Universidade Estadual Paulista

Câmpus de São José do Rio Preto

Instituto de Biociências, Letras e Ciências Exatas

Teorema de Kronecker-Weber e Aplicações

Ana Cláudia Machado Mendonça

Orientador: Prof. Dr. Antonio Aparecido de Andrade

São José do Rio Preto

2012

Ana Cláudia Machado Mendonça

Teorema de Kronecker-Weber e aplicações

Dissertação apresentada para obtenção do título de Mestre em Matemática, junto ao Programa de Pós Graduação em Matemática do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus São José do Rio Preto.

Orientador: Prof. Dr. Antonio Aparecido de Andrade

São José do Rio Preto

2012

Mendonça, Ana Cláudia Machado.

Teorema de Kronecker-Weber e aplicações / Ana Cláudia Machado Mendonça. - São José do Rio Preto : [s.n.], 2012.

111 f. ; 30 cm.

Orientador: Antonio Aparecido de Andrade

Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Biociências, Letras e Ciências Exatas

1. Álgebra. 2. Teoria dos números algébricos. 3. Corpos ciclotômicos. 4. Corpos de números abelianos. 5. Ramificação de ideais. I. Andrade, Antonio Aparecido de. II. Universidade Estadual Paulista, Instituto de Biociências, Letras e Ciências Exatas. III. Título.

CDU - 511.23

Ficha catalográfica elaborada pela Biblioteca do IBILCE

Campus de São José do Rio Preto - UNESP

Ana Cláudia Machado Mendonça

Teorema de Kronecker-Weber e aplicações

Dissertação apresentada para obtenção do título de Mestre em Matemática, junto ao Programa de Pós Graduação em Matemática do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus São José do Rio Preto.

BANCA EXAMINADORA

Prof. Dr. Antonio Aparecido de Andrade
Professor Doutor - IBILCE - UNESP
Orientador

Prof. Dr. Clotilzio Moreira dos Santos
Professor Doutor - IBILCE - UNESP

Prof. Dr. Edson Donizete de Carvalho
Professor Doutor - FEIS - UNESP

São José do Rio Preto, 24 de fevereiro de 2012.

Aos meus pais,

aos meus irmãos e

em especial ao meu esposo

dedico.

Agradecimentos

Ao concluir este trabalho, agradeço:

Primeiramente à Deus.

Ao meu esposo Ederson pelo amor, companheirismo, amizade e carinho nos momentos em que mais precisei.

Aos meus pais, pelo incentivo ao estudo.

Ao meu orientador, Prof. Dr. Antonio Aparecido de Andrade, pela paciência, pelos conselhos e pela confiança ao designar a mim este trabalho.

Aos meus colegas de pós-graduação Glauce, Amanda, Érica, André, Andréa, Wanderson entre outros, pelos momentos de alegria e ajuda de estudos.

À banca examinadora: Prof. Dr. Clotilzio Moreira dos Santos (IBILCE - UNESP) e Prof. Dr. Edson Donizete de Carvalho (FEIS - UNESP).

À CAPES, pelo apoio financeiro.

A todos que de alguma forma contribuiram para a realização deste trabalho.

“Problemas não são obstáculos,
mas oportunidades ímpares
de superação e evolução.”
(Maurício Rodrigues de Morais)

Resumo

O objetivo deste trabalho é demonstrar o Teorema de Kronecker-Weber de uma forma mais elementar, usando o artigo "An Elementary Proof of the Kronecker-Weber Theorem". O trabalho traz como aplicação uma fórmula para o cálculo do condutor de um corpo de números abeliano.

Palavras chave: corpos ciclotômicos, corpos de números abelianos, ramificação de ideais, condutor.

Abstract

The objective of this work is to demonstrate the Kronecker-Weber Theorem in a form more elementary, using article "An Elementary Proof of the Kronecker-Weber Theorem". Application as the work gives a formula for calculating the conductor of a field of numbers abelian.

Keywords: ***cyclotomic fields, fields of numbers abelian, ramification of ideals, conductor.***

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 da matriz A

(a_{ij}): matriz

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

$A[x]$: anel de polinômios com coeficientes em A

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

$\#X = card(X)$: cardinalidade do conjunto X

$car(\mathbb{K})$: característica do corpo $\mathbb{K}$

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

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

$min_{\mathbb{K}}\alpha$: polinômio minimal de α sobre $\mathbb{K}$

$gr(p(x))$: grau do polinômio $p(x)$

$Ker(f)$: núcleo da aplicação f

$\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{m}$: ideais

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

$\mathfrak{P}$, $\mathfrak{B}$, $\mathfrak{M}$: ideais de $\mathcal{O}_{\mathbb{L}}$

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

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

$\zeta_n = e^{\frac{2\pi i}{n}} = cos\frac{2\pi}{n} + isen\frac{2\pi}{n}$: raiz n-ésima da unidade

U_n: grupo das raízes n-ésimas da unidade

$\mathbb{K}^*$: grupo multiplicativo dos elementos inversíveis de $\mathbb{K}$

$\mathfrak{D}_{\mathbb{K}}$: ideal gerado pelo discriminante de $\mathbb{K}$

M^*: codiferente do conjunto M

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

$v(x)$: valorização de x

$e(\mathfrak{P}|\mathfrak{p})$: índice de ramificação de $\mathfrak{P}$ sobre $\mathfrak{p}$

$f(\mathfrak{P}|\mathfrak{p})$: grau de inércia de $\mathfrak{P}$ sobre $\mathfrak{p}$

$g(\mathfrak{P}|\mathfrak{p})$: números de ideais primos de $\mathcal{O}_{\mathbb{L}}$ acima de $\mathfrak{p}$

$Z(\mathfrak{P}|\mathfrak{p})$: grupo de decomposição de $\mathfrak{P}$

$T(\mathfrak{P}|\mathfrak{p})$: grupo de inércia de $\mathfrak{P}$

$V_j(\mathfrak{P}|\mathfrak{p})$: j-ésimo grupo de ramificação de $\mathfrak{P}$

$\mathbb{K}_H$: corpo fixo do grupo H

Sumário

Introdução

Um resultado conhecido da teoria de corpos é que toda extensão ciclotômica $\mathbb{Q}(\zeta_n)$ de $\mathbb{Q}$ é abeliana, pois $Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \simeq \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$ que é abeliano para qualquer $n \in \mathbb{N}$. O Teorema de Kronecker-Weber garante que toda extensão abeliana finita $\mathbb{K}$ de $\mathbb{Q}$ está contida em um corpo ciclotômico, ou seja, $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$, para algum $n \in \mathbb{N}$. Assim, o estudo de extensões abelianas finitas de $\mathbb{Q}$ é reduzido ao estudo de subcorpos de corpos ciclotômicos.

O Teorema de Kronecker-Weber foi apresentado por Leopold Kronecker em 1853, porém a prova estava incompleta principalmente no caso em que a extensão tem grau uma potência de 2. Em 1886, Heinrich Martin Weber apresentou o que até então seria a prova completa do Teorema de Kronecker-Weber. Mas em 1896, David Hilbert encontrou erros na demonstração de Weber e conseguiu provar completamente o Teorema de Kronecker-Weber usando teoria da ramificação.

Neste trabalho apresentamos a demonstração do Teorema de Kronecker-Weber baseada na teoria da ramificação apresentada em [1]. Existem outras demonstrações deste teorema usando a teoria de classes de corpos e a teoria da localização, as quais podem ser encontradas em [2] e [3], respectivamente.

A teoria da ