(\alpha_j), \cdots, \Re\sigma_{r_1+r_2}(\alpha_j), \Im\sigma_{r_1+r_2}(\alpha_j)). \quad (2.7)$$

Agora calculemos o determinante D da matriz que tem a j-ésima coluna dada pela equação (2.7), fazendo uso das seguintes fórmulas $\Re(z) = \frac{1}{2}(z + \bar{z})$, $\Im(z) = \frac{1}{2i}(z - \bar{z})$ para $z \in \mathbb{C}$ e das transformações elementares no determinante, a saber, pela adição da $(r_1 + 2l)-$ésima linha a sua anterior e em seguida pela subtração da $(r_1 + 2l - 1)-$ésima coluna da sua posterior, para

$l = 1, \cdots, r_2$. A matriz geradora G do reticulado é dada por

$$D = \begin{vmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_j) & \dots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \dots & \sigma_2(\alpha_j) & \dots & \sigma_2(\alpha_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(\alpha_1) & \dots & \sigma_{r_1}(\alpha_j) & \dots & \sigma_{r_1}(\alpha_n) \\ \Re(\sigma_{r_1+1}(\alpha_1)) & \dots & \Re(\sigma_{r_1+1}(\alpha_j)) & \dots & \Re(\sigma_{r_1+1}(\alpha_n)) \\ \Im(\sigma_{r_1+1}(\alpha_1)) & \dots & \Im(\sigma_{r_1+1}(\alpha_j)) & \dots & \Im(\sigma_{r_1+1}(\alpha_n)) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \Re(\sigma_{r_1+r_2}(\alpha_1)) & \dots & \Re(\sigma_{r_1+r_2}(\alpha_j)) & \dots & \Re(\sigma_{r_1+r_2}(\alpha_n)) \\ \Im(\sigma_{r_1+r_2}(\alpha_1)) & \dots & \Im(\sigma_{r_1+r_2}(\alpha_j)) & \dots & \Im(\sigma_{r_1+r_2}(\alpha_n)) \end{vmatrix} = \left(\frac{1}{2}\right)^{r_2} \left(\frac{1}{2i}\right)^{r_2}.$$

$$\begin{vmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_j) & \dots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \dots & \sigma_2(\alpha_j) & \dots & \sigma_2(\alpha_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(\alpha_1) & \dots & \sigma_{r_1}(\alpha_j) & \dots & \sigma_{r_1}(\alpha_n) \\ \sigma_{r_1+1}(\alpha_1) + \overline{\sigma_{r_1+1}(\alpha_1)} & \dots & \sigma_{r_1+1}(\alpha_j) + \overline{\sigma_{r_1+1}(\alpha_j)} & \dots & \sigma_{r_1+1}(\alpha_n) + \overline{\sigma_{r_1+1}(\alpha_n)} \\ \sigma_{r_1+1}(\alpha_1) - \overline{\sigma_{r_1+1}(\alpha_1)} & \dots & \sigma_{r_1+1}(\alpha_j) - \overline{\sigma_{r_1+1}(\alpha_j)} & \dots & \sigma_{r_1+1}(\alpha_n) - \overline{\sigma_{r_1+1}(\alpha_n)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(\alpha_1) + \overline{\sigma_{r_1+r_2}(\alpha_1)} & \dots & \sigma_{r_1+r_2}(\alpha_j) + \overline{\sigma_{r_1+r_2}(\alpha_j)} & \dots & \sigma_{r_1+r_2}(\alpha_n) + \overline{\sigma_{r_1+r_2}(\alpha_n)} \\ \sigma_{r_1+r_2}(\alpha_1) - \overline{\sigma_{r_1+r_2}(\alpha_1)} & \dots & \sigma_{r_1+r_2}(\alpha_j) - \overline{\sigma_{r_1+r_2}(\alpha_j)} & \dots & \sigma_{r_1+r_2}(\alpha_n) - \overline{\sigma_{r_1+r_2}(\alpha_n)} \end{vmatrix} = \left(\frac{1}{2}\right)^{r_2}.$$

$$\left(\frac{1}{2i}\right)^{r_2} 2^{r_2} \begin{vmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_j) & \dots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \dots & \sigma_2(\alpha_j) & \dots & \sigma_2(\alpha_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(\alpha_1) & \dots & \sigma_{r_1}(\alpha_j) & \dots & \sigma_{r_1}(\alpha_n) \\ \sigma_{r_1+1}(\alpha_1) + \overline{\sigma_{r_1+1}(\alpha_1)} & \dots & \sigma_{r_1+1}(\alpha_j) + \overline{\sigma_{r_1+1}(\alpha_j)} & \dots & \sigma_{r_1+1}(\alpha_n) + \overline{\sigma_{r_1+1}(\alpha_n)} \\ \sigma_{r_1+1}(\alpha_1) - \overline{\sigma_{r_1+1}(\alpha_1)} & \dots & \sigma_{r_1+1}(\alpha_j) - \overline{\sigma_{r_1+1}(\alpha_j)} & \dots & \sigma_{r_1+1}(\alpha_n) - \overline{\sigma_{r_1+1}(\alpha_n)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(\alpha_1) + \overline{\sigma_{r_1+r_2}(\alpha_1)} & \dots & \sigma_{r_1+r_2}(\alpha_j) + \overline{\sigma_{r_1+r_2}(\alpha_j)} & \dots & \sigma_{r_1+r_2}(\alpha_n) + \overline{\sigma_{r_1+r_2}(\alpha_n)} \\ \sigma_{r_1+r_2}(\alpha_1) - \overline{\sigma_{r_1+r_2}(\alpha_1)} & \dots & \sigma_{r_1+r_2}(\alpha_j) - \overline{\sigma_{r_1+r_2}(\alpha_j)} & \dots & \sigma_{r_1+r_2}(\alpha_n) - \overline{\sigma_{r_1+r_2}(\alpha_n)} \end{vmatrix} =$$

$$(-1)^{r_2}\left(\frac{1}{2}\right)^{\frac{r_2}{2}}\left(\frac{1}{2i}\right)^{r_2}2^{r_2}\begin{vmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_j) & \dots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \dots & \sigma_2(\alpha_j) & \dots & \sigma_2(\alpha_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(\alpha_1) & \dots & \sigma_{r_1}(\alpha_j) & \dots & \sigma_{r_1}(\alpha_n) \\ \sigma_{r_1+1}(\alpha_1) & \dots & \sigma_{r_1+1}(\alpha_j) & \dots & \sigma_{r_1+1}(\alpha_n) \\ \overline{\sigma_{r_1+1}(\alpha_1)} & \dots & \overline{\sigma_{r_1+1}(\alpha_j)} & \dots & \overline{\sigma_{r_1+1}(\alpha_n)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(\alpha_1) & \dots & \sigma_{r_1+r_2}(\alpha_j) & \dots & \sigma_{r_1+r_2}(\alpha_n) \\ \overline{\sigma_{r_1+r_2}(\alpha_1)} & \dots & \overline{\sigma_{r_1+r_2}(\alpha_j)} & \dots & \overline{\sigma_{r_1+r_2}(\alpha_n)} \end{vmatrix} =$$

$$\left(\frac{1}{2i}\right)^{r_2}\begin{vmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_j) & \dots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \dots & \sigma_2(\alpha_j) & \dots & \sigma_2(\alpha_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(\alpha_1) & \dots & \sigma_{r_1}(\alpha_j) & \dots & \sigma_{r_1}(\alpha_n) \\ \sigma_{r_1+1}(\alpha_1) & \dots & \sigma_{r_1+1}(\alpha_j) & \dots & \sigma_{r_1+1}(\alpha_n) \\ \sigma_{r_1+2}(\alpha_1) & \dots & \sigma_{r_1+2}(\alpha_j) & \dots & \sigma_{r_1+2}(\alpha_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+2r_2}(\alpha_1) & \dots & \sigma_{r_1+2r_2}(\alpha_j) & \dots & \sigma_{r_1+2r_2}(\alpha_n) \end{vmatrix} = (2i)^{-r_2}\det(\sigma_j(\alpha_k)).$$

Portanto, $D = (2i)^{-r_2}\det(\sigma_j(\alpha_i))$, $j, i = 1, \cdots, n$. Como $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, segue da Proposição 2.3.5 que $\det(\sigma_j(\alpha_i)) \neq 0$, e portanto, $D \neq 0$. Assim, os vetores $\sigma(\alpha_j)$ do $\mathbb{R}^n$ são linearmente independente e geram $\sigma(M)$, ou seja, $\sigma(M)$ é um reticulado do $\mathbb{R}^n$. Do fato de $\{\alpha_1, \cdots, \alpha_n\}$ ser uma $\mathbb{Z}$-base de M, segue que $m = \sum_{j=1}^{n} a_j\alpha_j$, $a_j \in \mathbb{Z}$, e portanto, $m \in M$. Assim, $\sigma(m) = \sum_{j=1}^{n} a_j\sigma(\alpha_j)$, $a_j \in \mathbb{Z}$, ou seja, $\sigma(M) = \left\{\sum_{j=1}^{n} a_j\sigma(\alpha_j); a_j \in \mathbb{Z}\right\}$. Logo, $v(\sigma(M)) = |D| = 2^{-r_2}|\det(\sigma_i(\alpha_j))|$. ■

Exemplo 2.7.1 *Sejam $\mathbb{K} = \mathbb{Q}[\sqrt{7}]$ e $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\sqrt{7}]$ seu anel dos inteiros com $\mathbb{Z}-$base $\{1, \sqrt{7}\}$. Como $\mathbb{K}$ é totalmente real então $r_2 = 0$, e portanto*

$$v(\sigma(\mathcal{O}_\mathbb{K})) = \left|\det\begin{pmatrix} 1 & \sqrt{7} \\ 1 & -\sqrt{7} \end{pmatrix}\right| = 2\sqrt{7}.$$

A imagem do homomorfismo canônico $\sigma(\mathbb{Z}[\sqrt{7}]) \subseteq \mathbb{R}^2$ é um reticulado de posto 2 em $\mathbb{R}^2$ cujo volume é $2\sqrt{7}$.

Proposição 2.7.2 *Sejam $\delta_{\mathbb{K}|\mathbb{Q}}$ o discriminante absoluto de $\mathbb{K}$, $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros em $\mathbb{K}$, e $\mathcal{I}$ um ideal de $\mathcal{O}_{\mathbb{K}}$. Então, $\sigma(\mathcal{O}_{\mathbb{K}})$ e $\sigma(\mathcal{I})$ são reticulados, e*

$$v(\sigma(\mathcal{O}_{\mathbb{K}})) = 2^{-r_2}|\delta_{\mathbb{K}|\mathbb{Q}}|^{\frac{1}{2}} \text{ e } v(\sigma(\mathcal{I})) = 2^{-r_2}|\delta_{\mathbb{K}|\mathbb{Q}}|^{\frac{1}{2}}N(\mathcal{I}).$$

Demonstração: Pelo Corolário 1.2.3, temos que $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n e pelo Corolário 1.2.4, segue que $\mathcal{I}$ é um $\mathbb{Z}$-módulo livre de posto n. Segue da Proposição 2.7.1 que $\sigma(\mathcal{O}_{\mathbb{K}})$ e $\sigma(\mathcal{I})$ são reticulados. Se $\{\alpha_1, \cdots, \alpha_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$, então $\delta_{\mathbb{K}|\mathbb{Q}} = \det(\sigma_i(\alpha_j))^2$, ou seja, $|\delta_{\mathbb{K}|\mathbb{Q}}|^{\frac{1}{2}} = \det(\sigma_i(\alpha_j))$. Assim, pela Proposição 2.7.1, segue que $v(\sigma(\mathcal{O}_{\mathbb{K}})) = 2^{-r_2}|\delta_{\mathbb{K}|\mathbb{Q}}|^{\frac{1}{2}}$. Para a segunda fórmula, temos que $N(\mathcal{I}) = \#\mathcal{O}_{\mathbb{K}}/\mathcal{I} = \#\sigma(\mathcal{O}_{\mathbb{K}})/\sigma(\mathcal{I})$, pois $\sigma(\mathcal{I}) \subset \sigma(\mathcal{O}_{\mathbb{K}})$ é um subgrupo com índice $N(\mathcal{I})$. Como um domínio fundamental de $\sigma(\mathcal{I})$ é a união disjunta de $N(\mathcal{I})$ cópias de um domínio fundamental de $\sigma(\mathcal{O}_{\mathbb{K}})$, segue que $v(\sigma(\mathcal{I})) = 2^{-r_2}|\delta_{\mathbb{K}|\mathbb{Q}}|^{\frac{1}{2}}N(\mathcal{I})$. ∎

Observação 2.7.1 *A matriz geradora do reticulado $\sigma(\mathcal{I})$ é dada da seguinte maneita*

$$G_{\mathcal{I}} = \begin{vmatrix} \sigma_1(\gamma_1) & \cdots & \sigma_{r_1}(\gamma_1) & \Re\sigma_{r_1+1}(\gamma_1) & \Im\sigma_{r_1+1}(\gamma_1) & \cdots & \Re\sigma_{r_1+r_2}(\gamma_1) & \Im\sigma_{r_1+r_2}(\gamma_1) \\ \sigma_1(\gamma_2) & \cdots & \sigma_{r_1}(\gamma_2) & \Re\sigma_{r_1+1}(\gamma_2) & \Im\sigma_{r_1+1}(\gamma_2) & \cdots & \Re\sigma_{r_1+r_2}(\gamma_2) & \Im\sigma_{r_1+r_2}(\gamma_2) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(\gamma_n) & \cdots & \sigma_{r_1}(\gamma_n) & \Re\sigma_{r_1+1}(\gamma_n) & \Im\sigma_{r_1+1}(\gamma_n) & \cdots & \Re\sigma_{r_1+r_2}(\gamma_n) & \Im\sigma_{r_1+r_2}(\gamma_n) \end{vmatrix},$$

e pode ser obtida da matriz geradora G via a matriz mudança de base entre as $\mathbb{Z}-$bases de $\mathcal{I}$ e $\mathcal{O}_{\mathbb{K}}$. Assim, $G_{\mathcal{I}} = TG$.

Corolário 2.7.1 *Se Λ é um subreticulado do $\mathbb{Z}^n$ então $v(\Lambda) = o(\mathbb{Z}^n/\Lambda)$.* ∎

Proposição 2.7.3 *Sejam $\mathbb{Q} \subseteq \mathbb{K}$ uma extensão de grau n, r_1 e r_2 como definidos anteriormente, $\delta_{\mathbb{K}|\mathbb{Q}}$ o discriminante absoluto de $\mathbb{K}$ e $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$, um ideal não nulo, onde $\mathcal{O}_{\mathbb{K}}$ é o anel dos inteiros de $\mathbb{K}$. Então existe $x \subset \mathcal{I}, x \neq 0$ tal que $|N(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}|\delta_{\mathbb{K}|\mathbb{Q}}|^{\frac{1}{2}}N(\mathcal{I})$.*

Demonstração: Seja $\sigma : \mathbb{K} \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ o homomorfismo canônico. Seja

$$B_t = \left\{(y_1, \cdots, y_{r_1}, z_1, \cdots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}; \sum_{i=1}^{r_1}|y_i| + 2\sum_{j=1}^{r_2}|z_j| \leq t\right\},$$

onde $t \in \mathbb{R}$, e $t > 0$. Como B_t é fechado e limitado, segue que B_t é compacto. Além disso, B_t é simetrico em relação a origem do $\mathbb{R}^n$ e convexo, uma vez que se $x, y \in B_t$, tal que $x = (y_1, \cdots, y_{r_1}, z_1, \cdots, z_{r_2})$, $y = (y_1', \cdots, y_{r_1}', z_1', \cdots, z_{r_2}')$ e $0 \leq \alpha \leq 1$, temos que

$$\sum_{i=1}^{r_1}|y_i| + 2\sum_{j=1}^{r_2}|z_j| \leq t \text{ e } \sum_{i=1}^{r_1}|y_i'| + 2\sum_{j=1}^{r_2}|z_j'| \leq t.$$

Então,

$\alpha x + (1-\alpha)y = \alpha(y_1, \cdots, y_{r_1}, z_1, \cdots, z_{r_2}) + (1-\alpha)(y_1', \cdots, y_{r_1}', z_1', \cdots, z_{r_2}')$
$= (\alpha y_1 + (1-\alpha)y_1', \alpha y_2 + (1-\alpha)y_2', \cdots, \alpha y_{r_1} + (1-\alpha)y_{r_1}', \alpha z_1 + (1-\alpha)z_1', \cdots, \alpha z_{r_2} + (1-\alpha)z_{r_2}')$

e que

$$\sum_{i=1}^{r_1} |\alpha y_i + (1-\alpha)y_i'| + 2\sum_{j=1}^{r_2} |\alpha z_j + (1-\alpha)z_j'|$$
$$\leq \alpha \sum_{i=1}^{r_1} |y_i'| + (1-\alpha)\sum_{j=1}^{r_1} |y_i'| + 2\alpha \sum_{j=1}^{r_2} |z_j| + 2(1-\alpha)\sum_{j=1}^{r_2} |z_j'|$$
$$= \alpha\left(\sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} |z_j|\right) + (1-\alpha)\left(\sum_{i=1}^{r_2} |y_i'| + 2\sum_{j=1}^{r_2} |z_j'|\right) \leq \alpha t + (1-\alpha)t = t,$$

ou seja, $\alpha x + (1-\alpha)y \in B_t$. Também, $v(B_t) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^n}{n!}$. Agora, escolhemos t de maneira que

$$v(B_t) = 2^n v(\sigma(\mathcal{I})).$$

Assim, $2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^n}{n!} = 2^{n-r_2}|\delta_{\mathbb{K}|\mathbb{Q}}|^{\frac{1}{2}}N(\mathcal{I})$ e então $t^n = 2^{n-r_1}\pi^{-r_2}n!|\delta_{\mathbb{K}|\mathbb{Q}}|^{\frac{1}{2}}N(\mathcal{I})$. Pelo Teorema 2.6.3, existe $y \in B_t \cap \sigma(\mathcal{I})$, $y \neq 0$, ou seja, existe $x \in \mathcal{I} - \{0\}$ tal que $y = \sigma(x) \in B_t$. Como, $N(x) = \prod_{i=1}^{n}\sigma_i(x) = \prod_{i=1}^{r_1}\sigma_i(x)\prod_{i=1}^{r_1+r_2}|\sigma_i(x)|^2$, pois $|\sigma_i(x)|^2 = \sigma_i(x)\bar{\sigma}_i(x)$, temos que

$$N(x) = \prod_{i=1}^{r_1}\sigma_i(x)\prod_{i=1}^{r_1+r_2}|\sigma_i(x)|^2 \leq \left[\frac{1}{n}\sum_{i=1}^{r_1}|\sigma_i(x)|^n + \frac{2}{n}\sum_{i=r_1+1}^{r_1+r_2}|\sigma_i(x)|^n\right] \leq \frac{1}{n^n}t^n,$$

uma vez que $\sigma(x) \in B_t$. Portanto,

$$|N(x)| \leq \frac{1}{n^n}2^{n-r_1}\pi^{-r_2}n!|\delta_{\mathbb{K}|\mathbb{Q}}|^{\frac{1}{2}}N(\mathcal{I}) = 2^{2r_2}\pi^{-r_2}\frac{n!}{n^n}|\delta_{\mathbb{K}|\mathbb{Q}}|^{\frac{1}{2}}N(\mathcal{I}) = \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|\delta_{\mathbb{K}|\mathbb{Q}}|^{\frac{1}{2}}N(\mathcal{I}). \quad \blacksquare$$

Corolário 2.7.2 *Com as hipóteses da Proposição* 2.7.3*, temos que toda classe de ideais de* $\mathbb{K}$ *contém um ideal inteiro* $\mathcal{B}$ *tal que* $|N(\mathcal{B})| \leq \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|\delta_{\mathbb{K}|\mathbb{Q}}|^{\frac{1}{2}}$.

Demonstração: Seja $\mathcal{E}$ uma classe de ideais de $\mathbb{K}$. Seja $\mathcal{I}_0 \subset \mathcal{E}$ um ideal fracionário. Pelo Teorema 1.6.2, existe $\mathcal{I}_0^{-1}$ ideal fracionário tal que $\mathcal{I}_0\mathcal{I}_0^{-1} = \mathcal{O}_{\mathbb{K}}$. Assim, existe $d \in \mathcal{O}_{\mathbb{K}}$, $d \neq 0$, tal que $d\mathcal{I}_0^{-1} \subset \mathcal{O}_{\mathbb{K}}$ é um ideal inteiro e que $\mathcal{O}_{\mathbb{K}} = (d^{-1}\mathcal{I}_0)(d\mathcal{I}_0^{-1})$. Se $\mathcal{G} = d^{-1}\mathcal{I}_0$, então, $\mathcal{I} = \mathcal{G}^{-1} = (d^{-1}\mathcal{I}_0)^{-1} = d\mathcal{I}_0^{-1}$ é um ideal inteiro e $\mathcal{G} \subset \mathcal{E}$. Pela Proposição 2.7.3, existe $x \in \mathcal{G}$, $x \neq 0$, tal que

$$|N(x)| = N(\mathcal{O}_{\mathbb{K}}x) \leq \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|\delta_{\mathbb{K}|\mathbb{Q}}|^{\frac{1}{2}}N(\mathcal{I}).$$

Assim $\frac{N(Ax)}{N(\mathcal{I})} \leq \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|\delta_{\mathbb{K}|\mathbb{Q}}|^{\frac{1}{2}}$. Como $N(\mathcal{O}_{\mathbb{K}}x) = N(\mathcal{O}_{\mathbb{K}}x\mathcal{I}^{-1}\mathcal{I}) = N(\mathcal{O}_{\mathbb{K}}x\mathcal{I}^{-1})N(\mathcal{I})$, segue que

$$\frac{N(\mathcal{O}_{\mathbb{K}}x)}{N(\mathcal{I})} = N(\mathcal{O}_{\mathbb{K}}x\mathcal{I}^{-1}).$$

Falta mostrar que $\mathcal{B} = \mathcal{O}_{\mathbb{K}} x \mathcal{I}^{-1} = \mathcal{O}_{\mathbb{K}} x \mathcal{G}$ é um ideal inteiro. Temos que $\mathcal{B} \subset \mathcal{E}$, pois é um produto de um ideal principal por $\mathcal{G}$ e que $\mathcal{O}_{\mathbb{K}} x \subseteq \mathcal{I}$ se, e somente se, $\mathcal{I}$ divide $\mathcal{O}_{\mathbb{K}} x$ se, e somente se, existe $\mathcal{B}$ ideal inteiro tal que $\mathcal{O}_{\mathbb{K}} x = \mathcal{I}\mathcal{B}$. Portanto, $\mathcal{O}_{\mathbb{K}} x \mathcal{I}^{-1} = \mathcal{B}$ é ideal inteiro. ■

Corolário 2.7.3 *Com as mesmas hípóteses da Proposição 2.7.3, temos que*

$$|\delta_{\mathbb{K}|\mathbb{Q}}| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$$

e $\dfrac{n}{log(|\delta_{\mathbb{K}|\mathbb{Q}}|)}$ *é limitado por uma constante de* $\mathbb{R}$.

Demonstração: Pelo Corolário 2.7.2 existe $\mathcal{B}$ um ideal não nulo inteiro tal que

$$1 \leq N(\mathcal{B}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |\delta_{\mathbb{K}|\mathbb{Q}}|^{\frac{1}{2}}.$$

Assim, $|\delta_{\mathbb{K}|\mathbb{Q}}|^{\frac{1}{2}} \geq \left(\frac{\pi}{4}\right)^{r_2} \frac{n^n}{n!}$ e portanto, $|\delta_{\mathbb{K}|\mathbb{Q}}| \geq \left(\frac{\pi}{4}\right)^{2r_2} \frac{n^{2n}}{(n!)^2}$. Como $\frac{\pi}{4} < 1$ e $2r_2 < n$ temos que $|\delta_{\mathbb{K}|\mathbb{Q}}| \geq \left(\frac{\pi}{4}\right)^{n} \frac{n^{2n}}{(n!)^2}$. Se $a_n = \left(\frac{\pi}{4}\right)^{n} \frac{n^{2n}}{(n!)^2}$, então

$$\begin{aligned} \frac{a_{n+1}}{a_n} &= \frac{\left(\frac{\pi}{4}\right)^{n+1} \frac{(n+1)^{2(n+1)}}{((n+1)!)^2}}{\left(\frac{\pi}{4}\right)^{n} \frac{n^{2n}}{(n!)^2}} = \left(\frac{\pi}{4}\right) \frac{(n+1)^{2(n+1)}}{(n)^{2n}} \cdot \frac{1}{(n+1)^2} \\ &= \frac{\pi}{4}\left(\frac{n+1}{n}\right)^{2n} = \frac{\pi}{4}\left(1+\frac{1}{n}\right)^{2n} = \frac{\pi}{4}(1+2+\textit{termos positivos}) \geq \frac{3\pi}{4}. \end{aligned}$$

Assim, $a_n = \frac{a_n}{a_{n-1}} \cdot \frac{a_{n-1}}{a_{n-2}} \cdots \frac{a_3}{a_2} \cdot a_2 \geq \frac{3\pi}{4}^{n-2} \frac{\pi^2}{4} = \frac{3\pi}{4}^{n-2} \frac{3\pi}{4} \frac{\pi}{3} = \frac{3\pi}{4}^{n-1} \frac{\pi}{3}$. Logo, $|\delta_{\mathbb{K}|\mathbb{Q}}| \geq \frac{3\pi}{4}^{n-1} \frac{\pi}{3}$. Agora, temos que $|\delta_{\mathbb{K}|\mathbb{Q}}| \geq \left(\frac{3\pi}{4}\right)^{n} \left(\frac{4}{3\pi}\right) \left(\frac{\pi}{3}\right) = \left(\frac{3\pi}{4}\right)^{n} \frac{4}{9}$. Como

$$\frac{4}{9} = \left(\frac{2}{3}\right)^2 \geq \left(\frac{2}{3}\right)^n,$$

segue que $|\delta_{\mathbb{K}|\mathbb{Q}}| \geq \left(\frac{3\pi}{4}\right)^{n} \left(\frac{2}{3}\right)^{n} = \left(\frac{3\pi}{4} \cdot \frac{2}{3}\right)^{n} = \left(\frac{\pi}{2}\right)^{n}$. Portanto, $\log |\delta_{\mathbb{K}|\mathbb{Q}}| \geq \log \frac{\pi}{2}$, ou seja, $\dfrac{n}{\log |\delta_{\mathbb{K}|\mathbb{Q}}|} \leq \dfrac{1}{\log \frac{\pi}{2}}$. ■

Teorema 2.7.1 *(Hermite-Minkowski) Para todo corpo numérico* $\mathbb{K} \neq \mathbb{Q}$*, o discriminante é* $\neq \pm 1$.

Demonstração: Pelo Corolário 2.7.3 temos que $|\delta_{\mathbb{K}|\mathbb{Q}}| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$. Como $\frac{\pi}{3} > 1$ e $\frac{3\pi}{4} > 1$ segue que $|\delta_{\mathbb{K}|\mathbb{Q}}| > 1$. Portanto, $|\delta_{\mathbb{K}|\mathbb{Q}}| \neq \pm 1$. ■

Corolário 2.7.4 *Se $\mathbb{K}$ é uma extensão de $\mathbb{Q}$ não ramificada então $\mathbb{K} = \mathbb{Q}$.*

Demonstração: Suponhamos que $\mathbb{K} \neq \mathbb{Q}$. Pelo Teorema 2.7.1 temos que $|\delta_{\mathbb{K}|\mathbb{Q}}| > 1$. Assim, existe um primo p que divide $\delta_{\mathbb{K}|\mathbb{Q}}$. Pelo Teorema 2.4.2, temos que p ramifica, o que é um absurdo. Portanto, $\mathbb{K} = \mathbb{Q}$. ∎

Teorema 2.7.2 *(Hermite) Em $\mathbb{C}$ existe somente finitos corpos numéricos com um dado discriminante $\delta_{\mathbb{K}|\mathbb{Q}}$.*

Demonstração: Pelo Corolário 2.7.3, o grau de tal corpo é limitado. Fixemos n, r_1, r_2. Seja $\mathbb{K}$ este corpo. Em $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ definimos o conjunto :
i) $D = \{(y_1, \cdots, y_{r_1}, z_1, \cdots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} : |y_1| \leq 2^n \left(\frac{\pi}{2}\right)^{-r_2} |\delta_{\mathbb{K}|\mathbb{Q}}|^{\frac{1}{2}}, |y_i| \leq \frac{1}{2}, i = 1, \cdots, r_1$ e $|z_j| \leq \frac{1}{2}, j = 1, \cdots, r_2,\ r_1 > 0\}$.
ii) $D = \{(z_1, \cdots, z_{r_2}) \in \mathbb{C}^{r_2} : |z_1 - \bar{z}_1| \leq 2^n \left(\frac{\pi}{2}\right)^{1-r_2} |\delta_{\mathbb{K}|\mathbb{Q}}|^{\frac{1}{2}}, |z_1 + \bar{z}_1| \leq \frac{1}{2}$ e $|z_j| \leq \frac{1}{2}, j = 2, \cdots, r_2,\ r_1{=}0.\}$
Temos que D é compacto, pois é fechado e limitado, e D é convexo e simétrico em relação a origem no $\mathbb{R}^n$. Vamos calcular o volume de D. Seja σ o homomorfismo canônico de $\mathbb{K}$. Se A é o anel dos inteiros, então $\sigma(A)$ é um reticulado com

$$v(\sigma(A)) = 2^{-r_2}|\delta_{\mathbb{K}|\mathbb{Q}}|^{\frac{1}{2}} \ e \ v(D) = 2^n v(\sigma(A)).$$

Assim, pelo Teorema 2.6.3, existe $g \in D \cap (\sigma(A) - \{0\})$. Assim, existe $x \in A - \{0\}$ tal que $\sigma(x) \in D$. Vamos mostrar que x é um elemento primitivo de $\mathbb{K}$ sobre $\mathbb{Q}$. No caso $i)$ temos que $|\sigma_i(x)| \leq \frac{1}{2}$, para $i \neq 1$. Como $|N(x)| = \prod_{i=1}^{n} |\sigma_i(x)|$ é um inteiro positivo, segue que $|\sigma_1(x)| \geq 1$. Assim,

$$|\sigma_1(x)| \neq |\sigma_i(x)|, \text{ para todo } i \neq 1.$$

Portanto, x é um elemento primitivo, pois caso contrário $\sigma_1(x)$ coincidiria com $\sigma_i(x)$, para algum i. No caso $ii)$ temos analogamente que $|\sigma_1(x)| = |\bar{\sigma}_1(x)| \geq 1$. Assim, $|\sigma_1(x)| \neq |\sigma_j(x)|$ quando $\sigma_1 \neq \sigma_j$ ou $\sigma_1 \neq \overline{\sigma}_j$. Agora, como

$$|\sigma_1(x) + i\sigma_1(x) + \sigma_1(x) - i\sigma_1(x)| = |2\sigma_1(x)| < \frac{1}{2},$$

segue que $\Re(\sigma_1(x)) \leq \frac{1}{4}$. Mas isto significa que $\sigma_1(x)$ não pode ser real, pois se for contradiz $|\sigma_1(x)| \geq 1$. De modo análogo a $i)$ concluímos que x é primitivo. Em $i)$ e $ii)$ segue que os conjugados $\sigma_i(x)$ de x são limitados. Portanto, as funções simétricas elementares dos $\sigma_i(x)'s$

são limitadas. Em outras palavras, os coeficientes, assim como o grau do polinômio minimal, são limitados. Como x é inteiro, segue que seu polinômio minimal é mônico com coeficientes em $\mathbb{Z}$. Como o grau e os coeficientes do polinômio minimal são limitados, existe somente um número finito de possibilidades de valores de $x \in \mathbb{C}$. Como x gera $\mathbb{K}$, existe finitos $\mathbb{K}$. ■

Capítulo 3

Ramificação e diferente

Sejam 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 A. Pelo Teorema 1.6.1 temos que $\mathcal{O}_{\mathbb{L}}$ também é um anel de Dedekind. Vimos no capítulo 2, quais ideais primos $\mathcal{P}$ de A que ramificam em $\mathbb{L}$. Neste capítulo, veremos como determinar os ideais primos $\mathcal{Q}$ de $\mathcal{O}_{\mathbb{L}}$ que ramificam em $\mathbb{L}$. Para encontrar estes ideais introduzimos o conceito de diferente. Neste capítulo usamos as referências [4] e [8].

3.1 Diferente

Nesta seção, introduzimos o conceito de diferente e apresentamos suas principais propriedades. Para isso, seja $\mathbb{L}$ um corpo e $\mathbb{L}_1$ o dual de $\mathbb{L}$. Pelo Corolário 1.2.2, temos que existe um isomorfismo $\varphi : \mathbb{L} \longrightarrow \mathbb{L}_1$ tal que $\varphi(x) = S_x$, onde $x \in \mathbb{L}$ e $S_x(y) = Tr_{\mathbb{L}|\mathbb{K}}(xy)$, para $y \in \mathbb{L}$. Seja $\{x_1, \cdots, x_n\}$ uma $\mathbb{K}$-base de $\mathbb{L}$ e seja $x_1^*, \cdots, x_n^*$ elementos de $\mathbb{L}$ tal que $\{\varphi_{x_1^*}, \cdots, \varphi_{x_n^*}\}$ é uma base dual, 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 $i \neq j$. Assim, $\{x_1^*, \cdots, x_n^*\}$ é também uma base de $\mathbb{L}$, chamada de base complementar de $\{x_1, \cdots, x_n\}$.

Proposição 3.1.1 *Com as notações acima, temos que* $D(x_1, \cdots, x_n)D(x_1^*, \cdots, x_n^*) = 1$.

Demonstração: Sejam $\sigma_1, \cdots, \sigma_n$ os $\mathbb{K}$-isomorfismos de $\mathbb{L}$. Consideremos as matrizes

$$X = (\sigma_i(x_j))_{ij} \text{ e } X^* = (\sigma_i(x_j^*))_{ij}.$$

Denotando X^t para a matriz transposta de X, temos que $(X^*)^t X = (Tr_{\mathbb{L}|\mathbb{K}}(x_i^* x_j))_{ij}$. Assim, $\det(X^*)^t \det(X) = 1$. Pela Proposição 2.3.5, temos que

$$D(x_1, \cdots, x_n) = \det(X)^2 \text{ e } D(x_1^*, \cdots, x_n^*) = \det(X^*)^2.$$

Portanto, $D(x_1, \cdots, x_n)D(x_1^*, \cdots, x_n^*) = 1$. ■

Definição 3.1.1 *Seja M um subconjunto do corpo $\mathbb{L}$. O conjunto dado por*

$$M^* = \{x \in \mathbb{L} | Tr_{\mathbb{L}|\mathbb{K}}(xy) \in A, \forall y \in M\}$$

é definido como o codiferente de M sobre $\mathbb{K}$, que também é chamado de dual ou complementar de M.

Proposição 3.1.2 *Sejam M um subconjunto de $\mathbb{L}$ e M^* o codiferente de M sobre $\mathbb{K}$.*

1. *M^* é um A-módulo. Se $\mathcal{O}_{\mathbb{L}}M \subseteq M$ então M^* é um módulo sobre $\mathcal{O}_{\mathbb{L}}$.*
2. *Se $M_1 \subseteq M_2 \subseteq \mathbb{L}$ então $M_2^* \subseteq M_1^* \subseteq \mathbb{L}$.*
3. *$\mathcal{O}_{\mathbb{L}} \subseteq \mathcal{O}_{\mathbb{L}}^*$.*
4. *Se M é um A-módulo livre com base $\{x_1, \cdots, x_n\}$ então M^* é um A-módulo livre com base $\{x_1^*, \cdots, x_n^*\}$ e $M^{**} = M$.*

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

$$Tr_{\mathbb{L}|\mathbb{K}}((x_1 + x_2)y) = Tr_{\mathbb{L}|\mathbb{K}}(x_1y) + Tr_{\mathbb{L}|\mathbb{K}}(x_2y) \in A.$$

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

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

Assim, $ax \in M^*$. Portanto, M^* é um A-módulo. Agora, assumimos que $\mathcal{O}_{\mathbb{L}}M \subseteq M$. Se $b \in \mathcal{O}_{\mathbb{L}}$, $x \in M^*$e $y \in M$ temos que

$$Tr_{\mathbb{L}|\mathbb{K}}((bx)y) = Tr_{\mathbb{L}|\mathbb{K}}(x(by)) \in A,$$

pois $by \in M$. Assim, $bx \in M^*$. Portanto, M^* é um $\mathcal{O}_{\mathbb{L}}$-módulo.
2) Suponhamos que $M_1 \subseteq M_2$. Se $x_2 \in M_2^*$, então, $x_2 \in \mathbb{L}$ e $Tr_{\mathbb{L}|\mathbb{K}}(x_2y) \in A, \forall y \in M_2$. Como $M_1 \subset M_2$ temos que $Tr_{\mathbb{L}|\mathbb{K}}(x_2y) \in A, \forall y \in M_1$. Logo, $x_2 \in M_1^*$. Portanto, $M_2^* \subseteq M_1^* \subseteq \mathbb{L}$.
3) Como $\mathcal{O}_{\mathbb{L}}$ é inteiro sobre A e integralmente fechado segue que $Tr_{\mathbb{L}|\mathbb{K}}(\mathcal{O}_{\mathbb{L}}) \subset A$. Assim, se $x, y \in \mathcal{O}_{\mathbb{L}}$ então $Tr(xy) \in A$, e deste modo $x \in \mathcal{O}_{\mathbb{L}}^*$. Portanto, $\mathcal{O}_{\mathbb{L}} \subseteq \mathcal{O}_{\mathbb{L}}^*$.
4) Seja $\{x_1, \cdots, x_n\}$ uma base de M e seja $\{x_1^*, \cdots, x_n^*\}$ uma base de $\mathbb{L}$ tal que $Tr_{\mathbb{L}|\mathbb{K}}(x_i^*x_j) = 0$ se $i \neq j$, e $Tr_{\mathbb{L}|\mathbb{K}}(x_i^*x_i) = 1$. Como $0, 1 \in A$ segue que

$$x_i^* \in M^* = \{x_i^* \in \mathbb{L} | Tr_{\mathbb{L}|\mathbb{K}}(x_i^*x_j) \in A, \forall x_j \in M\}.$$

Portanto, $\sum_{i=1}^{n} Ax_i^* \subseteq M^*$. Reciprocamente, seja $\sum_{i=1}^{n} a_i x_i^* \in M^*$, com $a_i \in \mathbb{K}$, para $i = 1, \cdots, n$. Então, para $j = 1, \cdots, n$, temos que

$$a_j = Tr\left(\left(\sum_{i=1}^{n} a_i x_i^*\right) x_j\right) \in A,$$

e deste modo $M^* \subseteq \sum_{i=1}^{n} Ax_i^*$. Assim, $M^* = \sum_{i=1}^{n} Ax_i^*$. Portanto, M^* é um A-módulo livre e $M^{**} = M$. ∎

Teorema 3.1.1 *Se $\mathbb{L} = \mathbb{K}[\alpha]$, onde α é inteiro sobre A e $g(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in A[X]$ o polinômio minimal de α sobre $\mathbb{K}$, então:*
1) $Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{\alpha^i}{g'(\alpha)}\right) = 0$, para $i = 1, \cdots, n-2$, e $Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{\alpha^{n-1}}{g'(\alpha)}\right) = 1$.
2) $A[\alpha]^* = \frac{1}{g'(\alpha)} A[\alpha]$.

Demonstração: 1) Sejam $\alpha = \alpha_1, \cdots, \alpha_n$ os conjugados de α sobre $\mathbb{K}$, onde são necessariamente distintos e pertencem a uma extensão de Galois $\mathbb{L}_1$ de grau finito sobre $\mathbb{K}$. Devemos calcular $Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{\alpha^i}{g'(\alpha)}\right) = \sum_{k=1}^{n} \frac{\alpha_k^i}{g'(\alpha_k)}$, para $i = 1, \cdots, n-1$. Como $g(x)$ é o polinômio minimal de α, temos que $g(x) = \prod_{k=1}^{n}(x - \alpha_k)$. Assim,

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

e podemos expressar este produto como a soma $\sum_{k=1}^{n} \frac{a_k}{x - \alpha_k}$, para certos elementos a_k, $k = 1, \cdots, n$. Sendo $\frac{1}{g(x)} = \sum_{k=1}^{n} \frac{a_k}{x - \alpha_k}$, temos que

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

para todo $i = 1, \cdots, n$. Assim, para $j = 1, \cdots, n$, temos que

$$1 = \sum_{k=1}^{n} a_k \left(\prod_{i \neq k}(\alpha_j - \alpha_i)\right) = a_j \prod_{i \neq j}(\alpha_j - \alpha_i).$$

Logo, $a_j = \frac{1}{\prod_{i \neq j}(\alpha_j - \alpha_i)} = \frac{1}{g'(\alpha_j)}$, para $j = 1, 2, \cdots, n$ e $\frac{1}{g(x)} = \sum_{k=1}^{n} \frac{1}{g'(\alpha_k)(x - \alpha_k)}$. Pelo algoritmo da divisão longa de Euclides, temos que

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

e

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

Assim, temos que $\sum_{k=1}^{n} \frac{1}{g'(\alpha_k)} \left[\frac{1}{x} + \frac{\alpha_k}{x^2} + \frac{\alpha_k^2}{x^3} + \cdots \right] = \frac{1}{x^n} + c_1 \frac{1}{x^{n+1}} + \cdots$. Comparando esta última igualdade, temos que $\sum_{k=1}^{n} \left(\frac{\alpha_k^i}{g'(\alpha_k)} \right) = 0$, para $i = 1, \cdots, n-2$ e $\sum_{k=1}^{n} \left(\frac{\alpha_k^{n-1}}{g'(\alpha_k)} \right) = 1$.

2) Primeiramente, temos que $\left\{ \frac{\alpha^j}{g'(\alpha)} \right\}_{j=0,\cdots,n-1}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, uma vez que, se

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

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

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 $j = 0, 1, \cdots, n-1$, e como a dimensão é n, segue que é uma base. Agora, tomando $y = \sum_{i=0}^{n-1} a_i \alpha^i \in A[\alpha]$ temos que

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

e assim, $\frac{\alpha^j}{g'(\alpha)} \in A[\alpha]^*$, para todo $j = 0, \cdots, n-1$. Portanto, $A[\alpha]\frac{1}{g'(\alpha)} \subseteq A[\alpha]^*$. Para mostrar a outra inclusão, se $y \in A[\alpha]^*$, então $y = \sum_{j=0}^{n-1} a_j \left(\frac{\alpha^j}{g'(\alpha)} \right)$, uma vez que os elementos $\frac{\alpha^j}{g'(\alpha)}$, para $j = 0, \cdots, n-1$, formam uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Assim,

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

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

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

$$
\begin{aligned}
&= a_{n-2} + a_{n-1} Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{\alpha^n}{g'(\alpha)}\right) = a_{n-2} - a_{n-1}\left(\sum_{i=0}^{n} c_i Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{\alpha^{n-i}}{g'(\alpha)}\right)\right)\\
&= a_{n-2} - a_{n-1}c_1,
\end{aligned}
$$

pois $\alpha^n = -(c_1\alpha^{n-1} + c_2\alpha^{n-2} + \cdots + c_n)$, com $c_i \in A$. Como $a_{n-2} - a_{n-1}c_1 \in A$ segue que $a_{n-2} \in A$. De modo análogo, $a_i \in A$, para todo $i = 1, \cdots, n-1$. Portanto, $A[\alpha]^* = \dfrac{1}{g'(\alpha)}A[\alpha]$, o que demonstra o Teorema. ■

Proposição 3.1.3 *Se $\mathbb{L} = \mathbb{K}[\alpha]$, onde α é inteiro sobre A, então $\mathcal{O}_{\mathbb{L}}^*$ é um $\mathcal{O}_{\mathbb{L}}$-módulo finitamente gerado.*

Demonstração: Pelo Teorema 1.1.1 temos que $A[\alpha]$ é um A-módulo livre de posto finito. Pela Proposição 3.1.2 item 4) segue que $A[\alpha]^*$ é um A-módulo finitamente gerado. Como $A[\alpha] \subseteq \mathcal{O}_{\mathbb{L}}$, segue que $\mathcal{O}_{\mathbb{L}}^* \subseteq A[\alpha]^*$. Como A é Noetheriano, pois é Dedekind, segue que $\mathcal{O}_{\mathbb{L}}^*$ é um A-módulo finitamente gerado. Portanto, $\mathcal{O}_{\mathbb{L}}^*$ também é um $\mathcal{O}_{\mathbb{L}}$-módulo finitamente gerado. ■

Corolário 3.1.1 *$\mathcal{O}_{\mathbb{L}}^*$ é um ideal fracionário de $\mathbb{L}$.*

Demonstração: Pela Proposição 3.1.3 segue que $\mathcal{O}_{\mathbb{L}}^*$ é um $\mathcal{O}_{\mathbb{L}}$-módulo finitamente gerado. Assim, $d\mathcal{O}_{\mathbb{L}}^* \subseteq \mathcal{O}_{\mathbb{L}}$, onde d é o máximo divisor comum dos números dos geradores de $\mathcal{O}_{\mathbb{L}}^*$.■

Definição 3.1.2 *O ideal $(\mathcal{O}_{\mathbb{L}}^*)^{-1} \subseteq \mathcal{O}_{\mathbb{L}}$ é chamado diferente de $\mathcal{O}_{\mathbb{L}}$ sobre A e é denotado por $\Delta(\mathcal{O}_{\mathbb{L}}|A)$ ou $\Delta(\mathbb{L}|\mathbb{K})$.*

Exemplo 3.1.1 *Seja $\mathbb{L} = \mathbb{Q}(\sqrt{2})$ e $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\sqrt{2}]$. Temos que*

$$\mathcal{O}_{\mathbb{L}}^* = \mathbb{Z}[\sqrt{2}]^* = \left\{\frac{m}{2} + \frac{n\sqrt{2}}{4} : m, n \in \mathbb{Z}\right\},$$

assim $\Delta(\mathbb{Z}[\sqrt{2}]|\mathbb{Z}) = (\mathcal{O}_{\mathbb{L}}^*)^{-1} = \{4a + 2\sqrt{2}b : a, b \in \mathbb{Z}\} = 2\sqrt{2}\mathbb{Z}[\sqrt{2}]$.

Observação 3.1.1 *Como $\mathcal{O}_{\mathbb{L}} \subseteq \mathcal{O}_{\mathbb{L}}^*$ então $\Delta(\mathcal{O}_{\mathbb{L}}|A)$ é um ideal inteiro de $\mathcal{O}_{\mathbb{L}}$. Sendo $\mathcal{O}_{\mathbb{L}}$ um domínio de Dedekind, então $\Delta(\mathcal{O}_{\mathbb{L}}|A)$ pode ser escrito de modo único como $\Delta(\mathcal{O}_{\mathbb{L}}|A) = \prod \mathcal{Q}^{s_{\mathcal{Q}}}$, onde $\mathcal{Q}$ são ideais primos de $\mathcal{O}_{\mathbb{L}}$ e $s_{\mathcal{Q}} \geq 0$ são inteiros.*

Definição 3.1.3 *O inteiro $s_{\mathcal{Q}}$ é chamado expoente para $\mathcal{Q}$ do diferente $\Delta(\mathcal{O}_{\mathbb{L}}|A)$.*

Proposição 3.1.4 *Se $\mathbb{L} = \mathbb{K}[\alpha]$, onde $\alpha \in \mathcal{O}_{\mathbb{L}}$ e $g(x) \in A[x]$ é o polinômio minimal de α sobre $\mathbb{K}$, então $\Delta(\mathcal{O}_{\mathbb{L}}|A) = \mathcal{O}_{\mathbb{L}}g'(\alpha)$ se, e somente se, $\mathcal{O}_{\mathbb{L}} = A[\alpha]$.*

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

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

Reciprocamente, sejam $\mathcal{O}_{\mathbb{L}}^* = \dfrac{1}{g'(\alpha)}\mathcal{O}_{\mathbb{L}}$ e $z \in \mathcal{O}_{\mathbb{L}}$ um elemento. Assim, existe um polinômio $h(x) \in \mathbb{K}[x]$ de grau menor que $n = [\mathbb{L} : \mathbb{K}]$ tal que $z = h(\alpha)$. Na demonstração do Teorema 3.1.1, 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 $\alpha = \alpha_1, \cdots, \alpha_n$ são os conjugados de α sobre $\mathbb{K}$. O polinômio $h_1(x) = \displaystyle\sum_{k=1}^{n} h(\alpha_k) \prod_{i\neq k} \frac{x-\alpha_i}{\alpha_k-\alpha_i}$ tem grau menor que n e $h_1(\alpha_j) = \displaystyle\sum_{k=1}^{n} h(\alpha_k) \prod_{i\neq k} \frac{\alpha_j-\alpha_i}{\alpha_k-\alpha_i} = h(\alpha_j)$, pois se $k \neq j$ temos que $\displaystyle\prod_{i\neq k} \frac{\alpha_j-\alpha_i}{\alpha_k-\alpha_i} = 0$. Então $h(x) = h_1(x)$, pois o polinômio $h(x) - h_1(x)$ tem n raízes. Mas,

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

Como todo coeficiente de $\dfrac{g(x)}{x-\alpha}$ está em $\mathbb{L}$ e é inteiro sobre A, segue que $\dfrac{g(x)}{x-\alpha} \in \mathcal{O}_{\mathbb{L}}[x]$. Como $\dfrac{z}{g'(\alpha)} \in \mathcal{O}_{\mathbb{L}}^*$ segue que $h(x) = Tr_{\mathbb{L}|\mathbb{K}}\left(\dfrac{zg(x)}{g'(\alpha)(x-\alpha)}\right) \in A[x]$. Assim, $z = h(\alpha) \in A[\alpha]$. Portanto, $\mathcal{O}_{\mathbb{L}} = A[\alpha]$. ∎

Exemplo 3.1.2 *Sejam* $\mathbb{L} = \mathbb{Q}(\sqrt{3})$ *e* $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\sqrt{3}]$. *O polinômio minimal de* $\sqrt{3}$ *é* $x^2 - 3$. *Assim,* $\Delta(\mathcal{O}_{\mathbb{L}}|A) = 2\sqrt{3}\mathbb{Z}[\sqrt{3}]$.

Proposição 3.1.5 *Seja* $\mathcal{J}$ *um ideal fracionário de* $\mathcal{O}_{\mathbb{L}}$. *Então* $Tr_{\mathbb{L}|\mathbb{K}}(\mathcal{J}) \subseteq A$ *se, e somente se,* $\mathcal{J} \subseteq \mathcal{O}_{\mathbb{L}}^* = \Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1}$.

Demonstração: Se $\mathcal{J} \subset \mathcal{O}_{\mathbb{L}}^*$ então $Tr_{\mathbb{L}|\mathbb{K}}(\mathcal{J}) \subseteq A$. Por outro lado, se $x \in \mathcal{O}_{\mathbb{L}}$ e $y \in \mathcal{J}$, temos que $xy \in \mathcal{O}_{\mathbb{L}}\mathcal{J} = \mathcal{J}$. Como $Tr_{\mathbb{L}|\mathbb{K}}(\mathcal{J}) \subseteq A$, segue que $Tr_{\mathbb{L}|\mathbb{K}}(xy) \in A$, $\forall x \in \mathcal{O}_{\mathbb{L}}$. Portanto, $\mathcal{J} \subset \mathcal{O}_{\mathbb{L}}^*$. ∎

Lema 3.1.1 *Sejam* $\mathcal{A}$, $\mathcal{B}$ *ideais fracionários de* $\mathbb{L}$. *Se para todo* $\mathcal{M}$ *ideal fracionário de* $\mathbb{L}$ *tem-se que* $\mathcal{M} \subseteq \mathcal{A}$ *se, e somente se,* $\mathcal{M} \subseteq \mathcal{B}$, *então* $\mathcal{A} = \mathcal{B}$.

Demonstração: Se $x \in \mathcal{A}$ então $\mathcal{M} = \langle x \rangle \subset \mathcal{A}$. Assim, $\mathcal{M} \subset \mathcal{B}$, ou seja, $x \in \mathcal{B}$. Logo, $\mathcal{A} \subseteq \mathcal{B}$. Análogo, para $\mathcal{B} \subseteq \mathcal{A}$. Portanto, $\mathcal{A} = \mathcal{B}$. ∎

Proposição 3.1.6 *Seja $\mathbb{L}_1$ uma extensão separável de $\mathbb{L}$ de grau finito. Seja $\mathcal{O}_{\mathbb{L}_1}$, $\mathcal{O}_{\mathbb{L}}$ e A o anel dos inteiros de $\mathbb{L}_1$, $\mathbb{L}$ e $\mathbb{K}$, respectivamente. Então*

$$\Delta(\mathcal{O}_{\mathbb{L}_1}|A) = \mathcal{O}_{\mathbb{L}_1}\Delta(\mathcal{O}_{\mathbb{L}}|A)\Delta(\mathcal{O}_{\mathbb{L}_1}|\mathcal{O}_{\mathbb{L}}).$$

Demonstração: Seja $\mathcal{M}$ um ideal fracionário de $\mathcal{O}_{\mathbb{L}_1}$ tal que $\mathcal{M} \subseteq \Delta(\mathcal{O}_{\mathbb{L}_1}|\mathcal{O}_{\mathbb{L}})^{-1}$. Pela Proposição 3.1.5, temos que $Tr_{\mathbb{L}_1|\mathbb{L}}(\mathcal{M}) \subseteq \mathcal{O}_{\mathbb{L}}$. Assim,

$$\Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1} \supseteq \Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1}Tr_{\mathbb{L}_1|\mathbb{L}}(\mathcal{M}).$$

Como $\mathcal{M} = \mathcal{M}\mathcal{O}_{\mathbb{L}_1}$ temos que $\Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1} \supseteq Tr_{\mathbb{L}_1|\mathbb{L}}(\mathcal{O}_{\mathbb{L}_1}\Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1}\mathcal{M})$. Temos também que

$$A \supseteq Tr_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1}) \supseteq Tr_{\mathbb{L}|\mathbb{K}}(Tr_{\mathbb{L}_1|\mathbb{L}}(\mathcal{O}_{\mathbb{L}_1}\Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1})\mathcal{M}) = Tr_{\mathbb{L}_1|\mathbb{K}}(\mathcal{O}_{\mathbb{L}_1}\Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1}\mathcal{M}).$$

Novamente, pela Proposição 3.1.5, temos que

$$\mathcal{O}_{\mathbb{L}_1}\Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1}\mathcal{M} \subseteq \Delta(\mathcal{O}_{\mathbb{L}_1}|A)^{-1} \text{ e que } \mathcal{M} \subseteq \mathcal{O}_{\mathbb{L}_1}\Delta(\mathcal{O}_{\mathbb{L}}|A)\Delta(\mathcal{O}_{\mathbb{L}_1}|A)^{-1}.$$

Pelo Lema 3.1.1 segue que $\Delta(\mathcal{O}_{\mathbb{L}_1}|\mathcal{O}_{\mathbb{L}})^{-1} = \mathcal{O}_{\mathbb{L}_1}\Delta(\mathcal{O}_{\mathbb{L}}|A)\Delta(\mathcal{O}_{\mathbb{L}_1}|A)^{-1}$. Portanto, $\Delta(\mathcal{O}_{\mathbb{L}_1}|A) = \mathcal{O}_{\mathbb{L}_1}\Delta(\mathcal{O}_{\mathbb{L}}|A)\Delta(\mathcal{O}_{\mathbb{L}_1}|\mathcal{O}_{\mathbb{L}})$. ∎

Definição 3.1.4 *Sejam $\mathbb{K}$ um corpo de números, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n, e A e $\mathcal{O}_{\mathbb{L}}$ os anéis de inteiros de $\mathbb{K}$ e $\mathbb{L}$, respectivamente.*
(i) O diferente $\Delta(\mathcal{O}_{\mathbb{L}}|A)$, também denotado por $\Delta_{\mathbb{L}|\mathbb{K}}$, é chamado de diferente de $\mathbb{L}|\mathbb{K}$. Em particular, se $\mathbb{K} = \mathbb{Q}$, o diferente de $\mathbb{L}|\mathbb{Q}$ é chamado de diferente absoluto e denotado por $\Delta_{\mathbb{L}}$.
(ii) Sejam $\mathcal{P}$ um ideal primo de A, $S = A - \mathcal{P}$, $A' = S^{-1}A$ e $\mathcal{O}'_{\mathbb{L}} = S^{-1}\mathcal{O}_{\mathbb{L}}$. O diferente $\Delta(\mathcal{O}'_{\mathbb{L}}|A')$ é chamado de diferente de $\mathbb{L}|\mathbb{K}$ sobre $\mathcal{P}$ é denotado por $\Delta_{\mathcal{P}}(\mathbb{L}|\mathbb{K})$ ou $\Delta_{\mathcal{P}}$.

Proposição 3.1.7 *Com as notações da Definição 3.1.4, temos que $\mathcal{O}'_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{L}}|A) = \Delta(\mathcal{O}'_{\mathbb{L}}|A')$.*

Demonstração: Se $x \in \mathcal{O}'_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{L}}|A)$ então x é da forma $\frac{y}{s}$, com $y \in \Delta(\mathcal{O}_{\mathbb{L}}|A)$ e $s \in S$. Seja $z \in (\mathcal{O}'_{\mathbb{L}})^*$, onde $(\mathcal{O}'_{\mathbb{L}})^*$ o codiferente do A'-módulo $\mathcal{O}'_{\mathbb{L}}$. Assim, $Tr_{\mathbb{L}|\mathbb{K}}(z\mathcal{O}'_{\mathbb{L}}) \subset A'$. Sendo $\mathcal{O}_{\mathbb{L}}$ um A-módulo finitamente gerado, então considere $\{t_1, \cdots, t_m\}$ um sistema de geradores. Seja $Tr_{\mathbb{L}|\mathbb{K}}(zt_i) = \frac{a_i}{s_i}$, com $a_i \in A$ e $s_i \in S$. Se $s_0 = s_1 \cdots s_m \in S$ então

$$Tr_{\mathbb{L}|\mathbb{K}}(zs_0t_i) = s_0Tr_{\mathbb{L}|\mathbb{K}}(zt_i) \in A, \forall i = 1, \cdots, m.$$

Assim, $Tr_{\mathbb{L}|\mathbb{K}}(zs_0\mathcal{O}_{\mathbb{L}}) \subseteq A$ e portanto $zs_0 \in \mathcal{O}^*_{\mathbb{L}}$, isto é, $yzs_0 \in \mathcal{O}_{\mathbb{L}}$, pois $y \in \Delta(\mathcal{O}_{\mathbb{L}}|A)$. Logo,

$$xz = \frac{yz}{s} = \frac{yzs_0}{ss_0} \in \mathcal{O}'_{\mathbb{L}}$$

o que implica que $x \in \Delta(\mathcal{O}_{\mathbb{L}}^{'}|A^{'})$. Assim, $\mathcal{O}_{\mathbb{L}}^{'}\Delta(\mathcal{O}_{\mathbb{L}}|A) \subseteq \Delta(\mathcal{O}_{\mathbb{L}}^{'}|A^{'})$. Por outro lado, seja $x \in \Delta(\mathcal{O}_{\mathbb{L}}^{'}|A^{'})$. Sendo $\mathcal{O}_{\mathbb{L}}^{*}$ um ideal fracionário de $\mathcal{O}_{\mathbb{L}}$, segue que $\mathcal{O}_{\mathbb{L}}^{*}$ é um A-módulo finitamente gerado. Seja $\{z_1, \cdots, z_m\}$ um sistema de geradores do A-módulo $\mathcal{O}_{\mathbb{L}}^{*}$. Temos que o traço $Tr_{\mathbb{L}|\mathbb{K}}(z_i\mathcal{O}_{\mathbb{L}}) \subseteq A$, para $i = 1, \cdots, m$. Como $S \subseteq \mathbb{K}$, segue que $Tr_{\mathbb{L}|\mathbb{K}}(z_i\mathcal{O}_{\mathbb{L}}^{'}) \subseteq A^{'}$, ou seja, $z_i \in (\mathcal{O}_{\mathbb{L}}^{'})^{*}$. Assim,

$$xz_i \in \mathcal{O}_{\mathbb{L}}^{'}, \text{ ou seja, } xz_i = \frac{b_i}{s_i} \text{ com } b_i \in \mathcal{O}_{\mathbb{L}} \text{ e } s_i \in S.$$

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

3.2 Ramificação e diferente

Nesta seção apresentamos um importante Teorema, que relaciona o conceito de diferente e ramificação. Provamos neste Teorema que os ideais primos de $\mathcal{O}_{\mathbb{L}}$ ramifica se, e somente se, estes divide o diferente. Sejam A um domínio de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{K} \subseteq \mathbb{L}$ uma extensão separável de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros de A em $\mathbb{L}$. Se $\mathcal{P}$ é um ideal primo não nulo de A, então $\mathcal{P}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{g} \mathcal{Q}_i^{e_i}$, onde cada $\mathcal{Q}_i$ é um ideal primo de $\mathcal{O}_{\mathbb{L}}$, uma vez que $\mathcal{O}_{\mathbb{L}}$ é um domínio de Dedekind. Sejam

$$\psi : A \longrightarrow A/\mathcal{P} = \bar{K}, \quad \psi_0 : \mathcal{O}_{\mathbb{L}} \longrightarrow \mathcal{O}_{\mathbb{L}}/\mathcal{P}\mathcal{O}_{\mathbb{L}}, \quad \psi_i : \mathcal{O}_{\mathbb{L}} \longrightarrow \mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i = \bar{\mathbb{L}}_i,$$

os homomorfismos canônicos de anéis, para todo $i = 1, \cdots, n$. Seja $\pi_i : \mathcal{O}_{\mathbb{L}}/\mathcal{P}\mathcal{O}_{\mathbb{L}} \longrightarrow \mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i^{e_i}$ a i-ésima projeção induzida do isomorfismo natural $\mathcal{O}_{\mathbb{L}}/\mathcal{P}\mathcal{O}_{\mathbb{L}} \simeq \prod_{i=1}^{g} \mathcal{O}_{\mathbb{L}}/\mathcal{Q}_i^{e_i}$. Assim, se $y \in \mathcal{O}_{\mathbb{L}}$ então

$$\psi_0(y) = y + \mathcal{P}\mathcal{O}_{\mathbb{L}} \text{ e } \pi_i(\psi_0(y)) = y + \mathcal{Q}_i^{e_i}.$$

Estas funções são naturalmente extendidas para os polinômios, pela ação dos coeficientes. Seja $S = A - \mathcal{P}$, $A^{'} = S^{-1}A$, $\mathcal{O}_{\mathbb{L}}^{'} = S^{-1}\mathcal{O}_{\mathbb{L}}$ e $\mathcal{P}^{'} = A^{'}\mathcal{P}$. Nesta seção, analizamos quando um ideal $\mathcal{Q}$ de $\mathcal{O}_{\mathbb{L}}$ ramifica em $\mathbb{L}$.

Lema 3.2.1 *Se $x \in \mathcal{O}_{\mathbb{L}}$ então $m_{\mathbb{L}|\mathbb{K}} \in A[x]$ e $\psi(m_{\mathbb{L}|\mathbb{K}}(x)) = \prod_{j=1}^{g}[p_{\bar{\mathbb{L}}_j|\bar{\mathbb{K}}}(\psi_j(x))]^{e_j}$*

$$\psi(Tr_{\mathbb{L}|\mathbb{K}}(x)) = \sum_{j=1}^{g} e_j[Tr_{\bar{\mathbb{L}}_j|\bar{\mathbb{K}}}(\psi_j(x))] \text{ e } \psi(N_{\mathbb{L}|\mathbb{K}}(x)) = \prod_{j=1}^{g}[N_{\bar{\mathbb{L}}_j|\bar{\mathbb{K}}}(\psi_j(x))]^{e_j}.$$

Demonstração: Como $x \in \mathcal{O}_{\mathbb{L}}$ segue que o seu polinômio minimal sobre $\mathbb{K}$ tem coeficientes em A. Pela Observação 1.2.2 temos que o seu polinômio característico é uma potência do polinômio minimal e também pertence $A[x]$. Pelo Teorema 1.8.2, temos que

$$\mathcal{O}_{\mathbb{L}}^{'}/\mathcal{P}\mathcal{O}_{\mathbb{L}}^{'} \simeq \mathcal{O}_{\mathbb{L}}/\mathcal{P}\mathcal{O}_{\mathbb{L}} \text{ e } A^{'}/A^{'}\mathcal{P} \simeq A/\mathcal{P}.$$

Como $A^{'}$ é um domínio de ideais principais pela Proposição 1.8.5, segue que $\mathcal{O}_{\mathbb{L}}^{'}$ é um $A^{'}$-módulo livre de posto n. Pela Proposição 2.4.1, temos que $m_{\mathcal{O}_{\mathbb{L}}^{'}|A^{'}}(x) = m_{\mathbb{L}|\mathbb{K}}(x)$. Como $\mathcal{O}_{\mathbb{L}}^{'}/\mathcal{P}\mathcal{O}_{\mathbb{L}}^{'} \simeq \mathcal{O}_{\mathbb{L}}/\mathcal{P}\mathcal{O}_{\mathbb{L}}$ é um espaço vetorial de dimensão n sobre $A^{'}/A^{'}\mathcal{P} \simeq A/\mathcal{P}$, segue da Proposição 1.2.4 e da Observação 2.4.1 que

$$\begin{aligned}\psi(m_{\mathbb{L}|\mathbb{K}}(x)) &= \psi(m_{\mathcal{O}_{\mathbb{L}}^{'}|A^{'}}(x)) = m_{(\mathcal{O}_{\mathbb{L}}^{'}/\mathcal{P}\mathcal{O}_{\mathbb{L}}^{'})|(A^{'}/A^{'}\mathcal{P})}(\psi_0(x)) \\ &= m_{(\mathcal{O}_{\mathbb{L}}/\mathcal{P}\mathcal{O}_{\mathbb{L}})|(A/\mathcal{P})}(\psi_0(x)) = \prod_{j=1}^{g} m_{(\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_j^{e_j})|(A/\mathcal{P})}(\pi_j(\psi_0(x))).\end{aligned}$$

Agora falta determinar o polinômio característico. Para isso, sejam

$$k = e_j, R = \mathcal{O}_{\mathbb{L}}/\mathcal{Q}_j^k, R_1 = \mathcal{Q}_j/\mathcal{Q}_j^k, \cdots, R_i = \mathcal{Q}_j^i/\mathcal{Q}_j^k, \cdots, R_{k-1} = \mathcal{Q}_j^{k-1}/\mathcal{Q}_j^k, R_k = 0.$$

Temos que R é um anel, $A/\mathcal{P} = \overline{\mathbb{K}}$ é um corpo contido em R e R é um $\overline{\mathbb{K}}$- espaço vetorial, cuja dimensão finita é igual ao grau de inércia de $\mathcal{Q}_j$ em $\mathbb{K} \subseteq \mathbb{L}$. Assim, temos uma cadeia estritamente decrescente de $\overline{\mathbb{K}}$ -subespaços vetoriais

$$R \supset R_1 \supset R_2 \supset \cdots \supset R_{k-1} \supset R_k = 0,$$

e definimos uma multiplicação escalar como segue: $(b + \mathcal{Q}_j^k)(y + \mathcal{Q}_j^k) = by + \mathcal{Q}_j^k$, onde $b \in \mathcal{O}_{\mathbb{L}}$ e $y \in \mathcal{Q}_j^i$. Deste modo, cada R_i torna um ideal de R. Como $\mathcal{O}_{\mathbb{L}}$ é um domínio de Dedekind, segue que não existe um ideal $\mathcal{J}$ tal que $\mathcal{Q}_j^{i-1} \supset \mathcal{J} \supset \mathcal{Q}_j^i$, pois caso contrário existirão ideais $\mathcal{C}$ e $\mathcal{D}$ tais que $\mathcal{Q}_j^i = \mathcal{J}\mathcal{C}$ e $\mathcal{J} = \mathcal{Q}_j^{i-1}\mathcal{D}$. Logo, $\mathcal{Q}_j^i = \mathcal{Q}_j^{i-1}\mathcal{D}\mathcal{C}$ e assim, $\mathcal{Q}_j = \mathcal{D}\mathcal{C}$. Como $\mathcal{Q}_j \subseteq \mathcal{D} \subseteq A$ e $\mathcal{Q}_j \subseteq \mathcal{C} \subseteq A$, e como $\mathcal{Q}_j$ é maximal segue que $\mathcal{Q}_j = \mathcal{D}$ ou $\mathcal{D} = A$. Assim, a condição 2) do Teorema 1.2.3 é satisfeita. A condição 3) também é satisfeita, uma vez que se $y \in R_1$ e $z \in R_{i-1}$ então $yz \in R_i$. A condição 4) segue do fato que $\mathcal{O}_{\mathbb{L}}$ é um domínio de Dedekind e se $y, z \in \mathcal{O}_{\mathbb{L}}$, temos que

$$\bar{y} = y + \mathcal{Q}_j^k \in R,\ \bar{z} = z + \mathcal{Q}_j^k \in R \text{ e } \bar{y}\bar{z} = yz + \mathcal{Q}_j^k \in R_i.$$

Como $\bar{y} \notin R_1$ então $y \notin \mathcal{Q}_j$ e $yz \in \mathcal{Q}_j^i$. Assim, $z \in \mathcal{Q}_j^i$ e $\bar{z} \in R_i$. Agora, se $x \in \mathcal{O}_{\mathbb{L}}$ e $\bar{x} = x + \mathcal{Q}_j^k \in R$ então $m_{R|\bar{\mathbb{K}}}(\bar{x}) = [m_{(R/R_1|\bar{\mathbb{K}})}(\theta_1)]^k$, onde $\theta_1 : R/R_1 \longrightarrow R/R_1$ é definida por

$\theta_1(\bar{y}+R_1)=\bar{x}\bar{y}+R_1$. Assim, θ_1 é a função de multiplicação por $\bar{x}=\pi_j\psi_0(x)$. Agora, temos que

$$R/R_1=(\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_j^k)/(\mathcal{Q}_j/\mathcal{Q}_j^k)\simeq\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_j=\overline{\mathbb{L}}_j,$$

onde o isomorfismo $\eta: R/R_1\longrightarrow\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_j$ é definido como $\eta(\bar{y}+R_1)=\psi_j(y)$, onde $\bar{y}+R_1\in R/R_1$, com $y\in\mathcal{O}_{\mathbb{L}}$. Assim, temos que

$$\begin{array}{ccc} R/R_1 & \xrightarrow{\eta} & \bar{\mathbb{L}}_j \\ \theta_1\downarrow & & \downarrow\theta_{\psi_j(x)} \\ R/R_1 & \xrightarrow{\eta} & \bar{\mathbb{L}}_j \end{array}$$

e que

$$\theta_{(\psi_j(x))}\circ\eta(\bar{y}+R_1)=\psi_j(x)\psi_j(y)=\psi_j(xy)=\eta(\bar{x}\bar{y}+R_1)=\eta\circ\theta_1(\bar{y}+R_1).$$

Então $m_{(R/R_1/\bar{\mathbb{K}})}(\theta_1)=m_{\bar{\mathbb{L}}_j|\bar{\mathbb{K}}}(\psi_j(x))$. Portanto, $\psi(m_{\mathbb{L}|\mathbb{K}}(x))=\prod_{j=1}^{g}[m_{\bar{\mathbb{L}}_j|\bar{\mathbb{K}}}(\psi_j(x))]^{e_j}$. A prova do traço e da norma segue de modo análogo. ∎

Lema 3.2.2 *Sejam $\mathcal{Q}$ um ideal primo de $\mathcal{O}_{\mathbb{L}}$, $\mathcal{P}=\mathcal{Q}\cap A$, $S=A-\mathcal{P}$, $A'=S^{-1}A$ e $\mathcal{O}'_{\mathbb{L}}=S^{-1}\mathcal{O}_{\mathbb{L}}$. Então $\prod_{i=1}^{g}\mathcal{O}'_{\mathbb{L}}\mathcal{Q}_i^{1-e_i}\subseteq(\mathcal{O}'_{\mathbb{L}})^*$.*

Demonstração: Como $\Delta(\mathcal{O}_{\mathbb{L}}|A)$ é um ideal de $\mathcal{O}_{\mathbb{L}}$ e $\mathcal{O}_{\mathbb{L}}$ é um domínio de Dedekind, segue que $\Delta(\mathcal{O}_{\mathbb{L}}|A)$ pode ser escrito de modo único como $\Delta(\mathcal{O}_{\mathbb{L}}|A)=\prod\mathcal{Q}^{s_{\mathcal{Q}}}$, onde $\mathcal{Q}$ são ideais primos de $\mathcal{O}_{\mathbb{L}}$ e $s_{\mathcal{Q}}\geq 0$ são inteiros, e $\mathcal{P}\mathcal{O}_{\mathbb{L}}=\prod_{i=1}^{g}\mathcal{Q}_i^{e_i}$, onde $\mathcal{Q}_i$ são ideais primos de $\mathcal{O}_{\mathbb{L}}$ tal que $\mathcal{Q}_i\cap A=\mathcal{P}$, para $i=1,\cdots,g$. Pelo Corolário 1.8.2, segue que $\mathcal{P}\mathcal{O}'_{\mathbb{L}}=\prod_{i=1}^{g}\mathcal{O}'_{\mathbb{L}}\mathcal{Q}_i^{e_i}$. Pela Proposição 3.1.7, temos que

$$\mathcal{O}'_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{L}}|A)=\Delta(\mathcal{O}'_{\mathbb{L}}|A')=\prod_{i=1}^{g}\mathcal{O}'_{\mathbb{L}}\mathcal{Q}_i^{s_i},$$

onde $s_i=s_{\mathcal{Q}_i}$, para $i=1,\cdots,g$. Desta maneira, o módulo complementar do A'-módulo $\mathcal{O}'_{\mathbb{L}}$ é $(\mathcal{O}'_{\mathbb{L}})^*=\prod_{i=1}^{g}\mathcal{O}'_{\mathbb{L}}\mathcal{Q}_i^{-s_i}$. Seja $x\in\prod_{i=1}^{g}\mathcal{O}'_{\mathbb{L}}\mathcal{Q}_i^{1-e_i}$. Como $\mathcal{P}'=A'\mathcal{P}$ é um ideal principal pela Proposição 1.8.5, segue que existe $t\in\mathbb{K}$ tal que $\mathcal{P}'=A't$. Como $\mathcal{O}'_{\mathbb{L}}t=\mathcal{O}'_{\mathbb{L}}\mathcal{P}=\prod_{i=1}^{g}\mathcal{O}'_{\mathbb{L}}\mathcal{Q}_i^{e_i}$, segue que $xt\in\prod_{i=1}^{g}\mathcal{O}'_{\mathbb{L}}\mathcal{Q}_i\subseteq\bigcap_{i=1}^{g}\mathcal{O}'_{\mathbb{L}}\mathcal{Q}_i$. Isto implica que $Tr_{\mathbb{L}|\mathbb{K}}(xt)\in A'\mathcal{P}$, uma vez que se $\widetilde{\mathbb{L}}$ é a

menor extensão de Galois $\mathbb{K}$ contendo $\mathbb{L}$ e se o anel dos inteiros é $\widetilde{\mathcal{O}_{\mathbb{L}}}$, segue que $xt \in S^{-1}\widetilde{\mathcal{O}_{\mathbb{L}}}\widetilde{\mathcal{Q}}$ para todo ideal primo $\widetilde{\mathcal{Q}}$ de $\widetilde{\mathcal{O}_{\mathbb{L}}}$ tal que $\widetilde{\mathcal{Q}} \cap A = \mathcal{P}$. Então vale para todos os conjugados de xt em $\mathbb{K} \subseteq \widetilde{\mathbb{L}}$ e assim

$$Tr_{\widetilde{\mathbb{L}}|\mathbb{K}}(xt) = [\widetilde{\mathbb{L}} : \mathbb{L}]Tr_{\mathbb{L}|\mathbb{K}}(xt) \in \left(\bigcap_{\widetilde{\mathcal{Q}}} S^{-1}\widetilde{\mathcal{O}_{\mathbb{L}}}\widetilde{\mathcal{Q}}\right) \cap A' = A'\mathcal{P}.$$

Assim, $Tr_{\mathbb{L}|\mathbb{K}}(xt) = tTr_{\mathbb{L}|\mathbb{K}}(x) \in A'\mathcal{P} = A't$. Portanto, $Tr_{\mathbb{L}|\mathbb{K}}(x) \in A'$. Agora, se $y \in \mathcal{O}'_{\mathbb{L}}$ temos que $xy \in \prod_{i=1}^{g} \mathcal{O}'_{\mathbb{L}}\mathcal{Q}_i^{1-e_i}$ assim $Tr_{\mathbb{L}|\mathbb{K}}(xy) \in A'$. Logo, $x \in (\mathcal{O}'_{\mathbb{L}})^*$. Portanto, $\prod_{i=1}^{g} \mathcal{O}'_{\mathbb{L}}\mathcal{Q}_i^{1-e_i} \subseteq (\mathcal{O}'_{\mathbb{L}})^*$. ■

Corolário 3.2.1 *Com as notações do Lema 3.2.2 temos que $s_i \geq e_i - 1$, para $i = 1, \cdots, g$, se, e somente se, $\prod_{i=1}^{g} \mathcal{O}'_{\mathbb{L}}\mathcal{Q}_i^{1-e_i} \subseteq (\mathcal{O}'_{\mathbb{L}})^*$.* ■

Teorema 3.2.1 *Com as notações do Lema 3.2.2 temos que $s_{\mathcal{Q}} = e_{\mathcal{Q}} - 1$ se, e somente se, a característica de $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}$ não divide o índice de ramificação $e_{\mathcal{Q}}$.*

Demonstração: Seja $\mathcal{Q}_1$ um ideal primo de $\mathcal{O}_{\mathbb{L}}$. Suponha que a característica de $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_1 = \mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}\mathcal{Q}_1$ divide o índice de ramificação e_1. Se mostrarmos que $\mathcal{J} = \mathcal{O}'_{\mathbb{L}}\mathcal{Q}_1^{-e_1}\prod_{i=2}^{g} \mathcal{O}'_{\mathbb{L}}\mathcal{Q}_i^{1-e_i} \subseteq (\mathcal{O}'_{\mathbb{L}})^*$ segue que $s_1 \geq e_1$. Assim, se $x \in \mathcal{J}$, pelo Lema 3.2.2, temos que $xt \in \bigcap_{i=2}^{g} \mathcal{O}'_{\mathbb{L}}\mathcal{Q}_i$. Pelo Lema 3.2.1, se $\psi : A' \longrightarrow A'/\mathcal{P}'$ e $\psi_i : \mathcal{O}'_{\mathbb{L}} \longrightarrow \mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}\mathcal{Q}_i$ são os homomorfismos canônicos, temos que

$$\psi(Tr_{\mathbb{L}|\mathbb{K}}(xt)) = \sum_{i=1}^{g} e_i Tr_{(\mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}\mathcal{Q}_i)|(A'/\mathcal{P}')}(\psi_i(xt)) = e_1 Tr_{(\mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}\mathcal{Q}_1)|(A'/\mathcal{P}')}(\psi_1(xt)).$$

Mas como e_1 é múltiplo da característica de $\mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}\mathcal{Q}_1$, segue que $\psi(Tr_{\mathbb{L}|\mathbb{K}}(xt)) = 0$, e então

$$tTr_{\mathbb{L}|\mathbb{K}}(x) = Tr_{\mathbb{L}|\mathbb{K}}(xt) \in \mathcal{P}' = A't,$$

ou seja, $Tr_{\mathbb{L}|\mathbb{K}}(x) \in A'$. Agora, se $y \in \mathcal{O}'_{\mathbb{L}}$, então $xy \in \mathcal{J}$. Logo $Tr_{\mathbb{L}|\mathbb{K}}(xy) \in A'$ e assim, $x \in (\mathcal{O}'_{\mathbb{L}})^*$. Portanto, $s_1 \geq e_1$, o que é um absurdo. Reciprocamente, suponhamos que a característica de $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}_1 = \mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}\mathcal{Q}_1$ não divide o índice de ramificação e_1. Seja $x \in \mathcal{O}'_{\mathbb{L}}$ um elemento tal que a imagem $\psi_1(x) \in \mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}\mathcal{Q}_1$ tem o traço não nulo. Pelo Lema 2.1.6, aplicado ao domínio de Dedekind $\mathcal{O}'_{\mathbb{L}}$, temos que existe $y \in \mathcal{O}'_{\mathbb{L}}$, tal que $y - x \in \mathcal{O}'_{\mathbb{L}}\mathcal{Q}_1$ e $y \in \mathcal{O}'_{\mathbb{L}}\mathcal{Q}_i^{e_i}$, para $i = 2, \cdots, g$. Então, pelo Lema 3.2.1,

$$\psi(Tr_{\mathbb{L}|\mathbb{K}}(y)) = \sum_{i=1}^{g} e_i Tr_{(\mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}\mathcal{Q}_i)|(A'/\mathcal{P}')}(\psi_i(y)) = e_1 Tr_{(\mathcal{O}'_{\mathbb{L}}/\mathcal{O}'_{\mathbb{L}}\mathcal{Q}_1)|(A'/\mathcal{P}')}(\psi_1(x)) \neq 0,$$

pois e_1 não é múltiplo da característica de $\mathcal{O}_{\mathbb{L}}^{'}/\mathcal{O}_{\mathbb{L}}^{'}\mathcal{Q}_1$. Assim, $Tr_{\mathbb{L}|\mathbb{K}}(y) \notin \mathcal{P}^{'} = A^{'}t$. Logo $Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{y}{t}\right) = \frac{1}{t}Tr_{\mathbb{L}|\mathbb{K}}(y)$, ou seja, $Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{y}{t}\right) \notin A^{'}$. Isto mostra que $\frac{y}{t} \notin (\mathcal{O}_{\mathbb{L}}^{'})^{*}$. Como $\mathcal{O}_{\mathbb{L}}^{'}t = \mathcal{O}_{\mathbb{L}}^{'}\mathcal{P}$ e $y \in \mathcal{O}_{\mathbb{L}}^{'}\mathcal{Q}_i^{e_i}$, para $i = 2, \cdots, g$, segue que $\frac{y}{t} \in \mathcal{O}_{\mathbb{L}}^{'}\mathcal{Q}_1^{-e_1} \not\subset (\mathcal{O}_{\mathbb{L}}^{'})^{*}$ e 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 3.2.2 *Um ideal $\mathcal{Q}$ de $\mathcal{O}_{\mathbb{L}}$ ramifica em $\mathbb{L}$ se, e somente se, $\mathcal{Q}$ divide o diferente $\Delta(\mathcal{O}_{\mathbb{L}}|A)$.*

Demonstração: Se $\mathcal{Q}$ ramifica em $\mathbb{L}$ então $e_{\mathcal{Q}} \geq 2$, e assim $s_{\mathcal{Q}} \geq 1$. Portanto, $\mathcal{Q}$ divide o diferente $\Delta(\mathcal{O}_{\mathbb{L}}|A)$. Reciprocamente, se $e_{\mathcal{Q}} = 1$ e como a característica de $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}$ não divide o índice de rafimicação $e_{\mathcal{Q}}$, temos pelo Teorema 3.2.1, que $s_{\mathcal{Q}} = e_{\mathcal{Q}} - 1 = 0$. Então $\mathcal{Q}$ não divide o diferente, o que contradiz a hipótese. Portanto, $e_{\mathcal{Q}} \geq 2$. ■

Lema 3.2.3 *Sejam $\mathcal{P}$ um ideal primo não nulo de A, $S = A - \mathcal{P}$, $A^{'} = S^{-1}A$ e $\mathcal{O}_{\mathbb{L}}^{'} = S^{-1}\mathcal{O}_{\mathbb{L}}$. Se $\{x_1^{'}, \cdots, x_n^{'}\}$ é uma base do $A^{'}$-módulo $\mathcal{O}_{\mathbb{L}}^{'}$ então $A^{'}D(x_1^{'}, \cdots, x_n^{'}) = A^{'}N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A))$.*

Demonstração: Pelo Teorema 1.8.1 temos que $\mathcal{O}_{\mathbb{L}}^{'}$ é um domínio de Dedekind. Pela Proposição 1.8.2, temos que $\mathcal{O}_{\mathbb{L}}^{'}$ tem somente um número finito de ideais primos e pela Proposição 2.1.3, $\mathcal{O}_{\mathbb{L}}^{'}$ é um domínio de ideais principais. Se $(\mathcal{O}_{\mathbb{L}}^{'})^{*}$ é o codiferente do $A^{'}$-módulo $\mathcal{O}_{\mathbb{L}}^{'}$ livre temos que $(\mathcal{O}_{\mathbb{L}}^{'})^{*}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{L}}^{'}$. Logo, existe $y \in \mathbb{L}$, $y \neq 0$, tal que $(\mathcal{O}_{\mathbb{L}}^{'})^{*} = \mathcal{O}_{\mathbb{L}}^{'}y$. Assim, pela Proposição 3.1.7, temos que

$$\mathcal{O}_{\mathbb{L}}^{'}y^{-1} = \Delta(\mathcal{O}_{\mathbb{L}}^{'}|A^{'}) = \mathcal{O}_{\mathbb{L}}^{'}\Delta(\mathcal{O}_{\mathbb{L}}|A).$$

Se $\{x_1^{'}, \cdots, x_n^{'}\}$ é uma base do $A^{'}$-módulo $\mathcal{O}_{\mathbb{L}}^{'}$ então $\{yx_1^{'}, \cdots, yx_n^{'}\}$ é uma base de $(\mathcal{O}_{\mathbb{L}}^{'})^{*}$. Pela Proposição 3.1.2, temos que $(\mathcal{O}_{\mathbb{L}}^{'})^{*}$ tem uma base complementar $\{(x_1^{'})^{*}, \cdots, (x_n^{'})^{*}\}$ sobre $A^{'}$. Pelas Proposições 2.3.6 e 2.4.1, temos que

$$D_{\mathbb{L}|\mathbb{K}}((x_1^{'})^{*}, \cdots, (x_n^{'})^{*}) = D_{((\mathcal{O}_{\mathbb{L}}^{'})^{*}|A^{'})}((x_1^{'})^{*}, \cdots, (x_n^{'})^{*})$$

e $D_{\mathbb{L}|\mathbb{K}}(yx_1^{'}, \cdots, yx_n^{'}) = D_{((\mathcal{O}_{\mathbb{L}}^{'})^{*}|A^{'})}(y(x_1^{'}), \cdots, y(x_n^{'}))$ são elementos associados de $A^{'}$. Mas

$$D_{\mathbb{L}|\mathbb{K}}(x_1^{'}, \cdots, x_n^{'})D_{\mathbb{L}|\mathbb{K}}((x_1^{'})^{*}, \cdots, (x_n^{'})^{*}) = 1$$

e $D_{\mathbb{L}|\mathbb{K}}(yx_1^{'}, \cdots, yx_n^{'}) = [N_{\mathbb{L}|\mathbb{K}}(y)]^2\ D_{\mathbb{L}|\mathbb{K}}(x_1^{'}, \cdots, x_n^{'})$. Portanto, $[N_{\mathbb{L}|\mathbb{K}}(y)]^2[D_{\mathbb{L}|\mathbb{K}}(x_1^{'}, \cdots, x_n^{'})]^2$ é uma unidade de $A^{'}$. Portanto, $A^{'}D_{\mathbb{L}|\mathbb{K}}(x_1^{'}, \cdots, x_n^{'}) = A^{'}N_{\mathbb{L}|\mathbb{K}}(y^{-1})$. Seja $y = \frac{z}{a}$, onde $z \in \mathcal{O}_{\mathbb{L}}$, $a \in S$. Como $\mathcal{O}_{\mathbb{L}}^{'}y^{-1} = \mathcal{O}_{\mathbb{L}}^{'}\Delta(\mathcal{O}_{\mathbb{L}}|A)$, segue que

$$\mathcal{O}_{\mathbb{L}}^{'}(\mathcal{O}_{\mathbb{L}}a) = \mathcal{O}_{\mathbb{L}}^{'}(\mathcal{O}_{\mathbb{L}}z\Delta(\mathcal{O}_{\mathbb{L}}|A)).$$

Logo, $\mathcal{O}_{\mathbb{L}}a = \mathcal{O}_{\mathbb{L}}z\Delta(\mathcal{O}_{\mathbb{L}}|A)$. Assim, $N_{\mathbb{L}|\mathbb{K}}(\mathcal{O}_{\mathbb{L}}a) = N_{\mathbb{L}|\mathbb{K}}(\mathcal{O}_{\mathbb{L}}z)N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A))$, e $a^nA = AN_{\mathbb{L}|\mathbb{K}}(z)N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A))$. Assim, $a^nA' = A'N_{\mathbb{L}|\mathbb{K}}(z)N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A))$ e consequentemente $N_{\mathbb{L}|\mathbb{K}}(a)A'N_{\mathbb{L}|\mathbb{K}}(z^{-1}) = A'N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A))$. Logo, $N_{\mathbb{L}|\mathbb{K}}(az^{-1})A' = A'N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A))$, e assim,

$$N_{\mathbb{L}|\mathbb{K}}(y^{-1})A' = A'N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A)).$$

Portanto, $A'D(x_1', \cdots, x_n') = A'N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A))$. ∎

Teorema 3.2.3 *Com as mesmas notações do Lema 3.2.3, temos que*

$$N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A)) = D(x_1, \cdots, x_n),$$

onde $\{x_1, \cdots, x_n\}$ *é uma* $\mathbb{K}$*-base de* $\mathbb{L}$.

Demonstração: Sejam $\{x_1, \cdots, x_n\}$ uma $\mathbb{K}$-base de $\mathbb{L}$ contida em $\mathcal{O}_{\mathbb{L}}$ e $\{x_1', \cdots, x_n'\}$ uma base do A'-módulo $\mathcal{O}_{\mathbb{L}}'$. Assim $x_j = \sum_{i=1}^{n} a_{ij}'x_i'$, com $a_{ij}' \in A'$, para $j = 1, \cdots, n$. Logo, $D_{\mathbb{L}|\mathbb{K}}(x_1, \cdots, x_n) \in A'D_{\mathbb{L}|\mathbb{K}}(x_1', \cdots, x_n')$. Pelo Lema 3.2.3, segue que

$$D_{\mathbb{L}|\mathbb{K}}(x_1, \cdots, x_n) \subseteq A'N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A)),$$

e isto implica que $D_{\mathbb{L}|\mathbb{K}}(x_1, \cdots, x_n) \subseteq \bigcap A'N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A))$. Pela Proposição 1.8.3, temos que

$$D_{\mathbb{L}|\mathbb{K}}(x_1, \cdots, x_n) \subseteq N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A)).$$

Reciprocamente, sejam $D_{\mathbb{L}|\mathbb{K}}(x_1, \cdots, x_n) = \mathcal{P}^s\mathcal{J}$ e $N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A)) = \mathcal{P}^{s'}\mathcal{J}'$, onde $\mathcal{J}, \mathcal{J}'$ são ideais de A, não múltiplos de $\mathcal{P}$. Devemos mostrar que $s \leq s'$, pois se é verdadeiro para todo ideal primo $\mathcal{P} \neq 0$ de A, temos que $D_{\mathbb{L}|\mathbb{K}}(x_1, \cdots, x_n)$ divide $N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A))$, ou seja, $N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A)) \subseteq D_{\mathbb{L}|\mathbb{K}}(x_1, \cdots, x_n)$. Para todo ideal primo $\mathcal{P} \neq 0$ de A, escolhemos uma base $\{x_1', \cdots, x_n'\}$ do A'-módulo $\mathcal{O}_{\mathbb{L}}'$. Multiplicando por um elemento conveniente de S temos que cada $x_i' \in \mathcal{O}_{\mathbb{L}}$. Seja $AD_{\mathbb{L}|\mathbb{K}}(x_1', \cdots, x_n') = \mathcal{P}^r\mathcal{I}$, onde $\mathcal{I}$ é um ideal A não múltiplo de $\mathcal{P}$. Pelo Corolário 1.8.2, temos que

$$A'D_{\mathbb{L}|\mathbb{K}}(x_1', \cdots, x_n') = (A'\mathcal{P})^r$$

e pelo Lema 3.2.3, temos que $A'D_{\mathbb{L}|\mathbb{K}}(x_1', \cdots, x_n') = A'N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A)) = (A'\mathcal{P})^{s'}$. Assim, $s' = r$. Como $D_{\mathbb{L}|\mathbb{K}}(x_1, \cdots, x_n) \supset AD_{\mathbb{L}|\mathbb{K}}(x_1', \cdots, x_n') = \mathcal{P}^{s'}\mathcal{I}$ segue que $D_{\mathbb{L}|\mathbb{K}}(x_1, \cdots, x_n)$ divide $\mathcal{P}^{s'}\mathcal{I}$, e então $s \leq s'$. Assim,

$$N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A)) \subseteq D_{\mathbb{L}|\mathbb{K}}(x_1, \cdots, x_n).$$

Portanto, $N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A)) = D_{\mathbb{L}|\mathbb{K}}(x_1, \cdots, x_n)$. ∎

Exemplo 3.2.1 *Seja* $\mathbb{K} = \mathbb{Q}[\sqrt{2}]$. *Temos pelo Exemplo 3.1.1, que* $\Delta(\mathcal{O}_{\mathbb{L}}|A) = 2\sqrt{2}\mathbb{Z}[\sqrt{2}]$. *Assim,* $N(2\sqrt{2}\mathbb{Z}[\sqrt{2}]) = 8 = D(1, \sqrt{2})$.

Proposição 3.2.1 *Se* $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{L}_1$ *são corpos de números algébricos, então*

$$\delta_{\mathbb{L}_1|\mathbb{K}} = (\delta_{\mathbb{L}|\mathbb{K}})^{[\mathbb{L}_1:\mathbb{L}]} N_{\mathbb{L}|\mathbb{K}}(\delta_{\mathbb{L}_1|\mathbb{L}}).$$

Demonstração: Pela Proposição 3.1.6, temos que $\Delta(\mathcal{O}_{\mathbb{L}_1}|A) = \mathcal{O}_{\mathbb{L}_1}\Delta(\mathcal{O}_{\mathbb{L}}|A)\Delta(\mathcal{O}_{\mathbb{L}_1}|\mathcal{O}_{\mathbb{L}})$, onde $\mathcal{O}_{\mathbb{L}_1}$ é o anel dos inteiros de $\mathbb{L}_1$. Então

$$N_{\mathbb{L}_1|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}_1}|A)) = N_{\mathbb{L}_1|\mathbb{K}}(\mathcal{O}_{\mathbb{L}_1}\Delta(\mathcal{O}_{\mathbb{L}}|A))N_{\mathbb{L}_1|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}_1}|\mathcal{O}_{\mathbb{L}})).$$

Pela Proposição 1.7.4 e pelo Teorema 3.2.3, temos que

$$\begin{aligned}
\delta_{\mathbb{L}_1|\mathbb{K}} &= N_{\mathbb{L}|\mathbb{K}}[N_{\mathbb{L}_1|\mathbb{L}}(\mathcal{O}_{\mathbb{L}_1}\Delta(\mathcal{O}_{\mathbb{L}}|A)]N_{\mathbb{L}|\mathbb{K}}[N_{\mathbb{L}_1|\mathbb{L}}(\Delta(\mathcal{O}_{\mathbb{L}_1}|\mathcal{O}_{\mathbb{L}}))] \\
&= N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|A))^{[\mathbb{L}_1:\mathbb{L}]}N_{\mathbb{L}|\mathbb{K}}(\delta_{\mathbb{L}_1|\mathbb{L}}) \\
&= (\delta_{\mathbb{L}|\mathbb{K}})^{[\mathbb{L}_1:\mathbb{L}]}N_{\mathbb{L}|\mathbb{K}}(\delta_{\mathbb{L}_1|\mathbb{L}}).
\end{aligned}$$

■

Corolário 3.2.2 *Sejam* $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L}$ *corpos de números. Se* $D(x_1, \cdots, x_n) = d$, *onde* d *é um inteiro livre de quadrados e* $\{x_1, \cdots, x_n\}$ *uma* $\mathbb{Q}-$*base de* $\mathbb{K}$, *então* $\mathbb{L} = \mathbb{K}$ *ou* $\mathbb{K} = \mathbb{Q}$.

Demonstração: Suponhamos que $\mathbb{K} \neq \mathbb{Q}$. Pelo Teorema 2.7.1, temos que $D(x_1, \cdots, x_n) \neq \pm 1$. Assim, existe um número primo p tal que p divide $D(x_1, \cdots, x_n)$. Pela Proposição 3.2.1, temos que $p^{[\mathbb{L}:\mathbb{K}]}$ divide $D(x_1, \cdots, x_n)$. Como $D(x_1, \cdots, x_n)$ é livre de quadrados, segue que $\mathbb{L} = \mathbb{K}$. ■

Definição 3.2.1 *Sejam* α *um elemento de* $\mathbb{L}$ *e* $g(x)$ *o polinômio minimal de* α *sobre* $\mathbb{K}$, *e* $g'(\alpha) = \prod_{i=2}^{n}(\alpha - \sigma_i(\alpha))$, *onde* $\sigma_1, \sigma_2, \cdots, \sigma_n$, *são os* $\mathbb{K}$*-isomorfismos de* $\mathbb{L}$. *Definimos* $g'(\alpha)$ *como o diferente do elemento* α *na extensão* $\mathbb{L}$ *de* $\mathbb{K}$.

Definição 3.2.2 *Seja* $F_\alpha = \{x \in \mathcal{O}_{\mathbb{L}} | xA[\alpha]^* \subseteq \mathcal{O}_{\mathbb{L}}^*\}$. *Temos que* F_α *é um ideal de* $\mathcal{O}_{\mathbb{L}}$ *chamado de condutor de* $A[\alpha]$ *em* $\mathcal{O}_{\mathbb{L}}$.

Lema 3.2.4 *Com as notações anteriores temos que* $F_\alpha = g'(\alpha)\mathcal{O}_{\mathbb{L}}^*$.

Demonstração: Pelo Teorema 3.1.1, temos que $g'(\alpha)A[\alpha]^* = A[\alpha] \subseteq \mathcal{O}_{\mathbb{L}}$. Assim,

$$(g'(\alpha)\mathcal{O}_{\mathbb{L}}^*)A[\alpha]^* = g'(\alpha)A[\alpha]^*\mathcal{O}_{\mathbb{L}}^* \subseteq \mathcal{O}_{\mathbb{L}}^*.$$

Reciprocamente, seja $x \in \mathcal{O}_{\mathbb{L}}$ tal que $xA[\alpha]^* \subseteq \mathcal{O}_{\mathbb{L}}^*$. Pelo Teorema 3.1.1, segue que $x \in xA[\alpha] \subseteq g'(\alpha)\mathcal{O}_{\mathbb{L}}^*$. Portanto, $F_\alpha = g'(\alpha)\mathcal{O}_{\mathbb{L}}^*$. ■

Proposição 3.2.2 *Com as notações anteriores temos que F_α é o maior ideal de $\mathcal{O}_\mathbb{L}$ contido em $A[\alpha]$.*

Demonstração: Pelo Teorema 3.1.1, temos que $\mathcal{O}_\mathbb{L}^* \subseteq A[\alpha]^* = \frac{A[\alpha]}{g'(\alpha)}$. Assim, $F_\alpha = g'(\alpha)\mathcal{O}_\mathbb{L}^* \subseteq A[\alpha]$. Seja $\mathcal{J}$ um ideal de $\mathcal{O}_\mathbb{L}$ tal que $\mathcal{J} \subseteq A[\alpha]$ e seja $x \in \mathcal{J}$. Pelo Teorema 3.1.1, temos que $Tr_{\mathbb{L}|\mathbb{K}}\left(\frac{x}{g'(\alpha)}\right) \in A$. Assim, $\frac{x}{g'(\alpha)} \in \mathcal{O}_\mathbb{L}^*$, pela definição de $\mathcal{O}_\mathbb{L}^*$. Portanto, $x \in g'(\alpha)\mathcal{O}_\mathbb{L}^* = F_\alpha$. ■

Lema 3.2.5 *Sejam $\mathcal{P}$ um ideal primo não nulo de A, $e \geq 1$. Se S é um sistema de representantes do A módulo $\mathcal{P}$, tal que $0 \in S$, $t \in \mathcal{P}$, $t \notin \mathcal{P}^2$, então*

$$R = \{s_0 + s_1 t + \cdots + s_{e-1}t^{e-1} | s_i \in S, \forall i = 1, \cdots, e-1\}$$

é um sistema de representantes do A-módulo $\mathcal{P}^e$.

Demonstração: Provaremos por indução sobre e. Para $e = 1$, temos por hipótese que R é um sistema de representantes do A-módulo $\mathcal{P}$. Suponhamos válido para $e-1$. Sejam $r = s_0 + tr_1$ e $r' = s_0' + tr_1'$ elementos distintos de R. Se $r - r' = (s_0 - s_0') + (r_1 - r_1')t + \mathcal{P}^e$, segue que

$$s_0 - s_0' \in -(r_1 - r_1')t + \mathcal{P}^e \subseteq \mathcal{P},$$

e assim $s_0 = s_0'$ e $(r_1 - r_1')t \in \mathcal{P}^e$. Por hipótese, $At = \mathcal{P}\mathcal{J}$, onde $\mathcal{P}$ não divide $\mathcal{J}$. Assim, existe um ideal $\mathcal{G}$ de A tal que $r_1 - r_1' \in \mathcal{P}^e\mathcal{G} = A(r_1 - r_1')At = A(r_1 - r_1')\mathcal{P}\mathcal{J}$ e portanto $\mathcal{P}^{e-1}$ divide $A(r_1 - r_1')\mathcal{J}$. Como $\mathcal{P}$ não divide $\mathcal{J}$ segue que $r_1 - r_1' \in \mathcal{P}^{e-1}$ e pela hipótese de indução, temos que $r_1 = r_1'$ e portanto $r = r'$. Assim, R contém $\#(A/\mathcal{P})^e$ diferentes representantes do A-módulo $\mathcal{P}^e$. Pela Proposição 1.7.3, segue que R é um sistema de representantes do A-módulo $\mathcal{P}^e$. ■

Lema 3.2.6 *Sejam $\mathcal{P} \subseteq A$ e $\mathcal{Q} \subseteq \mathcal{O}_\mathbb{L}$ tais que $\mathcal{Q} \cap A = \mathcal{P}$. Se $\mathcal{P}\mathcal{O}_\mathbb{L} = \mathcal{Q}^e \cdot \mathcal{J}$, onde $e \geq 1$ e $\mathcal{Q}$ não divide $\mathcal{J}$, então existe um elemento $\alpha \in \mathcal{J}$, $\alpha \notin \mathcal{Q}$ tal que:*
1) A imagem $\bar{\alpha}$ de α em $\mathcal{O}_\mathbb{L}/\mathcal{Q}$ é um gerador do grupo cíclico multiplicativo dos elementos não nulos do corpo finito $\mathcal{O}_\mathbb{L}/\mathcal{Q}$.
2) Para todo inteiro $l > 0$ e para todo $b \in \mathcal{O}_\mathbb{L}$ existe $c \in A[\alpha]$ tal que $b - c \in \mathcal{Q}^l$.

Demonstração: Seja $u \in \mathcal{O}_\mathbb{L}$, $u \notin \mathcal{Q}$ tal que a imagem $\bar{u}$ de u em $\mathcal{O}_\mathbb{L}/\mathcal{Q}$ é um gerador do grupo cíclico multiplicativo dos elementos não nulos de $\mathcal{O}_\mathbb{L}/\mathcal{Q}$. Se $\nu = N(\mathcal{Q}) = \#\mathcal{O}_\mathbb{L}/\mathcal{Q}$ então $u^{\nu-1} \equiv 1\ (modulo \mathcal{Q})$, e assim, $u^\nu \equiv u (modulo \mathcal{Q})$. Se $u^\nu \equiv u (modulo \mathcal{Q}^2)$, seja $v \in \mathcal{Q}$, $v \notin \mathcal{Q}^2$. Então $\overline{u+v} = \bar{u}$ e

$$(u+v)^\nu = u^\nu + \nu u^{\nu-1}v + \cdots + v^\nu \in u^\nu + \mathcal{Q}^2,$$

pois $N(\mathcal{Q}) \in \mathcal{Q}$. Assim,

$$(u+v)^{\nu} \equiv (u+v)(modulo \mathcal{Q}) \; e \; (u+v)^{\nu} - (u+v) \in (u^{\nu} - u) - v + z,$$

com $z \in \mathcal{Q}^2$, pois $\nu \geq 2$. Agora, se $u_1 = u + v$, temos que $u_1^{\nu} - u_1 \in \mathcal{Q}$ e $u_1^{\nu} - u_1 \notin \mathcal{Q}^2$. Como $\mathcal{Q}$ não divide $\mathcal{J}$ segue que $\mathcal{O}_{\mathbb{L}} = \mathcal{Q}^2 + \mathcal{J}$. Assim, podemos escrever $u_1 = v_1 + \alpha$, com $v_1 \in \mathcal{Q}^2$ e $\alpha \in \mathcal{J}$. Então a imagem de α em $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}$ é $\bar{\alpha} = \bar{u_1} = \bar{u}$. Logo, α é um gerador do grupo cíclico multiplicativo dos elementos não nulos de $\mathcal{O}_{\mathbb{L}}/\mathcal{Q}$ e $\alpha \notin \mathcal{Q}$. De modo análogo, temos que

$$\alpha^{\nu} - \alpha = (u_1^{\nu} - u_1) - v_1 + z_1,$$

com $z_1 \in \mathcal{Q}^2$. Como $v_1 \in \mathcal{Q}^2$ temos que $\alpha^{\nu} - \alpha \notin \mathcal{Q}^2$. Agora, seja S um sistema de representantes do $\mathcal{O}_{\mathbb{L}}$-módulo $\mathcal{Q}$. Se $w = \alpha^{\nu} - \alpha$ e $S = \{1, \alpha, \alpha^2, \cdots, \alpha^{\nu-1}\}$ então, para todo elemento $l > 0$ e para todo $b \in \mathcal{O}_{\mathbb{L}}$, segue pelo Lema 3.2.5 que existe um único elemento $c = s_0 + s_1 w + \cdots + s_{l-1} w^{l-1} \in A[\alpha]$, com cada $s_i \in \{1, \alpha, \alpha^2, \cdots, \alpha^{\nu-1}\}$, tal que $b - c \in \mathcal{Q}^l$. ∎

Lema 3.2.7 *Se $\alpha \in \mathcal{J}$ é tal que $\alpha \notin \mathcal{Q}$, então $F_{\alpha} \not\subseteq \mathcal{Q}$.*

Demonstração: Seja $a \in \mathcal{O}_{\mathbb{L}} g^{'}(\alpha) \cap A$, com $a \neq 0$. Seja $Aa = \mathcal{P}^r \mathcal{I}$, onde $r \geq 0$ e $\mathcal{P}$ não divide o ideal $\mathcal{I}$. Se h é o número das classes de $\mathbb{K}$, então pela Proposição 1.6.1 temos que $(Aa)^h$ e $(\mathcal{P})^{rh}$ são ideais principais, ou seja, $Aa^h = Aa_1$, $\mathcal{P}^{rh} = Aa_2$, com $a_1, a_2 \in A$. Assim $a_1 = a_2 a_3$, onde $a_3 \in \mathcal{I}^h$. Logo, $a_3 \notin \mathcal{P}$, pois a maior potência de $\mathcal{P}$ que divide a_1 é rh. O ideal principal $\mathcal{O}_{\mathbb{L}}(a_3 \alpha^{rh})$ está contido em $A[\alpha]$, pois pelo Lema 3.2.6, existem $b \in \mathcal{O}_{\mathbb{L}}$ e $c \in A[\alpha]$ tal que $b - c \in \mathcal{Q}^{erh}$. Assim,

$$b a_3 \alpha^{rh} = (b-c) a_3 \alpha^{rh} + c a_3 \alpha^{rh}.$$

Como $c a_3 \alpha^{rh} \in A[\alpha]$ é suficiente mostrar que $(b-c) a_3 \alpha^{rh} \in A[\alpha]$. Temos que

$$\mathcal{O}_{\mathbb{L}}(b-c) a_3 \alpha^{rh} = \frac{\mathcal{O}_{\mathbb{L}} a_2 a_3 (b-c) \alpha^{rh}}{\mathcal{P}^{rh} \mathcal{O}_{\mathbb{L}}} \subseteq \frac{\mathcal{O}_{\mathbb{L}} a_1 \mathcal{Q}^{erh} \cdot \mathcal{O}_{\mathbb{L}} \alpha^{rh}}{\mathcal{Q}^{erh} \cdot \mathcal{J}^{rh}} \subseteq \mathcal{O}_{\mathbb{L}} a^h \mathcal{O}_{\mathbb{L}} \subseteq g^{'}(\alpha) \mathcal{O}_{\mathbb{L}} \subseteq A[\alpha],$$

pois $\alpha \in \mathcal{J}$ e $g^{'}(\alpha) \mathcal{O}_{\mathbb{L}}^{*} \subseteq A[\alpha]$. Portanto, $\mathcal{O}_{\mathbb{L}}(a_3 \alpha^{rh}) \subseteq A[\alpha]$. Pela Proposição 3.2.2, temos que $\mathcal{O}_{\mathbb{L}}(a_3 \alpha^{rh}) \subseteq F_{\alpha}$. Como $a_3 \notin \mathcal{P}$, segue que $a_3 \notin \mathcal{Q}$ e $\alpha \notin \mathcal{Q}$. Assim, $a_3 \alpha^{rh} \notin \mathcal{Q}$. Portanto, $F_{\alpha} \not\subseteq \mathcal{Q}$. ∎

Lema 3.2.8 *Com as notações anteriores temos que $\mathcal{O}_{\mathbb{L}} = \sum_{\alpha \in \mathcal{O}_{\mathbb{L}}} F_{\alpha}$.*

Demonstração: Como $F_{\alpha} \subseteq \mathcal{O}_{\mathbb{L}}$ para cada $\alpha \in \mathcal{O}_{\mathbb{L}}$, segue que $\sum_{\alpha \in \mathcal{O}_{\mathbb{L}}} F_{\alpha} \subseteq \mathcal{O}_{\mathbb{L}}$. Para provar a igualdade é suficiente mostrar que os ideais F_{α}, com $\alpha \in \mathcal{O}_{\mathbb{L}}$ são comaximais, ou seja, o máximo divisor comum dos $F_{\alpha}, \alpha \in \mathcal{O}_{\mathbb{L}}$, é igual a $\mathcal{O}_{\mathbb{L}}$. Mas isto segue do Lema 3.2.7, ou seja, não existe $\mathcal{Q} \subseteq \mathcal{O}_{\mathbb{L}}$ um ideal primo tal que $\mathcal{Q}$ divide $F_{\alpha}, \alpha \in \mathcal{O}_{\mathbb{L}}$. Portanto, $\sum_{\alpha \in \mathcal{O}_{\mathbb{L}}} F_{\alpha} = \mathcal{O}_{\mathbb{L}}$. ∎

Teorema 3.2.4 *Sejam $\Delta(\mathcal{O}_{\mathbb{L}}|A)$ o diferente de $\mathcal{O}_{\mathbb{L}}$ sobre A e $g^{'}(\alpha)$ o diferente do elemento α. Então, $\Delta(\mathcal{O}_{\mathbb{L}}|A)$ é um ideal de $\mathcal{O}_{\mathbb{L}}$ gerado pelos diferentes $g^{'}(\alpha)$ de todos os elementos $\alpha \in \mathcal{O}_{\mathbb{L}}$.*

Demonstração: Se $\alpha \in \mathcal{O}_{\mathbb{L}}$ segue que $\mathcal{O}_{\mathbb{L}}^{*} \subseteq A[t]^{*} = \dfrac{A[t]}{g^{'}(t)} \subseteq \mathcal{O}_{\mathbb{L}}\left(\dfrac{1}{g^{'}(t)}\right)$. Assim $g^{'}(t)\mathcal{O}_{\mathbb{L}}^{*} \subseteq \mathcal{O}_{\mathbb{L}}$. Portanto, $g^{'}(t) \in \Delta(\mathcal{O}_{\mathbb{L}}|A)$. Pelo Lema 3.2.8, temos que $\sum_{\alpha\in\mathcal{O}_{\mathbb{L}}} F_{\alpha} = \mathcal{O}_{\mathbb{L}}$. Assim, pelo Lema 3.2.4, temos que

$$\begin{aligned}\Delta(\mathcal{O}_{\mathbb{L}}|A) &= \Delta(\mathcal{O}_{\mathbb{L}}|A)\mathcal{O}_{\mathbb{L}} = \Delta(\mathcal{O}_{\mathbb{L}}|A)\left(\sum_{\alpha\in\mathcal{O}_{\mathbb{L}}} F_{\alpha}\right)\\ &= \sum_{\alpha\in\mathcal{O}_{\mathbb{L}}} \Delta(\mathcal{O}_{\mathbb{L}}|A)F_{\alpha} = \sum_{\alpha\in\mathcal{O}_{\mathbb{L}}} \Delta(\mathcal{O}_{\mathbb{L}}|A)g^{'}(\alpha)\mathcal{O}_{\mathbb{L}}^{*} = \sum_{\alpha\in\mathcal{O}_{\mathbb{L}}} \mathcal{O}_{\mathbb{L}}g^{'}(\alpha),\end{aligned}$$

uma vez que $\Delta(\mathcal{O}_{\mathbb{L}}|A)\mathcal{O}_{\mathbb{L}}^{*} = \mathcal{O}_{\mathbb{L}}$. ∎

Lema 3.2.9 *Sejam $\mathbb{K} \subseteq \mathbb{K}_1$ e $\mathbb{K} \subseteq \mathbb{K}_2$ corpos de números. Se $\mathbb{L} = \mathbb{K}_1\mathbb{K}_2$, então $\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}_2})$ divide $\mathcal{O}_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{K}_1}|A)$ e $\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}_1})$ divide $\mathcal{O}_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{K}_2}|A)$, onde $A, \mathcal{O}_{\mathbb{K}_1}$, $\mathcal{O}_{\mathbb{K}_2}$ e $\mathcal{O}_{\mathbb{L}}$ são os anéis dos inteiros de $\mathbb{K}$, $\mathbb{K}_1$, $\mathbb{K}_2$ e $\mathbb{L}$, respectivamente.*

Demonstração: Sejam $\alpha \in \mathcal{O}_{\mathbb{K}_1} \subseteq \mathcal{O}_{\mathbb{L}}$, $g(x) \in \mathbb{K}[x]$ o polinômio minimal de α sobre $\mathbb{K}$ e $h(x) \in \mathbb{K}_2[x]$ o polinômio minimal de α sobre $\mathbb{K}_2$. Assim, existe $k(x) \in \mathbb{K}_2[x]$ tal que $g(x) = h(x)k(x)$. Como α é inteiro segue que $g(x) \in A[x]$, $h(x) \in \mathcal{O}_{\mathbb{K}_2}[x]$ e $h(x)$ é mônico. Assim $k(x) \in \mathcal{O}_{\mathbb{K}_2}[x]$ e $g^{'}(\alpha) = h^{'}(\alpha)k(\alpha)$, com $h^{'}(\alpha) \in \Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}_2})$ e $k(\alpha) \in \mathcal{O}_{\mathbb{L}}$. Pelo Teorema 3.2.4, segue que $\Delta(\mathcal{O}_{\mathbb{K}_1}|A) = \sum_{\alpha\in\mathcal{O}_{\mathbb{K}_1}} \mathcal{O}_{\mathbb{K}_1}g^{'}(\alpha) = \sum_{\alpha\in\mathcal{O}_{\mathbb{K}_1}} \mathcal{O}_{\mathbb{K}_1}h^{'}(\alpha)k(\alpha) \subseteq \Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}_2})$. Portanto, $\Delta(\mathcal{O}_{\mathbb{K}_1}|A) \subseteq \Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}_2})$. De modo análogo, temos que $\Delta(\mathcal{O}_{\mathbb{K}_2}|A) \subseteq \Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}_2})$. ∎

Proposição 3.2.3 *Com as hipóteses do Lema 3.2.9, seja $\mathcal{P}$ um ideal primo não nulo do anel de inteiros A de $\mathbb{K}$. Então $\mathcal{P}$ não ramifica em $\mathbb{L}$ se, e somente se, $\mathcal{P}$ não ramifica em $\mathbb{K}_1$ e em $\mathbb{K}_2$.*

Demonstração: Se $\mathcal{P}$ não ramifica em $\mathbb{L}$ então $\mathcal{P}$ não ramifica em $\mathbb{K}_1$ e em $\mathbb{K}_2$. Reciprocamente, suponhamos que $\mathcal{P}$ ramifica em $\mathbb{L}$ e não ramifica em $\mathbb{K}_2$. Pelo Teorema 2.4.2, temos que $\mathcal{P}$ divide $\delta_{\mathbb{L}|\mathbb{K}}$ e $\mathcal{P}$ não divide $\delta_{\mathbb{K}_2|\mathbb{K}}$. Pela Proposição 3.2.1, temos que

$$\delta_{\mathbb{L}|\mathbb{K}} = (\delta_{\mathbb{K}_2|\mathbb{K}})^{[\mathbb{L}:\mathbb{K}_2]}N_{\mathbb{K}_2|\mathbb{K}}(\delta_{\mathbb{L}|\mathbb{K}_2}).$$

Assim, $\mathcal{P}$ divide $N_{\mathbb{K}_2|\mathbb{K}}(\delta_{\mathbb{L}|\mathbb{K}_2})$. Pelo Teorema 3.2.3 e pela transitividade da norma, temos que $\mathcal{P}$ divide

$$N_{\mathbb{K}_2|\mathbb{K}}(\delta_{\mathbb{L}|\mathbb{K}_2}) = N_{\mathbb{K}_2|\mathbb{K}}(N_{\mathbb{L}|\mathbb{K}_2}(\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}_2}))) = N_{\mathbb{L}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}_2})).$$

Pelo Lema 3.2.9 e pelo Teorema 3.2.3, temos que $\mathcal{P}$ divide

$$N_{\mathbb{L}|\mathbb{K}}(\mathcal{O}_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{K}_1}|A)) = N_{\mathbb{K}_1|\mathbb{K}}(N_{\mathbb{L}|\mathbb{K}_1}(\mathcal{O}_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{K}_1}|A))) = N_{\mathbb{K}_1|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{K}_1}|A))^{[\mathbb{L}:\mathbb{K}_1]} = \delta_{\mathbb{K}_1|\mathbb{K}}^{[\mathbb{L}:\mathbb{K}_1]}.$$

Assim, $\mathcal{P}$ divide $\delta_{\mathbb{K}_1|\mathbb{K}}$. Pelo Teorema 2.4.2, segue que $\mathcal{P}$ ramifica em $\mathbb{K}_1$, o que contradiz a hipótese. ∎

Corolário 3.2.3 *Sejam $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ corpos de números onde $\mathbb{M}$ é o menor corpo contendo $\mathbb{L}$ tal que $\mathbb{K} \subseteq \mathbb{M}$ é uma extensão de Galois. Seja $\mathcal{P}$ um ideal primo do anel dos inteiros A de $\mathbb{K}$. Então $\mathcal{P}$ não ramifica em $\mathbb{L}$ se, e somente se, $\mathcal{P}$ não ramifica em $\mathbb{M}$.*

Demonstração: Sejam $\mathbb{L} = \mathbb{L}_1, \mathbb{L}_2, \cdots, \mathbb{L}_n$, onde cada $\mathbb{L}_i$, $i = 1, \cdots, n$, é um conjugado de $\mathbb{L}$ sobre $\mathbb{K}$. Assim, $\mathbb{M} = \mathbb{L}_1\mathbb{L}_2 \cdots \mathbb{L}_n$, e o resultado segue pela Proposição 3.2.3. ∎

Proposição 3.2.4 *Sejam $\mathbb{K} \subseteq \mathbb{K}_1$ e $\mathbb{K} \subseteq \mathbb{K}_2$ corpos de números. Se $\mathbb{L} = \mathbb{K}_1\mathbb{K}_2$ e $\mathcal{P}$ é um ideal primo não nulo do anel de inteiros A de $\mathbb{K}$, então $N_{\mathbb{K}_2|\mathbb{K}}(\delta_{\mathbb{L}|\mathbb{K}_2})$ divide $(\delta_{\mathbb{K}_1|\mathbb{K}})^{[\mathbb{L}:\mathbb{K}_1]}$ e $N_{\mathbb{K}_1|\mathbb{K}}(\delta_{\mathbb{L}|\mathbb{K}_1})$ divide $(\delta_{\mathbb{K}_2|\mathbb{K}})^{[\mathbb{L}:\mathbb{K}_2]}$.*

Demonstração: Pelo Lema 3.2.9, temos que $\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}_2})$ divide $\mathcal{O}_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{K}_1}|A)$. Usando a norma, obtemos que $N_{\mathbb{K}_2|\mathbb{K}}(N_{\mathbb{L}|\mathbb{K}_2}(\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}_2}))$ divide $N_{\mathbb{K}_2|\mathbb{K}}(N_{\mathbb{L}|\mathbb{K}_2}(\mathcal{O}_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{K}_1}|A))$. Pelo Teorema 3.2.3, segue que $N_{\mathbb{K}_2|\mathbb{K}}(\delta_{\mathbb{L}|\mathbb{K}_2})$ divide

$$\begin{aligned} N_{\mathbb{K}_2|\mathbb{K}}(N_{\mathbb{L}|\mathbb{K}_2}(\mathcal{O}_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{K}_1}|A)) &= (N_{\mathbb{L}|\mathbb{K}}(\mathcal{O}_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{K}_1}|A))) = N_{\mathbb{K}_1|\mathbb{K}}(N_{\mathbb{L}|\mathbb{K}_1}(\mathcal{O}_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{K}_1}|A))) \\ &= N_{\mathbb{K}_1|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{K}_1}|A))^{[\mathbb{L}:\mathbb{K}_1]} = (\delta_{\mathbb{K}_1|\mathbb{K}})^{[\mathbb{L}:\mathbb{K}_1]}. \end{aligned}$$

De modo análogo, $N_{\mathbb{K}_1|\mathbb{K}}(\delta_{\mathbb{L}|\mathbb{K}_1})$ divide $(\delta_{\mathbb{K}_2|\mathbb{K}})^{[\mathbb{L}:\mathbb{K}_2]}$. ∎

Proposição 3.2.5 *Sejam $\mathbb{K} \subseteq \mathbb{K}_1$ e $\mathbb{K} \subseteq \mathbb{K}_2$ corpos de números com graus n_1 e n_2, respectivamente, tais que $\delta_{\mathbb{K}_1|\mathbb{K}}$ e $\delta_{\mathbb{K}_2|\mathbb{K}}$ sejam relativamente primos. Se $\mathbb{L} = \mathbb{K}_1\mathbb{K}_2$, então $[\mathbb{L} : \mathbb{Q}] = n_1n_2$.*

Demonstração: Temos que $[\mathbb{L} : \mathbb{Q}] = [\mathbb{L} : \mathbb{K}_2][\mathbb{K}_2 : \mathbb{Q}] = [\mathbb{L} : \mathbb{K}_2]n_2$. Se $[\mathbb{L} : \mathbb{Q}] < n_1n_2$ então $[\mathbb{L} : \mathbb{K}_2] < n_1$. Sejam $\mathbb{K}_1 = \mathbb{Q}[\alpha]$, onde $\alpha \in \mathbb{L}$ e $g(x) \in \mathbb{Q}[x]$ o polinômio minimal de α sobre $\mathbb{Q}$. Assim, $gr(g) = n_1$. Considere $h(x)$ o polinômio minimal de α sobre $\mathbb{K}_2$. Como $[\mathbb{L} : \mathbb{K}_2] < n_1$, segue que $h(x)$ tem grau menor que n_1 e divide $g(x)$. Se $\mathbb{M}$ é o subcorpo de $\mathbb{K}_2$ gerado pelos coeficientes de $h(x)$, então $\mathbb{M} \neq \mathbb{Q}$. Como $\mathbb{M} \subseteq \mathbb{K}_2$ temos que $\delta_{\mathbb{M}}$ divide $\delta_{\mathbb{K}_2|\mathbb{K}}$. Por outro lado, os coeficientes de $h(x)$ são funções simétricas elementares das raízes de $h(x)$, que estão entre os conjugados de α. Assim $h \in \mathbb{M}_1$, onde $\mathbb{M}_1$ é a menor extensão de Galois de $\mathbb{Q}$ contendo $\mathbb{K}_1$. Assim, $\mathbb{M} \subseteq \mathbb{M}_1$ e novamente $\delta_{\mathbb{M}}$ divide $\delta_{\mathbb{M}_1}$. Se p é um número primo que divide $\delta_{\mathbb{M}}$, então p

divide $\delta_{\mathbb{K}_2|\mathbb{K}}$ e $\delta_{\mathbb{M}_1}$. Pelo Teorema 2.4.2 e pelo Corolário 3.2.3, segue que p divide $\delta_{\mathbb{K}_1|\mathbb{K}}$, o que contradiz o fato de $mdc(\delta_{\mathbb{K}_1|\mathbb{K}}, \delta_{\mathbb{K}_2|\mathbb{K}}) = 1$. Assim, $|\delta_{\mathbb{M}}| = 1$. Pelo Teorema 2.7.1, temos que $\mathbb{M} = \mathbb{Q}$, o que é um absurdo. Portanto, $[\mathbb{L} : \mathbb{Q}] = n_1 n_2$. ∎

Proposição 3.2.6 *Sejam $\mathbb{K} \subseteq \mathbb{K}_1$ e $\mathbb{K} \subseteq \mathbb{K}_2$ corpos de números com graus n_1 e n_2, respectivamente, tais que $\delta_{\mathbb{K}_1|\mathbb{K}}$ e $\delta_{\mathbb{K}_2|\mathbb{K}}$ sejam relativamente primos. Se $\mathbb{L} = \mathbb{K}_1\mathbb{K}_2$, então*

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

Demonstração: Pela Proposição 3.2.1, temos que

$$\delta_{\mathbb{L}|\mathbb{K}} = (\delta_{\mathbb{K}_1|\mathbb{K}})^{n_2} N_{\mathbb{K}_1|\mathbb{K}}(\delta_{\mathbb{L}|\mathbb{K}_1}) = (\delta_{\mathbb{K}_2|\mathbb{K}})^{n_1} N_{\mathbb{K}_2|\mathbb{K}}(\delta_{\mathbb{L}|\mathbb{K}_2}).$$

Assim, $(\delta_{\mathbb{K}_1|\mathbb{K}})^{n_2}$ e $(\delta_{\mathbb{K}_2|\mathbb{K}})^{n_1}$ dividem $\delta_{\mathbb{L}|\mathbb{K}}$ e como $mdc(\delta_{\mathbb{K}_1|\mathbb{K}}, \delta_{\mathbb{K}_2|\mathbb{K}}) = 1$ temos que $(\delta_{\mathbb{K}_1|\mathbb{K}})^{n_2}$ $(\delta_{\mathbb{K}_2|\mathbb{K}})^{n_1}$ divide $\delta_{\mathbb{L}|\mathbb{K}}$. Por outro lado, pela Proposição 3.2.4, temos que $N_{\mathbb{K}_2|\mathbb{K}}(\delta_{\mathbb{L}|\mathbb{K}_2})$ divide $(\delta_{\mathbb{K}_1|\mathbb{K}})^{[\mathbb{L}:\mathbb{K}_1]} = \delta^{n_2}_{\mathbb{K}_1|\mathbb{K}}$, onde a última igualdade segue da Proposição 3.2.5. Assim,

$$\delta_{\mathbb{L}|\mathbb{K}} = N_{\mathbb{K}_2|\mathbb{K}}(\delta_{\mathbb{L}|\mathbb{K}_2})(\delta_{\mathbb{K}_2|\mathbb{K}})^{n_1}$$

divide $(\delta_{\mathbb{K}_1|\mathbb{K}})^{n_2}(\delta_{\mathbb{K}_2|\mathbb{K}})^{n_1}$. Portanto, $\delta_{\mathbb{L}|\mathbb{K}} = (\delta_{\mathbb{K}_1|\mathbb{K}})^{n_2}(\delta_{\mathbb{K}_2|\mathbb{K}})^{n_1}$. ∎

Exemplo 3.2.2 *Sejam $\mathbb{K}_1 = \mathbb{Q}(\sqrt{5})$ e $\mathbb{K}_2 = \mathbb{Q}(\sqrt[3]{2})$. Como $D(1, \frac{1+\sqrt{5}}{2}) = 5$ e $D(1, \sqrt[3]{2}, (\sqrt[3]{2})^2) = -2^2 3^3$ são relativamente primos segue que o discriminante de $\mathbb{L}$ sobre $\mathbb{K}$ é $(5)^3(-2^2 3^3)^2$.*

Teorema 3.2.5 *Sejam $n \in \mathbb{N}$, $n > 2$, e $\mathbb{K} = \mathbb{Q}(\xi_n)$, onde ξ_n é um 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*

$$D(1, \xi_n ..., \xi_n^{\varphi(n)-1}) = \prod_{j=1}^{r} \delta^{\phi(n/p_j^{a_j})}_{\mathbb{Q}(\xi_{p_j^{a_j}})} = \frac{(-1)^{\frac{\phi(n)r}{2}} n^{\phi(n)}}{\prod_{j=1}^{r} p_j^{\frac{\phi(n)}{p_j - 1}}}.$$

Demonstração: Vamos provar por indução sobre r. Para o caso $r = 1$, foi provado na Proposição 2.3.10. Suponhamos que o resultado é válido para $r - 1$, onde $r > 1$. Assim, pela Proposição 2.3.10 e pela hipótese de indução temos que o $mdc(\delta_{\mathbb{Q}(\xi_{n'})}, \delta_{\mathbb{Q}(\xi_{p_r^{a_r}})}) = 1$, onde $n' = \frac{n}{p_r^{a_r}}$. Pela Proposição 3.2.6, temos que $D(1, \xi_n ..., \xi_n^{\varphi(n)-1}) = \prod_{j=1}^{r} \delta^{\phi(n/p_j^{a_j})}_{\mathbb{Q}(\xi_{p_j^{a_j}})} = \delta^{\phi(p_r^{a_r})}_{\mathbb{Q}(\xi_{n'})}$ $\delta^{\phi(n')}_{\mathbb{Q}(\xi_{p_r^{a_r}})}$. Assim, pela hipótese de indução, temos que $\delta^{\phi(p_r^{a_r})}_{\mathbb{Q}(\xi_{n'})} = \frac{(-1)^{\frac{\phi(n')r-1\phi(p_r^{a_r})}{2}} (n')^{\phi(n')\phi(p_r^{a_r})}}{\prod_{j=1}^{r-1} p_j^{\frac{\phi(n')\phi(p_r^{a_r})}{p_j - 1}}} =$

$\frac{(-1)^{\frac{\phi(n)r-1}{2}}(n^{'})^{\phi(n)}}{\prod_{j=1}^{r-1} p_j^{\frac{\phi(n)}{p_j-1}}}$, e novamente pela hipótese de indução, segue que o discriminante $\delta_{\mathbb{Q}(\xi_{p_r^{a_r}})}^{\phi(n^{'})} = \frac{(-1)^{\frac{\phi(p_r^{a_r})\phi(n^{'})}{2}}(p_r^{a_r})^{\phi(n^{'})\phi(p_r^{a_r})}}{p_r^{\frac{\phi(p_r^{a_r})}{\phi(n^{'})(p_r-1)}}} = \frac{(-1)^{\frac{\phi(n)}{2}}(p_r^{a_r})^{\phi(n)}}{p_r^{\frac{\phi(n)}{p_r-1}}}$. Assim, multiplicando as duas últimas igualdades, temos que $D(1,\xi,...,\xi_n^{\varphi(n)-1}) = \frac{(-1)^{\frac{\phi(n)r}{2}}n^{\phi(n)}}{\prod_{j=1}^{r} p_j^{\frac{\phi(n)}{p_j-1}}}$, o que demonstra a proposição. ∎

Proposição 3.2.7 *Sejam $\mathbb{K} \subseteq \mathbb{K}_1$ e $\mathbb{K} \subseteq \mathbb{K}_2$ corpos de números com graus n_1 e n_2, respectivamente, tais que $\delta_{\mathbb{K}_1|\mathbb{K}}$ e $\delta_{\mathbb{K}_2|\mathbb{K}}$ sejam relativamente primos. Considere $\mathbb{L} = \mathbb{K}_1\mathbb{K}_2$. Se $\mathcal{O}_{\mathbb{K}_1}, \mathcal{O}_{\mathbb{K}_2}$ e $\mathcal{O}_{\mathbb{L}}$ são os anéis dos inteiros de $\mathbb{K}_1, \mathbb{K}_2$ e $\mathbb{L}$, respectivamente, $\{x_1, \cdots, x_{n_1}\}$ é uma base integral de $\mathbb{K}_1$, e $\{y_1, \cdots, y_{n_2}\}$ é uma base integral de $\mathbb{K}_2$, então*
1) $D(x_1y_1, \cdots, x_{n_1}y_{n_2}) = D(x_1, \cdots, x_{n_1})^{n_2} D(y_1, \cdots, y_{n_2})^{n_1}$.
2) $\{x_1y_1, \cdots, x_{n_1}y_{n_2}\}$ é uma base integral de $\mathbb{L}$.
3) $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}_1}\mathcal{O}_{\mathbb{K}_2}$.

Demonstração: 1) Observamos que se σ é um isomorfismo 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 injetora, pois $\mathbb{L} = \mathbb{K}_1\mathbb{K}_2$, e também sobrejetora pois $[\mathbb{L} : \mathbb{Q}] = n_1n_2$. Assim, $D(x_1y_1, \cdots, x_{n_1}y_{n_2}) = [\det(\sigma_i\tau_j(x_ky_l))]^2$, onde $\sigma_1, \cdots, \sigma_{n_1}$ são os isomorfismos de $\mathbb{K}_1$ e $\tau_1, \cdots, \tau_{n_2}$ são os isomorfismos de $\mathbb{K}_2$. O determinante desta matriz é o produto de Kronecker das matrizes $(\sigma_i(x_k))_{i,k=1,\cdots,n_1}$ e $(\tau_j(y_l))_{j,l=1,\cdots,n_2}$. Assim,

$$[\det(\sigma_i(x_k))]^{2n_2}[\det(\tau_j(y_l))]^{2n_1} = D(x_1, \cdots, x_{n_1})^{n_2} D(y_1, \cdots, y_{n_2})^{n_1}.$$

Portanto, $D(x_1y_1, \cdots, x_{n_1}y_{n_2}) = D(x_1, \cdots, x_{n_1})^{n_2} D(y_1, \cdots, y_{n_2})^{n_1}$. Para 2) como $\mathcal{O}_{\mathbb{K}_1}\mathcal{O}_{\mathbb{K}_2} \subseteq \mathbb{L}$ é o menor anel contendo $\mathcal{O}_{\mathbb{K}_1}$ e $\mathcal{O}_{\mathbb{K}_2}$, segue que $\mathcal{O}_{\mathbb{K}_1}\mathcal{O}_{\mathbb{K}_2} \subseteq \mathcal{O}_{\mathbb{L}}$ e assim, temos que $\mathcal{O}_{\mathbb{K}_1}\mathcal{O}_{\mathbb{K}_2}$ tem a $\mathbb{Z}$-base $\{x_1y_1, \cdots, x_{n_1}y_{n_2}\}$. Suponhamos que $\{z_1, \cdots, z_{n_1n_2}\}$ é uma base integral de $\mathcal{O}_{\mathbb{L}}$. Assim, pela Proposição 2.3.1, segue que $D(x_1y_1, \cdots, x_{n_1}y_{n_2}) = \det(a_{ij})^2 D(z_1, \cdots, z_{n_1n_2})$. Por 2) temos que

$$\delta = \langle D(x_1y_1, \cdots, x_{n_1}y_{n_2})\rangle = \langle D(x_1, \cdots, x_{n_2})\rangle^{n_1}\langle D(y_1, \cdots, y_{n_2})\rangle^{n_1} = \delta_{\mathbb{L}},$$

onde a última igualdade é dada pela Proposição 3.2.6. Assim,

$$\langle D(x_1y_1, \cdots, x_{n_1}y_{n_2})\rangle = \langle D(z_1, \cdots, z_{n_1n_2})\rangle$$

o que implica que $D(x_1y_1, \cdots, x_{n_1}y_{n_2}) = uD(z_1, \cdots, z_{n_1n_2}) = \det(a_{ij})^2 D(z_1, \cdots, z_{n_1n_2})$, onde u é a unidade de $\mathbb{Z}$. Logo, $\det(a_{ij})^2 = u$. Assim, a matriz da transformação linear tem determinante com valor absoluto igual a 1. Portanto, $\{x_1y_1, \cdots, x_{n_1}y_{n_2}\}$ é uma base integral de $\mathbb{L}$. Finalmente, 3) segue por 2) que $\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{K}_1}\mathcal{O}_{\mathbb{K}_2}$. ■

Capítulo 4

Reticulados e códigos

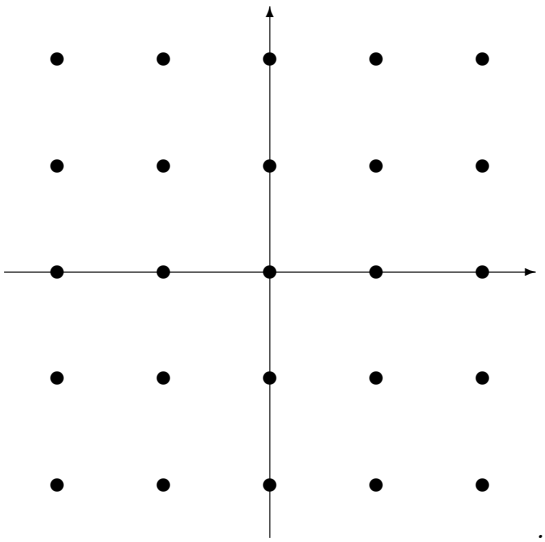
Neste capítulo, usando discriminante e diferente apresentamos um estudo sobre reticulados e códigos. Lembramos da Seção 2.6 que um reticulado é um subgrupo discreto $\Lambda \subseteq \mathbb{R}^n$ que é um $\mathbb{Z}$-módulo livre de posto finito. Inicialmente, apresentamos a idéia de Forney e depois os conceitos de reticulados, os quais são obtidos via Eva Bayer. Em seguida, introduzimos o conceito de obter reticulados rotacionados, onde podemos obter no $\mathbb{R}^n$ reticulados tão bons quantos os conhecidos. Para finalizar o capítulo, apresentamos um estudo sobre códigos lineares, álgebra dos quatérnios e introduzimos os códigos de bloco espaço-tempo. Neste capítulo usamos as seguintes referências [9], [10], [11], [12], [13], [16] e [17].

4.1 Reticulados

Nesta seção, primeiramente apresentamos o método de Forney para obtermos reticulados, depois o método de Eva Bayer e para finalizar os conceitos de Viterbo. Segundo Forney, em relação a um reticulado $\Lambda \subseteq \mathbb{R}^n$ conseguimos obter outros reticulados através dos seguintes fatos:

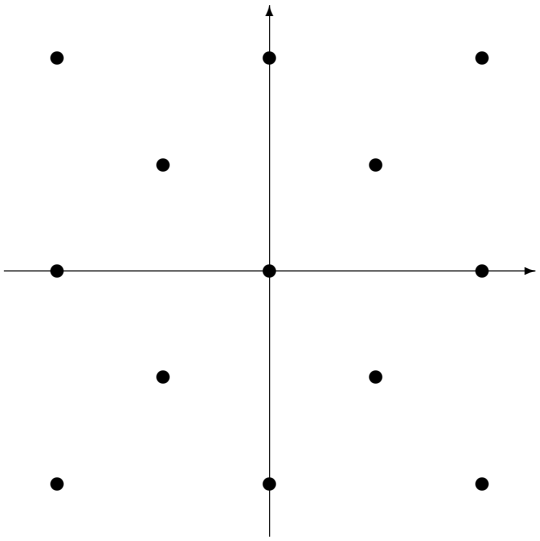
1. Se $\lambda \in \mathbb{R}$ então $\lambda\Lambda = \{\lambda x : x \in \Lambda\} \subset \mathbb{R}^n$ é um reticulado.

Exemplo 4.1.1 *Para* $2 \in \mathbb{R}$ *temos que* $2\mathbb{Z}^2 = \{2x : x \in \mathbb{Z}^2\}$ *é um reticulado*



2. Se $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ é uma transformação ortogonal então $T(\Lambda) = \{T(x) : x \in \Lambda\}$ é um reticulado.

Exemplo 4.1.2 *Seja a matriz* $T = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. *Então* $T(\mathbb{Z}^2)$ *é um reticulado.*



3. Se $m \in \mathbb{N}$, então Λ^m é um reticulado.

Definição 4.1.1 *Se um reticulado pode ser obtido a partir de outro por uma rotação, reflexão e multiplicação por escalar, dizemos que estes reticulados são equivalentes.*

Definição 4.1.2 *Seja* $\Lambda \subseteq \mathbb{R}^n$ *um reticulado. Um subreticulado* Λ' *do reticulado* Λ *é um subgrupo do grupo aditivo* Λ.

Observação 4.1.1 *Duas n-uplas são equivalentes módulo* Λ *se sua diferença é um ponto de* Λ*. Assim, a classe* $c+\Lambda$ *é o conjunto dos pontos equivalentes módulo* Λ*.*

Definição 4.1.3 *Para um subreticulado* $\Lambda^{'}$ *de um grupo* Λ*, o grupo formado pelas classes laterais de* Λ *módulo* $\Lambda^{'}$ *sob a operação* $(a+\Lambda^{'})+(b+\Lambda^{'})=(a+b)\Lambda^{'}$ *é chamado grupo quociente de* Λ *módulo* $\Lambda^{'}$ *e é denotado por* $\Lambda/\Lambda^{'}$*.*

Definição 4.1.4 *A ordem do grupo* $\Lambda/\Lambda^{'}$ *é o número das classes de equivalências e denotado por* $o\left(\Lambda/\Lambda^{'}\right)$*, também é a ordem da partição.*

Se tomarmos um elemento de cada classe de equivalência, obtemos um sistema de representantes da partição $\Lambda/\Lambda^{'}$, denotado por $\left[\Lambda/\Lambda^{'}\right]$. Assim, todo elemento de Λ pode ser escrito de modo único como a soma $\lambda=\lambda^{'}+c$, onde $c\in\left[\Lambda/\Lambda^{'}\right]$ é o representante da classe de equivalência em que λ está, e $\lambda^{'}=\lambda-c$ é um elemento de $\Lambda^{'}$, uma vez que $\lambda\equiv c(modulo\ \Lambda^{'})$. Assim, $\Lambda=\Lambda^{'}+\left[\Lambda/\Lambda^{'}\right]$ e é chamado uma classe de decomposição de Λ. Uma partição $\Lambda/\Lambda^{'}$ também induz uma classe de decomposição de qualquer classe de Λ como $c+\Lambda=c+\Lambda^{'}+\left[\Lambda/\Lambda^{'}\right]$.

Uma cadeia de partição $\Lambda/\Lambda^{'}/\Lambda^{''}/\cdots$ é uma sequência de reticulados tal que cada um é um subreticulado do anterior, ou seja, $\Lambda\supset\Lambda^{'}\supset\Lambda^{''}\supset\cdots$. Uma cadeia de partição induz uma cadeia de classes de decomposições com um termo correspondente a cada partição. Por exemplo, se $\Lambda/\Lambda^{'}/\Lambda^{''}$ é uma cadeia de partição então

$$\Lambda=\Lambda^{''}+\left[\Lambda^{'}/\Lambda^{''}\right]+\left[\Lambda/\Lambda^{'}\right],$$

o que significa que todo elemento de Λ pode ser escrito como um elemento de $\Lambda^{''}$, mais um representante de classe de $\left[\Lambda^{'}/\Lambda^{''}\right]$ e mais um representante da classe de $\left[\Lambda/\Lambda^{'}\right]$.

Exemplo 4.1.3 *A cadeia de partição* $\mathbb{Z}/2\mathbb{Z}/4\mathbb{Z}/\cdots$ *fornece uma representação binária de um inteiro m, uma vez que*

$$m=a_0+2a_1+4a_2+\cdots,$$

onde $a_i\in\{0,1\}$*, para* $i=0,1,2,\cdots$*, tal que* a_0 *representa a classe na partição* $\mathbb{Z}/2\mathbb{Z}$*,* $2a_1$ *representa a classe na partição* $2\mathbb{Z}/4\mathbb{Z}$*, e assim por diante. Assim,*

$$\mathbb{Z}=[\mathbb{Z}/2\mathbb{Z}]+[2\mathbb{Z}/4\mathbb{Z}]+[4\mathbb{Z}/8\mathbb{Z}]+\cdots.$$

Se $\Lambda\subseteq\mathbb{R}^n$ é um reticulado, temos que $\mathbb{R}^n/\Lambda$ é uma partição. Definimos uma região fundamental de Λ, P_Λ, como uma região no $\mathbb{R}^n$ que contém um e somente um ponto de cada classe de equivalência módulo Λ. Assim, P_Λ é um sistema de representantes da partição $\mathbb{R}^n/\Lambda$. Assim, $\mathbb{R}^n=\Lambda+P_\Lambda$. Geometricamente, isto é uma translações do $\mathbb{R}^n$ por translações das regiões fundamentais de Λ.

Definição 4.1.5 *O ganho de codificação fundamental $g(\Lambda)$ de um reticulado $\Lambda \subseteq \mathbb{R}^n$ é definido como*

$$g(\Lambda) = \frac{d^2_{min}(\Lambda)}{v(\Lambda)^{\frac{2}{n}}},$$

onde $d^2_{min}(\Lambda) = min\{d^2(x,y) = ||x-y||^2 : x, y \in \Lambda\}$ e $v(\Lambda)$ é o volume de Λ. Dizemos que um reticulado Λ é mais denso que um reticulado Λ' se $g(\Lambda) > g(\Lambda')$ sempre que Λ e Λ' tem a mesma dimensão. O número de Kissing é o número de elementos de Λ com norma mínima $d^2_{min}(\Lambda)$.

Na literatura, $g(\Lambda)$ é também chamado de parâmetro de Hermite, e satisfaz as seguintes propriedades:

1. $g(\Lambda)$ é invariante por escalar, ou seja, $g(r\Lambda) = g(\Lambda)$, uma vez que $d^2_{min}(r\Lambda) = r^2 d^2_{min}(\Lambda)$ e $v(r\Lambda) = r^n v(\Lambda)$.

2. $g(\Lambda)$ é invariante via uma transformação ortogonal T, ou seja, $g(T(\Lambda)) = g(\Lambda)$, uma vez que $d^2_{min}(T(\Lambda)) = |\det T|^{\frac{2}{n}} d^2_{min}(\Lambda)$ e $v(T(\Lambda)) = |\det T| v(\Lambda)$, onde $\det T$ é o determinante de T. Assim, qualquer versão de Λ tem o mesmo ganho de codificação fundamental.

3. $g(\Lambda)$ é invariante via o produto cartesiano, ou seja, $g(\Lambda^n) = g(\Lambda)$ uma vez que $d^2_{min}(\Lambda^n) = d^2_{min}(\Lambda)$ e $v(\Lambda^n) = v(\Lambda)^n$.

Exemplo 4.1.4 *Temos que $g(\mathbb{Z}^n) = 1$.*

Exemplo 4.1.5 *Temos que $T(\mathbb{Z}^2)$, onde*

$$T = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

é uma rotação de $\mathbb{Z}^2$ com $d^2_{min}(T(\mathbb{Z}^2)) = 2$. A partição $\mathbb{Z}^2/T(\mathbb{Z}^2)$ tem ordem 2 e assim $v(T(\mathbb{Z}^2)) = 2$. Portanto, $g(\mathbb{Z}^2) = 1$.

Exemplo 4.1.6 *Seja $D_4 = \{(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4 : a_i \in 2\mathbb{Z},\ i = 0, 1, 2, 3\}$. A ordem da partição $\mathbb{Z}^4/D_4$ é dois, uma vez que $\mathbb{Z}^4$ é a união de D_4 e a classe $(1,0,0,0) + D_4$. Assim, $v(D_4) = 2$ e $d^2_{min}(D_4) = 2$. Portanto, o ganho fundamental de D_4 é $g(D_4) = \frac{2}{2^{\frac{2}{4}}} = \sqrt{2}$. Assim, D_4 é mais denso que $\mathbb{Z}^4$.*

Definição 4.1.6 *Um reticulado complexo Λ é um conjunto discreto de pontos de $\mathbb{C}^n$ que forma um grupo aditivo.*

Os parâmetros $d^2_{min}(\Lambda)$, $v(\Lambda)$ e $g(\Lambda)$ são definidos de modo análogo aos reticulados reais. Mas quando trabalhamos com o produto escalar ou produto interno devemos tomar cuidado. Além disso, se $\Lambda_r \subseteq \mathbb{R}^{2n}$ é um reticulado de dimensão $2n$ e se $\Lambda_c \subseteq \mathbb{C}^n$ é um reticulado de dimensão n, então existe um isomorfismo natural entre Λ_r e Λ_c, uma vez que existe uma correspondência natural entre $\mathbb{R}^{2n}$ e $\mathbb{C}^{n+1}$.

Exemplo 4.1.7 *Um exemplo de reticulado complexo é o reticulado complexo Λ_c que corresponde ao reticulado real $\mathbb{Z}^2$ de dimensão 2. Os pontos $(a, b) \in \mathbb{Z}^2$ correspondem aos pontos $a + bi$ de $\Lambda_c = \mathbb{Z}[i]$, onde $a, b \in \mathbb{Z}$. Ou seja, Λ_c é os inteiros Gaussianos.*

Seja $\Lambda_c = \mathbb{Z}[i]$ o reticulado dos inteiros Gaussianos. Os primos de Λ_c, em ordem de norma crescente, são $1 + i, 2 \pm i, 3, \cdots$, com normas $2, 5, 9, \cdots$. Seja $p = 1 + i$ o primo de menor norma. Multiplicando Λ_c por qualquer elemento $\lambda \in \Lambda_c$ obtemos um subreticulado $\lambda\Lambda_c$ de Λ_c. Pela Proposição 2.7.2 segue que a partição $\Lambda_c/\lambda\Lambda_c$ tem ordem $||\lambda||^2$, e portanto existem $||\lambda||^2$ classes de equivalência de Λ_c módulo λ.

Exemplo 4.1.8 *Temos que $p\Lambda_c$ é um subreticulado de Λ_c de ordem $||p||^2 = 2$, ou seja, é o reticulado complexo que corresponde ao reticulado real $T(\mathbb{Z}^2)$, onde*

$$T = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Do mesmo modo que $T(\mathbb{Z}^2)$, temos que $p\Lambda_c$ consiste de todos os elementos de Λ_c com norma par, $p\Lambda_c + 1$ consiste dos elementos de Λ_c com norma ímpar, e a união de $p\Lambda_c$ e $p\Lambda_c + 1$ é Λ_c. Assim, os representantes das classes $[\Lambda_c/p\Lambda_c]$ podem ser tomadas como $\{0, 1\}$, e são isomorfas a $GF(2)$ usando a aritmética módulo p, uma vez que $2 \equiv 0 (módulo\ p)$.

Exemplo 4.1.9 *Mais geralmente, $p^e\Lambda_c$ é um subreticulado de Λ_c de ordem $||p||^{2e} = 2^e$, e de fato, é o reticulado complexo que corresponde ao reticulado real $T^e(\mathbb{Z}^2)$, onde*

$$T = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

que é igual a $2^{\frac{e}{2}}\mathbb{Z}^2$ para e par e igual a $2^{\frac{e-1}{2}}\mathbb{Z}^2$ para e ímpar. Do mesmo modo que $T^e(\mathbb{Z}^2)$, temos $p^e\Lambda_c$ consiste de todos os elementos de Λ_c cujas normas são múltiplas de 2^e, e assim $d^2_{min}(p^e\Lambda_c) = 2^e$. Assim, existe uma cadeia infinita de partições

$$\Lambda_c/p\Lambda_c/p^2\Lambda_c/p^3\Lambda_c/\cdots$$

com distâncias $1/2/4/8/16/\cdots$, *que corresponde a cadeia real*

$$\mathbb{Z}^2/T(\mathbb{Z}^2)/2\mathbb{Z}^2/2T(\mathbb{Z}^2)/4\mathbb{Z}^2/\cdots .$$

De modo análogo ao Exemplo 4.1.3, esta cadeia fornece uma representação binária complexa de um inteiro Gaussiano, ou seja, se $g \in \Lambda_c$ *então*

$$g = a_0 + pa_1 + pa_2 + \cdots ,$$

onde $a_i \in \{0, 1\}$, *para* $i = 0, 1, 2, \cdots$, *tal que* a_1 *representa a classe de* $p\Lambda_c$ *na partição* $\Lambda_c/p\Lambda_c$, pa_1 *representa a classe de* $p^2\Lambda_c$ *na partição* $p\Lambda_c/p^2\Lambda_c$, *e assim por diante. Assim,*

$$\Lambda_c = [\Lambda_c/p\Lambda_c] + \left[p\Lambda_c/p^2\Lambda_c\right] + \left[p^2\Lambda_c/p^3\Lambda_c\right] + \cdots .$$

Se Λ é um reticulado, então para cada $\lambda \in \Lambda$ e $m \in \mathbb{Z}$ temos que $m\lambda \in \Lambda$. Assim, $\lambda\Lambda$ é um subreticulado de Λ, e Λ é um módulo sobre $\mathbb{Z}$. Contudo, um reticulado complexo Λ não é necessariamente um módulo sobre o anel $\mathbb{Z}[i]$. Por exemplo, o reticulado hexagonal de dimensão 2 não é. Assim, Λ é um módulo sobre $\mathbb{Z}[i]$ se, e somente se, $\lambda \in \Lambda$ implicar que $i\lambda \in \Lambda$. Assim, se $\alpha = a + bi \in \mathbb{Z}[i]$ então $\alpha\lambda = a\lambda + b(i\lambda) \in \Lambda$, ou seja, $\alpha\Lambda$ é um reticulado de Λ, para todo $\alpha \in \mathbb{Z}[i]$. Em particular, $i\Lambda$ é um subreticulado de Λ. Mas, como $i(i\Lambda) = -\Lambda = \Lambda$ é um subreticulado de $i\Lambda$, segue que $i\Lambda = \Lambda$. Tais reticulados são chamados de $\mathbb{Z}[i]$ reticulados.

4.2 Ideais reticulados

Nesta seção, apresentamos o conceito de reticulados, obtidos via Eva Bayer. Para isso, consideramos $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de um corpo de números $\mathbb{K}$. Lembramos que Craig [14] e [15], também apresentou resultados nesses sentido.

Definição 4.2.1 *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 identidade de* $\mathbb{K}$.
2) O conjunto $F = \{x \in \mathbb{K} | \phi(x) = x\}$ *é um corpo, chamado corpo fixo da involução. Temos que* $[\mathbb{K} : \mathbb{F}] \leq 2$.

Definição 4.2.2 *Sejam* $\mathcal{I} \subseteq \mathbb{K}$ *um ideal fracionário e* $\alpha \in \mathbb{F}$ *tal que* $\alpha\mathcal{I}\phi(\mathcal{I}) \subseteq \Delta(\mathcal{O}_{\mathbb{K}}|\mathbb{Z})^{-1}$. *Um ideal reticulado é definido por* $\Lambda = (\mathcal{I}, q_\alpha)$, *onde a função* $q_\alpha : \mathcal{I} \times \mathcal{I} \longrightarrow \mathbb{Z}$, *é tal que* $q_\alpha(x, y) = Tr_{\mathbb{K}|\mathbb{Q}}(\alpha x\phi(y))$ *para todo* $x, y \in \mathcal{I}$. *Se* $\alpha = 1$, *dizemos que* $\Lambda = (\mathcal{I}, q_\alpha)$ *é obtido por uma construção traço, ou que é do tipo traço.*

Observação 4.2.1 *Em particular, se $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$ e $\phi = id$, um ideal reticulado é definido por $\Lambda = (\mathcal{I}, q_\alpha)$, onde $q_\alpha : \mathcal{I} \times \mathcal{I} \longrightarrow \mathbb{Z}$, é tal que $q_\alpha(x, y) = Tr_{\mathbb{K}|\mathbb{Q}}(\alpha xy)$ para todo $x, y \in \mathcal{I}$, onde α é totalmente positivo.*

Definição 4.2.3 *Seja $\{w_1, \cdots, w_n\}$ uma $\mathbb{Z}-$base do ideal $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$. Seja a pertubação da imersão canônica $\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$ definida como*

$$\sigma_\alpha(x) = (\sqrt{\alpha_1}\sigma_1(w_1), \cdots, \sqrt{\alpha_n}\sigma_n(w_n)),$$

onde $\alpha_i = \sigma_i(\alpha) > 0$, para $i = 1, \cdots, n$.

Observação 4.2.2 *De modo análogo, ao homorfismo canônico, temos que $\sigma_\alpha(\mathcal{I})$ é um reticulado.*

Definição 4.2.4 *Usando a pertubação da imersão canônica, a matriz geradora M do reticulado $\Lambda = \sigma_\alpha(\mathcal{I})$ é dada por*

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(w_1) & \sqrt{\alpha_2}\sigma_2(w_1) & \cdots & \sqrt{\alpha_n}\sigma_n(w_1) \\ \sqrt{\alpha_1}\sigma_1(w_2) & \sqrt{\alpha_2}\sigma_2(w_2) & \cdots & \sqrt{\alpha_n}\sigma_n(w_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sqrt{\alpha_1}\sigma_1(w_n) & \sqrt{\alpha_2}\sigma_2(w_n) & \cdots & \sqrt{\alpha_n}\sigma_n(w_n) \end{pmatrix} = (\sigma_i(w_j))_{i,j=1}^n \begin{pmatrix} \sqrt{\alpha_1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sqrt{\alpha_n} \end{pmatrix}.$$

Observação 4.2.3 *A matriz de Gram é dada por $G = MM^t = (g_{ij})_{i,j=1}^n$, onde*

$$\begin{aligned} g_{ij} &= \sum_{k=1}^{n} \sqrt{\alpha_k}\sigma_k(w_i)\sqrt{\alpha_k}\sigma_k(w_j) \\ &= \sum_{k=1}^{n} \alpha_k\sigma_k(w_iw_j) = Tr(\alpha w_i w_j). \end{aligned}$$

Como a matriz de Gram é do tipo traço, temos que a matriz geradora M define um ideal reticulado. O determinante de Λ é o determinante da matriz G, ou seja, $det(\Lambda) = det(G)$.

Proposição 4.2.1 *Se $\mathcal{I}$ é um ideal de $\mathcal{O}_{\mathbb{K}}$ e se $\Lambda = (\mathcal{I}, q_\alpha)$ é um ideal reticulado, então*

$$|\det(\Lambda)| = |D(w_1, ..., w_n)|N_{\mathbb{K}|\mathbb{Q}}(\mathcal{I})^2 N_{\mathbb{K}|\mathbb{Q}}(\alpha)$$

Demonstração: *Segue da aplicação direta da Observação 4.2.3.* ∎

Definição 4.2.5 *Seja $\Lambda = (\mathcal{I}, q_\alpha)$ um ideal reticulado. Dizemos que $\Lambda = (\mathcal{I}, q_\alpha)$ é par, se $q_\alpha(x, x)$ é um número par para todo $x \in \Lambda$.*

Sejam ξ_m uma raiz m-ésima primitiva da unidade, onde m é um inteiro positivo, e $\mathbb{K} = \mathbb{Q}(\xi_m)$ é o corpo ciclotômico correspondente. Sejam $\phi : \mathbb{K} \longrightarrow \mathbb{K}$ a conjugação complexa e $\mathbb{F} = \mathbb{Q}(\xi_m + \xi_m^{-1})$ o corpo fixo da conjugação complexa. Temos que $\mathbb{F}$ é o maior corpo totalmente real contido em $\mathbb{K}$ e que $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\xi_m]$ é o anel dos inteiros de $\mathbb{K}$.

Em cima desses reticulados, conseguimos obter reticulados equivalentes aos conhecidos.

Exemplo 4.2.1 *Sejam $\mathbb{K} = \mathbb{Q}(\xi_8)$ e $\mathcal{P} \subset \mathcal{O}_\mathbb{K}$ o único ideal primo tal que $\mathcal{P} \cap \mathbb{Z} = \langle 2 \rangle$. Seja a função $q_\alpha : \mathcal{P} \times \mathcal{P} \longrightarrow \mathbb{Z}$ definida por $q_\alpha(x, y) = \frac{1}{4} Tr_{\mathbb{K}|\mathbb{Q}}(x\phi(y))$, onde $x, y \in \mathcal{P}$. Temos pela Definição 4.2.5 que $\Lambda = (\mathcal{P}, q_\alpha)$ é um ideal reticulado par e pela Proposição 4.2.1 tem determinante 4. Portanto, $\Lambda = (\mathcal{P}, q_\alpha)$ é equivalente a D_4, uma vez que o D_4 é o único reticulado nesses parâmetros.*

Exemplo 4.2.2 *Sejam $\mathbb{K} = \mathbb{Q}(\xi_9)$ e $\mathcal{P} \subset \mathcal{O}_\mathbb{K}$ o único ideal primo tal que $\mathcal{P} \cap \mathbb{Z} = \langle 3 \rangle$. Temos que $\mathcal{P}$ é totalmente ramificado e tem norma 3. Sejam $\mathcal{I} = \mathcal{P}^{-4}$ e $q_\alpha : \mathcal{I} \times \mathcal{I} \longrightarrow \mathbb{Z}$ definida por $q_\alpha(x, y) = Tr_{\mathbb{K}|\mathbb{Q}}(x\phi(y))$, para todo $x, y \in \mathcal{I}$. Assim, pela Definição 4.2.5, temos que $\Lambda = (\mathcal{I}, q_\alpha)$ é um ideal reticulado par e pela Proposição 4.2.1 tem determinante 3. Portanto, $\Lambda = (\mathcal{I}, q_\alpha)$ é equivalente a E_6, uma vez que o E_6 é o único reticulado nesses parâmetros.*

Definição 4.2.6 *Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado. A diversidade de Λ, denotada por $div(\Lambda)$, é definida por*

$$div(\Lambda) = min\{div(x) : x \in \Lambda, x \neq 0\},$$

onde $x = (x_1, \cdots, x_n)$ e $div(x) = \#\{i : x_i \neq 0\}$.

Proposição 4.2.2 *O reticulado $\sigma_\alpha(\mathcal{I})$ tem diversidade $r_1 + r_2$.*

Demonstração: Se $x \in \mathcal{I}$, $x \neq 0$, então $\sigma_\alpha(x)$ tem no mínimo $r_1 + r_2$ coordenadas não nulas. Assim, $div(\sigma_\alpha(\mathcal{I})) \geq r_1 + r_2$. Agora, se $x = 1$ segue que $div(\sigma_\alpha(\mathcal{I})) = r_1 + r_2$. ∎

Proposição 4.2.3 *Um ideal reticulado $\Lambda = (\mathcal{I}, \varphi)$ pode ser imerso no $\mathbb{R}^n$, com*
i) diversidade n se $\mathbb{K}$ é totalmente real.
ii) diversidade $\frac{n}{2}$ se $\mathbb{K}$ é totalmente complexo.

Demonstração: Seja $\Lambda = (\mathcal{I}, \varphi)$ um ideal reticulado. Assim, $\varphi : \mathcal{I} \times \mathcal{I} \longrightarrow \mathbb{Z}$ é definido por $\varphi(x, y) = Tr_{\mathbb{L}|\mathbb{K}}(\alpha x\phi(y))$, para todo $x, y \in \mathcal{I}$, onde $\mathcal{I}$ é um ideal fracionário de $\mathcal{O}_\mathbb{K}$ e $\sigma_i(\alpha)$ é real e positivo para todo $i = 1, 2, \cdots, r_1 + r_2$. Seja $\{w_1, \cdots, w_n\}$ uma base de $\mathcal{I}$. Seja $M = (\sigma_\alpha(w_i))_{i=1,\cdots,n}$. Assim, M é uma matriz geradora de $\sigma_\alpha(\mathcal{I})$ e $MM^t = (Tr_{\mathbb{L}|\mathbb{K}}(w_i\phi(w_j)))_{i,j}$,

o que implica que $\sigma_\alpha(\mathcal{I})$ com o produto escalar usual é isomorfo a Λ. Pela Proposição 4.2.2 temos que Λ tem diversidade n se $\mathbb{K}$ é totalmente real, e diversidade $\frac{n}{2}$ se $\mathbb{K}$ é totalmente complexo. ■

Definição 4.2.7 *Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado com diversidade n. A distância produto mínima do reticulado é definida por*

$$d_{p,min}(\Lambda) = min_{x\in\Lambda} d_p(x),$$

onde $x = (x_1, \cdots, x_n)$ e $d_p(x) = \prod_{i=1}^{n} |x_i|$.

Lema 4.2.1 *Se $\mathcal{I}$ é um ideal principal de $\mathcal{O}_\mathbb{K}$, então $min_{x\neq 0\in\mathcal{I}} N(x) = N(\mathcal{I})$.*

Demonstração: Como $\mathcal{I}$ é um ideal principal, temos que $\mathcal{I} = \langle a \rangle$, com $a \in \mathcal{I}$, e $N(\mathcal{I}) = |N(a)|$. Seja $x \in \mathcal{I}$, $x \neq 0$. Assim $x = ay$ para algum $y \in \mathcal{O}_K$. Assim,

$$|N(x)| = |N(a)||N(y)| \geq N(\mathcal{I})$$

e a igualdade é verdadeira se, e somente se, $N(y) = \pm 1$. O mínimo é atingido para $x = au$, onde u é uma unidade. ■

Quando $\mathcal{I}$ é principal, temos o valor exato da distância produto mínima de um ideal reticulado $(\mathcal{I}, \varphi)$, conforme o seguinte resultado.

Teorema 4.2.1 *Seja $\mathcal{I}$ um ideal principal de $\mathcal{O}_K$. A distância produto mínima de um ideal reticulado de determinante $D = \det(\Lambda)$ definido sobre $\mathcal{I}$ é dado por*

$$d_{p,min}(\Lambda) = \sqrt{\frac{D}{D(w_1, ..., w_n)}}.$$

Demonstração: Sejam $\{w_1, \cdots, w_n\}$ uma base de $\mathcal{I}$ e $x = \sum_{i=1}^{n} \lambda_i w_i$ para $\lambda_i \in \mathbb{Z}$, com $i = 1, \cdots, n$. Da matriz da Definição 4.2.4 temos que

$$\begin{aligned}
d_p(x) &= \prod_{j=1}^{n} \left| \sum_{i=1}^{n} \lambda_i \sqrt{\alpha_j} \sigma_j(w_i) \right| \\
&= \prod_{j=1}^{n} \left| \sqrt{\alpha_j} \sigma_j \left(\sum_{i=1}^{n} \lambda_i w_i \right) \right| \\
&= \prod_{j=1}^{n} |\sqrt{\alpha_j}| \prod_{j=1}^{n} \left| \sigma_j \left(\sum_{i=1}^{n} \lambda_i w_i \right) \right| \\
&= \sqrt{N(\alpha)} \left| N \left(\sum_{i=1}^{n} \lambda_i w_i \right) \right|.
\end{aligned}$$

Pela Proposição 4.2.1 temos que $\det(\Lambda) = N(\alpha)\delta_K N(\mathcal{I})^2$. Assim $N(\alpha) = D/N(\mathcal{I})^2 D(w_1, ..., w_n)$. Pelo Lema 4.2.1, segue que

$$\begin{aligned} d_{p,min}(\Lambda) &= \sqrt{N(\alpha)} min_{x\in\mathcal{I}} N(x) \\ &= \sqrt{\frac{D}{D(w_1, ..., w_n)}} \frac{min_{x\in\mathcal{I}} N(x)}{N(\mathcal{I})} = \sqrt{\frac{D}{D(w_1, ..., w_n)}}. \end{aligned}$$

4.3 Ideais reticulados rotacionados

Nesta seção, apresentamos através dos conceitos de Viterbo, onde podemos encontrar reticulados com diversidade máxima contidos no $\mathbb{Z}^n$. Geralmente, para encontrar esses reticulados temos os seguintes critérios:

1. A versão escalar de $\mathbb{Z}^n$ é da forma $(\sqrt{c}\mathbb{Z})^n$ para algum inteiro c, ou seja, $\det(G) = \det(M)^2 = c^n$.

2. Usando a Proposição 4.2.1, deduzimos a seguinte condição necessária

$$N(\mathcal{I})^2 N(\alpha) D(w_1, ..., w_n) = c^n$$

onde c é um número inteiro. Se assumirmos $\mathcal{I} = \mathcal{O}_{\mathbb{K}}$, temos que $N(\alpha)D(w_1, ..., w_n) = c^n$.

Exemplo 4.3.1 *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{5})$. Temos que $D\left(1, \frac{1+\sqrt{5}}{2}\right) = 5$. Como $\mathbb{K}$ é totalmente real, segue que as imersões são $\sigma_1(a+b\sqrt{5}) = a+b\sqrt{5}$ e $\sigma_2(a+b\sqrt{5}) = a-b\sqrt{5}$, onde $a, b \in \mathbb{Q}$. Uma condição necessária para obter $\mathbb{Z}^2$ é encontrar um elemento α tal que $D\left(1, \frac{1+\sqrt{5}}{2}\right) N(\alpha)$=$5N(\alpha)$ $= c^2, c \in \mathbb{Z}$. Uma possibilidade de encontrar um elemento $\alpha \in \mathbb{K}$ tal que $N(\alpha) = 5$. Sejam $\alpha = 2 + \frac{1-\sqrt{5}}{2}$ e $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. A matriz geradora M do reticulado $\sigma_\alpha(\mathcal{O}_{\mathbb{K}})$ é dada por*

$$M = \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & \sqrt{\sigma_2(\alpha)} \\ \sqrt{\sigma_1(\alpha)}\sigma_1(\frac{1+\sqrt{5}}{2}) & \sqrt{\sigma_2(\alpha)}\sigma_2(\frac{1+\sqrt{5}}{2}) \end{pmatrix}.$$

A matriz $G = MM^T$ é da forma

$$G = \begin{pmatrix} \sigma_1(\alpha) + \sigma_2(\alpha) & \sigma_1(\alpha\frac{1+\sqrt{5}}{2}) + \sigma_2(\alpha\frac{1+\sqrt{5}}{2}) \\ \sigma_1(\alpha\frac{1+\sqrt{5}}{2}) + \sigma_2(\alpha\frac{1+\sqrt{5}}{2}) & \sigma_1(\alpha(\frac{1+\sqrt{5}}{2})^2) + \sigma_2(\alpha(\frac{1+\sqrt{5}}{2})^2) \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}.$$

Esta matriz mostra a versão escalar de $\mathbb{Z}^2$. Depois da normalização, temos que $\mathbb{Z}^2$ pode ser construído a partir de $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, com matriz geradora $\frac{1}{\sqrt{5}}M$. Pelo Teorema 4.2.1 a distância produto mínima deste reticulado é

$$d_{p,min}(\Lambda) = \frac{1}{\sqrt{5}}.$$

Exemplo 4.3.2 *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{2})$. Pela Proposição 2.3.2, temos que $D(1, \sqrt{2}) = 8$. Como $\mathbb{K}$ é totalmente real, segue que as imersões são $\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$ e $\sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}$, onde $a, b \in \mathbb{Q}$. Uma condição necessária para obter $\mathbb{Z}^2$ é encontrar um elemento α tal que $D(1, \sqrt{2})N(\alpha)$=$8N(\alpha) = c^2, c \in \mathbb{Z}$. Uma possibilidade é encontrar um elemento $\alpha \in \mathbb{K}$ tal que $N(\alpha) = 2$. Sejam $\alpha = \sqrt{2} - 2$ e $\{1, 1 + \sqrt{2}\}$ uma $\mathbb{Z}$-base de um ideal $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$. A matriz geradora M do reticulado $\sigma_\alpha(\mathcal{I})$ é dada por*

$$M = \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & \sqrt{\sigma_2(\alpha)} \\ \sqrt{\sigma_1(\alpha)}\sigma_1(1+\sqrt{2}) & \sqrt{\sigma_2(\alpha)}\sigma_2(1+\sqrt{2}) \end{pmatrix}.$$

A matriz $G = MM^T$ é da forma

$$G = \begin{pmatrix} \sigma_1(\alpha) + \sigma_2(\alpha) & \sigma_1(\alpha(1+\sqrt{2})) + \sigma_2(\alpha(1+\sqrt{2})) \\ \sigma_1(\alpha(1+\sqrt{2})) + \sigma_2(\alpha(1+\sqrt{2})) & \sigma_1(\alpha(1+\sqrt{2})^2) + \sigma_2(\alpha(1+\sqrt{2})^2) \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}.$$

Esta matriz mostra a versão escalar de $\mathbb{Z}^2$. Depois da normalização, temos que $\mathbb{Z}^2$ pode ser construído a partir de $\mathcal{I} \subseteq \mathcal{O}_{\mathbb{K}}$, com matriz geradora $\frac{1}{2}M$. Pelo Teorema 4.2.1 a distância produto mínima deste reticulado é

$$d_{p,min}(\Lambda) = \frac{1}{\sqrt{8}}.$$

4.4 Códigos lineares

Nesta seção, apresentamos um breve estudo sobre códigos lineares e álgebra dos quatérnios.

Definição 4.4.1 *Seja A um conjunto e n um número natural.*

- *Um* **espaço de sequências** *A^I é o conjunto de todas as sequências $c = \{c_i \mid i \in I\}$ de elementos c_i sobre A, onde I é um conjunto de índices.*
- *Um* **código** *C sobre A é qualquer subconjunto não vazio do espaço de sequências A^I.*
- *Um* **código de bloco** *C* **de comprimento** *n sobre A é qualquer subconjunto não vazio do conjunto A^n de todas as sequências $c = \{c_i \mid 1 \leq i \leq n\}$(que agora chamamos* **palavras-código***).*
- *Dados dois elementos $u, v \in A^n$, definimos a* **distância de Hamming** *entre u e v como sendo $d(u, v) = \#\{i \mid u_i \neq v_i, 1 \leq i \leq n\}$.*

Observação 4.4.1 *Se C é um código sobre um conjunto A, temos os seguintes fatos*

- *As coordenadas de uma palavra-código são chamadas de* **símbolos**.
- *Quando o conjunto de índices I é finito temos o que chamamos de* **código de bloco**. *Neste caso, a cardinalidade de I, denotada por n, é denominada* **comprimento** *do código.*
- *Quando I é infinito temos um* **código convolucional** *ou um* **código treliça**.

É conveniente que o conjunto A tenha uma estrutura algébrica que pode ser grupo, anel ou corpo, de modo que a codificação e a decodificação sejam simplificadas. Além disso, o desempenho de um código pode ser avaliado através de uma distância. Em geral, quando pensamos em distância logo lembramos o conceito de métrica que é a estrutura matemática que mais se aproxima do conceito intuitivo de medir distâncias num determinado conjunto.

Definição 4.4.2 *(Álgebra dos quatérnios) Sejam $\mathbb{K}$ um corpo, e β, γ elementos não nulos de $\mathbb{K}$. A álgebra dos quatérnios sobre $\mathbb{K}$ é o anel*

$$Q_{\beta,\gamma}(\mathbb{K}) = \{a + bi + cj + dk | a, b, c, d \in \mathbb{K}\},$$

onde a multiplicação é dada pela relação $i^2 = \beta, j^2 = \gamma, k = ij = -ji$ e a adição é termo a termo.

Definição 4.4.3 *A norma reduzida de $x = a + bi + cj + dk \in Q_{\beta,\gamma}(\mathbb{K})$ é definida como*

$$N_{red}(x) = a^2 - \beta b^2 - \gamma c^2 + \beta\gamma d^2,$$

ou seja,

$$N_{red}(x) = x\bar{x},$$

onde $\bar{x} = a - bi - cj - dk$.

Definição 4.4.4 *Dizemos que a álgebra dos quatérnios $Q_{\beta,\gamma}(\mathbb{K})$ é uma álgebra de divisão se não existem divisores de zeros em $Q_{\beta,\gamma}(\mathbb{K})$.*

Proposição 4.4.1 *Com as notações anteriores temos que $Q_{\beta,\gamma}(\mathbb{K})$ é uma álgebra de divisão se, e somente se, $N_{red}(x) \neq 0$ para todo $x \in Q^*_{\beta,\gamma}(\mathbb{K})$.*

Demonstração: Os elementos em $Q_{\beta,\gamma}(\mathbb{K})$ podem ser representados na forma matricial no $\mathbb{R}^{2\times 2}$ ou em $\mathbb{C}^{2\times 2}$. Os elementos básicos de $Q_{\beta,\gamma}(\mathbb{K})$ são representados

$$i = \begin{pmatrix} \sqrt{\beta} & 0 \\ 0 & -\sqrt{\beta} \end{pmatrix} j = \begin{pmatrix} 0 & 1 \\ \gamma & 0 \end{pmatrix} k = ij = \begin{pmatrix} 0 & \sqrt{\beta} \\ -\gamma\sqrt{\beta} & 0 \end{pmatrix}.$$

Notemos que um elemento de $Q_{\beta,\gamma}(\mathbb{K})$ é dado por

$$x = a + bi + cj + dk = \begin{pmatrix} a + b\sqrt{\beta} & c + d\sqrt{\beta} \\ \gamma(c - d\sqrt{\beta}) & a - b\sqrt{\beta} \end{pmatrix}$$

e o determinante é

$$\det(x) = a^2 - \beta b^2 - \gamma c^2 + \beta\gamma d^2 = N_{red}(x).$$

Assim, se $N_{red}(x) \neq 0$ segue que $\det(x) \neq 0$. Portanto, x é inversível se, e somente se, x não é divisor de zero. ■

Observação 4.4.2 *Sejam $\mathbb{K} = \mathbb{Q}(i)$, $\beta = i$ e $\gamma \in \mathbb{Q}(i)$. Seja $\theta = exp\left(\frac{i\pi}{4}\right) = \sqrt{\beta}$. Então, os elementos de $Q_{\beta,\gamma}(\mathbb{K})$ são dados por*

$$\begin{pmatrix} a + b\theta & c + d\theta \\ \gamma(c - d\theta) & a - b\theta \end{pmatrix},$$

com $a, b, c, d \in \mathbb{Q}(i)$.

4.5 Código de bloco espaço-tempo

Seja S uma constelação n dimensional contendo $2^m = M$ sinais. A cada m-upla de bits de entrada, é associado um sinal $x = (x_1, \cdots, x_n) \in M$. Quando x é enviado pelo canal gaussiano, a ação do ruído faz com que o sinal recebido seja

$$r = x + \beta,$$

onde $\beta = (\beta_1, \cdots, \beta_n)$ é um processo aleatório gaussiano. Quando um sinal x é transmitido através de um canal com ruído Rayleigh com desvanecimento, o sinal recebido é

$$r = \alpha * x + \beta,$$

onde $\beta = (\beta_1, \cdots, \beta_n)$ é um vetor ruído, cujas componentes são variáveis aleatórias independentes com distribuição gaussiana, média 0 e variância N_0, $\alpha = (\alpha_1, \cdots, \alpha_n)$ são os coeficientes de desvanecimento com segundo momento unitário e * representa o produto componente a componente. Os M sinais são escolhidos de uma constelação finita S, que é obtida a partir de um reticulado Λ. Em particular, os pontos da constelação são escolhidos nas primeiras camadas do reticulado, de forma que o conjunto de sinais se aproxima da forma esférica. A eficiência espectral é medida em número de bits por duas dimensões,

$$\eta = \frac{2m}{n}$$

e a relação sinal ruído é dado por

$$SNR = \frac{E_b}{N_0},$$

onde E_b é a energia média por bit e $N_0/2$ é a densidade espectral de potência. Um demodulador de máxima verossimilhança deverá minimizar a métrica

$$m(x|r) = \sum_{i=1}^{n} |r_i - x_i|^2$$

para o canal gaussiano, e

$$m(x|r, \alpha) = \sum_{i=1}^{n} |r_i - \alpha_i x_i|^2,$$

para o canal Rayleigh com desvanecimento. Depois disto, é feita uma estimativa $\hat{x}$ do sinal enviado x e a suposta sequência de bits enviada é obtida. Dados x e $y \in \Lambda$, denotaremos por $P(x \longrightarrow y)$ a probabilidade de que quando x é transmitido, o ponto y seja detectado, ou seja, que o ponto recebido esteja mais próxima de y do que de x, na respectiva métrica. A probabilidade de erro na constelação S tomada a partir de Λ é dada por

$$P_e(S) \leq P_e(\Lambda) \leq \sum_{x \neq y} P(x \longrightarrow y).$$

Em cada tipo de canal, a expressão acima possibilita a obtenção de fórmula explícita para a probabilidade de erro, conforme veremos nos itens que seguem.

- **O canal gaussiano:** Por [12], a probabilidade de erro de símbolo é limitada superiormente por

  $$P_e \leq \frac{\tau}{2} erfc\left(\frac{d_{min}/2}{\sqrt{2N_0}}\right),$$

  onde τ é o número de vizinhos e d_{min} é a menor distância na constelação. O ganho de codificação é dado por

  $$\gamma = \frac{d_{min}^2}{v(\Lambda)^{2/n}},$$

  e representa o ganho de potência com relação a $\mathbb{Z}^n$, podendo ser obtido a partir da densidade de centro por

  $$\delta = (\gamma/4)^{n/2}.$$

- **O canal Rayleigh com Desvanecimento:** Para o canal Rayleigh com desvanecimento, a probabilidade de erro de símbolo par a par com alta relação sinal-ruído satisfaz, por [16],

  $$P_e(S) \leq \frac{1}{2} \prod_{x_i \neq y_i} \frac{1}{\frac{(x_i - y_i)^2}{8N_0}} = \frac{1}{2} \frac{1}{\left(\frac{\eta E_b}{8N_0}\right)^l d_p^l(x, y)^2},$$

onde E_b é a energia média por bit, l é a diversidade, $\eta = \dfrac{2m}{n}$ é a eficiência espectral e $d_p^2(x,y)$ é a distância l-produto normalizada de x a y, dada por

$$d_p^2(x,y) = \frac{\prod_{x_i \neq y_i} (x_i - y_i)^2}{(\frac{E}{n})^l},$$

onde $E = E(||x||^2)$ é a energia média por ponto da constelação.

Como o interesse é pelo caso $l = n$, omitiremos a notação l.

Seja

$$K_s = \sum_{x \in S} \frac{1}{d_p^2(x,0)}.$$

De [16], a probabilidade de erro de símbolo satisfaz

$$P_e(S) \leq \frac{1}{2} \frac{K_s}{\left(\dfrac{\eta E_b}{8N_0}\right)^n}.$$

Para minimizar a probabilidade de erro, precisamos:

• maximizar a diversidade;

• minimizar K_S, que equivale a simultaneamente maximizar a distância produto mínima e minimizar o número de vizinhos produto.

Seja um vetor informação $\mathbf{s} = (s_1, s_2, \cdots, s_q)$, onde $q \geq 1$ e s_j, para $j = 1, 2, \cdots, q$, pertence a uma dada constelação.

Definição 4.5.1 *Um código de bloco espaço-tempo (ST) associa cada vetor informação* $\mathbf{s}$ *a uma matriz* $T \times M$*, que denotamos por* $\mathbf{X}(\mathbf{s})$.

Para atingir altas eficiências num sistema de transmissão de dados necessitamos de múltiplas antenas no transmissor e no receptor. Neste caso, o sinal recebido é dado por

$$Y_{T \times N} = X_{T \times M} H_{M \times N} + W_{T \times N},$$

onde X é a palavra transmitida, H é a matriz canal (conhecida pelo receptor), W o ruído Gaussiano, M é o número de antenas transmissoras, N é o número de antenas receptoras e T é o comprimento da palavra código.

Definição 4.5.2 *Seja* $\mathcal{C}$ *um código de bloco ST. O determinante mínimo do código* $\mathcal{C}$ *é definido como*

$$\mathcal{G}_{min} = min_{X \in \mathcal{C}, X \neq 0} det(X^t X),$$

onde X^t *indica a transposta conjugada da matriz* X.

Na tentativa de minimizar a probabilidade de erro de que $\mathbf{s_2}$ seja recebido dado que $\mathbf{s}_1 \neq \mathbf{s}_2$ foi enviado, temos os seguintes critérios:

- Critério do posto. O posto mínimo r de $X(\mathbf{s}_1) - X(\mathbf{s}_2)$ tomados sobre todos os pares $(\mathbf{s}_1, \mathbf{s}_2)$ é o ganho de diversidade e será maximizado.
- Critério do determinante. Se $\mathbf{A} = X(\mathbf{s}_1) - X(\mathbf{s}_2)$, então o mínimo de $(\prod_{j=1}^{r} \lambda_j)^{1/r}$, tomado sobre todos os pares de palavras códigos distintas, é o ganho de codificação e deve ser maximizada, onde λ_j, para $j = 1, 2, \cdots, r$ são autovalores não nulos da matriz $\mathbf{A}\mathbf{A}^t$, onde $\mathbf{A}^t$ denota a matriz transposta conjugada de $\mathbf{A}$.

Exemplo 4.5.1 *O código de Alamouti dado por*

$$\mathbf{X} = \begin{pmatrix} s_1 & -s_2^* \\ s_2 & s_1^* \end{pmatrix},$$

onde s_1 e s_2 são símbolos de informação complexos, e s^* denota a conjugação complexa de s. Este código satisfaz os critérios dados acima, e seu ganho de codificação é dado por

$$\mathcal{G}_A = min_{(s_1,s_2)\neq(0,0)}(|\ s_1\ |^2 + |\ s_2\ |^2) > 0.$$

4.5.1 Código $B_{2,\phi}$

Nesta seção apresentamos código de bloco espaço tempo $B_{2,\phi}$, onde este código satisfaz o critério de posto e determinante. Seja o código bloco ST definido por

$$B_{2,\phi} = \frac{1}{\sqrt{2}} \begin{pmatrix} s_1 + s_2\phi & \theta(s_3 + s_4\phi) \\ \theta(s_3 - s_4\phi) & s_1 - s_2\phi \end{pmatrix},$$

onde $\theta^2 = \phi$, $\phi = e^{i\lambda}$, e λ é um parâmetro real para ser otimizado. Suponha que o vetor informação $\mathbf{s} = (s_1, \cdots, s_4)^t$ pertence a uma constelação 4-dimensional C contida em $\mathbb{Z}[i]^4$. Para este código temos que o ganho de codificação é dado por

$$\begin{aligned} \mathcal{G}_B(\phi) &= inf(\det(B_{2,\phi}B_{2,\phi}^t))^{\frac{1}{2}} \\ &= \tfrac{1}{2}(inf|s_1^2 - s_3^2\phi - s_2^2\phi^2 + s_4^2\phi^3|) \\ &= \tfrac{1}{2}(inf|\phi^t s\ |), \end{aligned}$$

onde $\mathbf{s} \neq (0,0,0,0)^t \in \mathbb{Z}[i]^4$, $\mathbf{s}\ = (s_1^2, -s_3^2, -s_2^2, s_4^2)^t$ e $\phi = (1, \phi, \phi^2, \phi^3)^t$.

Sobre uma constelação finita $\mathcal{C} \subset \mathbb{Z}[i]^4$, o ganho de codificação de $B_{2,\phi}$ é dado por

$$\mathcal{G}_B^C(\phi) = \frac{1}{2}(min|\phi^t s\ |) \geq \mathcal{G}_B(\phi). \tag{4.1}$$

A desigualdade $\mathcal{G}_B^C(\phi) \geq \mathcal{G}_B(\phi)$ é verdadeira para $C \subset \mathbb{Z}[i]^4$. Nosso objetivo agora é a escolha de ϕ tal que o código $B_{2,\phi}$ tenha diversidade máxima transmitida para todas as constelações contidas em $\mathbb{Z}[i]^4$.

Proposição 4.5.1 *Se ϕ é um número algébrico de grau 4 sobre $\mathbb{Q}[i]$ então a diversidade transmitida é máxima para todas as constelações $\mathcal{C} \subseteq \mathbb{Z}[i]^4$.*

Demonstração: Se ϕ é um número algébrico de grau 4 sobre $\mathbb{Q}[i]$, então $\{1, \phi, \phi^2, \phi^3\}$ é uma base de $\mathbb{Q}[i, \phi]$, e portanto, o conjunto é linearmente independente, ou seja, se

$$\sum_{j=0}^{3} a_j \phi^j = 0,$$

para $a_j \in \mathbb{Q}[i], j = 0, \cdots, 3$, então $a_0 = a_1 = a_2 = a_3 = 0$. Assim, $\mathcal{G}_B^C(\phi) \neq 0$, para todas as constelações contidas em $\mathbb{Z}[i]^4$. ∎

Proposição 4.5.2 *Se ϕ é um número algébrico de grau menor que 2 sobre $\mathbb{Q}[i]$ então existe uma constelação $\mathcal{C} \subseteq \mathbb{Z}[i]^4$, tal que $\mathcal{G}_B^C(\phi) = 0$*

Demonstração: Se o grau de ϕ é menor que 2, então existe um polinômio de grau 1 sobre $\mathbb{Q}[i]$, onde ϕ é uma raiz. Seja

$$p(x) = x + \frac{p}{q} \in \mathbb{Q}[ix]$$

tal polinômio. Então $\phi = -\frac{p}{q}$, e assim, $\phi^2 = \frac{p^2}{q^2}$. Seja a constelação finita $C \subset \mathbb{Z}[i]^4$ que contém dois vetores $\mathbf{s}_1 = (p, q, 0, 0) \neq \mathbf{s}_2 = (-p, -q, 0, 0)$ tal que $\frac{1}{2}(\mathbf{s}_1 - \mathbf{s}_2) = (p, q, 0, 0)^t$. Substituindo, na equação (4.1) obtemos $\mathcal{G}_B^C(\phi) \leq |p^2 - q^2\phi^2| = 0$. ∎

Exemplo 4.5.2 *Sejam $\phi = 1$ e $\mathcal{C}$ uma constelação $4 - QAM^4$ que contém os vetores*

$$\mathbf{s}_1 = (1+i, 1+i, 1+i, 1+i)^t \quad e \quad \mathbf{s}_2 = (-1+i, -1+i, 1+i, 1+i)^t.$$

Substituindo

$$\mathbf{s} = \left(\frac{1}{2}\right)(s_1 - s_2) = (1, 1, 0, 0)^t$$

na equação (4.1) obtemos $\mathcal{G}_B^C(\phi) \leq |1 - \phi^2| = 0$.

Proposição 4.5.3 *Se ϕ é um número algébrico de grau 2 sobre $\mathbb{Q}[i]$ e $\phi^2 \in \mathbb{Q}[i]$ então a diversidade transmitida é máxima sobre todas as constelações $\mathcal{C} \subseteq \mathbb{Z}[i]^4$.*

Demonstração: Seja $\mathbf{s} \neq (0,0,0,0)^t \in \mathbb{Z}[i]^4$ tal que

$$\tilde{\mathbf{s}}^t\phi = 0 = s_1^2 - s_3^2\phi - s_2^2\phi^2 + s_4^2\phi^3 = (s_1^2 - s_2^2\phi^2) - \phi(s_3^2 - s_4^2\phi^2).$$

Como $\{1, \phi\}$ é linearmente independente sobre $\mathbb{Q}[i]$ e como $\phi^2 \in \mathbb{Q}[i]$, segue que

$$s_1^2 - s_2^2\phi^2 = 0 \text{ e } s_3^2 - s_4^2\phi^2 = 0.$$

Como ϕ tem grau maior que 1, segue que ϕ^2 não é um quadrado em $\mathbb{Q}[i]$, ou seja, não existe $z_1z_2 \in \mathbb{Q}[i]$ tal que $\phi^2 = z_1^2z_2^2$. Assim $s_1^2 = s_2^2 = s_3^2 = s_4^2 = 0$ e portanto, $\mathbf{s} = (0,0,0,0)^t$. ∎

Exemplo 4.5.3 *Seja $\phi = e^{\frac{i\pi}{4}}$ de grau 2 sobre $\mathbb{Q}[i]$. Temos que $\phi^2 = i \in \mathbb{Q}[i]$, e não é um quadrado em $\mathbb{Q}[i]$, pois $\sqrt{i} = \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}$ não pertence a $\mathbb{Q}[i]$. Assim, pela Proposição 4.5.3, segue que $B_{2,\phi}$ tem diversidade máxima transmitida sobre todas as constelações contidas em $\mathbb{Z}[i]^4$.*

4.5.2 Código de Ouro

Nesta subseção apresentamos o código de ouro. Este é um código de bloco espaço tempo relacionado com o número de ouro $\frac{1+\sqrt{5}}{2}$. Seja $\mathbb{K} = \mathbb{Q}(i,\theta)$ uma extensão quadrática de $\mathbb{Q}(i)$. O conjunto das matrizes da forma

$$\mathcal{C}_\infty = \left\{ X = \begin{pmatrix} a+b\theta & c+d\theta \\ \gamma(c+d\bar{\theta}) & a+b\bar{\theta} \end{pmatrix} : a,b,c,d \in \mathbb{Z}[i],\ \gamma \in \mathbb{C} \right\},$$

onde $\bar{\theta}$ é o conjugado de θ sobre $\mathbb{Q}(i)$, é definido como um código linear infinito. Se $S \subseteq \mathbb{Z}[i]$ é uma constelação finita, temos que

$$\mathcal{C} = \left\{ X = \begin{pmatrix} a+b\theta & c+d\theta \\ \gamma(c+d\bar{\theta}) & a+b\bar{\theta} \end{pmatrix} : a,b,c,d \in S, \right\}.$$

é um código finito. O determinante mínimo de $\mathcal{C}_\infty$ é definido como

$$\mathcal{G}_{min}(\mathcal{C}_\infty) = min_{X \in \mathcal{C}_\infty, X \neq 0} |\det(X)|^2$$

e o determinante mínimo do código finito $\mathcal{C}$ como

$$\mathcal{G}_{min}(C) = min_{X_1, X_2 \in \mathcal{C}, X_1 \neq X_2} |\det(X_1 - X_2)|^2 \geq 4\mathcal{G}_{min}(\mathcal{C}_\infty).$$

Considerando $\theta = \dfrac{1+\sqrt{5}}{2}$ (número de ouro) temos que $\mathbb{K} = \mathbb{Q}(i,\sqrt{5}) = \{a + b\theta : a,b \in \mathbb{Q}(i)\}$ é uma extensão quadrática de $\mathbb{Q}(i)$, sendo $m(x) = x^2 - x - 1$ o polinômio minimal de θ. As

raízes de $m(x)$ são θ e $\overline{\theta} = \dfrac{1-\sqrt{5}}{2}$. Seja $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[i][\theta]$ o anel dos inteiros de $\mathbb{K}$ com base integral $B_{\mathbb{K}} = \{1, \theta\}$. A norma de $z = a + b\theta \in \mathcal{O}_{\mathbb{K}}$, com $a, b \in \mathbb{Z}[i]$, é definido como

$$N_{\mathbb{K}|\mathbb{Q}(i)}(z) = (a + b\theta)(a + b\overline{\theta}) = a^2 + ab - b^2 \in \mathbb{Z}[i].$$

Seja $\mathbb{L} = \{a + bi + c\theta + di\theta : a, b, c, d \in \mathbb{Q}\}$. Temos que $r_1 = 0$, $r_2 = 2$, e que $B_{\mathbb{L}} = \{1, i, \theta, i\theta\}$ é uma base integral de $\mathbb{L}$. O discriminante de $\mathbb{K}$ é $\delta_{\mathbb{K}} = 5$ e o discriminante de $\mathbb{L}$ é $\delta_{\mathbb{L}} = 2^4 5^2$.

Referências Bibliográficas

[1] **Samuel, P.** "*Algebraic theory of numbers.*" Paris, Hermana 1967.

[2] **Ribenboim, P.** "*Algebraic numbers.*" Wiley - Interscience, 1972.

[3] **Ribeiro, A.C.** "*Reticulados sobre corpos de números.*", 2003, f.84. Dissertação de Mestrado, IBILCE - UNESP, São José do Rio Preto, 2003.

[4] **Endler, O.** "*Teoria dos números algébricos.*" Rio de Janeiro, IMPA, 1986.

[5] **Stewart, I., Tall, D.** "*Algebric number theory.*" Chapman & New York, Hall1987.

[6] **Simonato, A. L.** "*Reticulados em corpos ciclotômicos.*", 2000, f. 82. Dissertação de Mestrado, IBILCE - UNESP, São José do Rio Preto, 2000.

[7] **Rodrigues, T. M.** "*Cúbicas galoisianas.*", Dissertação de Mestrado, IBILCE - UNESP, São José do Rio Preto, 2003.

[8] **Mollin, R.A.** "*Algebraic number theory.*" University of Calgary, Alberto Canada, 2003.

[9] **Forney Jr., G.D.** "*Part I: Introduction and geometrical classification.*"IEEE Trans. Inform. Theory, Vol. 34, N. 5, September 1988.

[10] **Viterbo, E.**"*Algebraic number theory and its application to code design for Rayleigh fading channels.*" Notas, August 2004.

[11] **Bayer, E.F.**"*Lattices and number fields.*"Contemporary Mathematics, Vol.241, 1999.

[12] **Conway, J.H., Sloane, N.J.A.** "*Sphere packing, lattices and groups.*" Springer-Verlag, 1988.

[13] **Bayer, E.F., Oggier, F. e Viterbo, E.** "*New algebraic constructions of rotated $\mathbb{Z}^n$-lattice. Constellations for the rayleigh fading channel.*" IEEE Trans. Inform. Theory, Vol. 50, N. 4, April 2004.

[14] **Craig, M.** "*Extreme forms and cyclotomy.*" Mathematika, Vol.25, pp 44-56, 1978.

[15] **Craig, M.** "*A cyclotomic construction of Leech's lattice.*" Mathematika, Vol.25, pp 236-241, 1978.

[16] **Boutros, J., Viterbo, E., Rastello, C. e Belfiori, J.C.** "*Good lattice constellations for both rayleigh fading and gaussian channels.*" IEEE Trans. Inform. Theory, Vol.42, N.2,pp 502-517, March 1996.

[17] **Damen, M.O., Tewfik, A. e Belfiore, J.C.** "*A constructions of a space-time code based on number theory.* " IEEE Trans. Inform. Theory, Vol.49, N.5,pp. 1037-1113, May 2003.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo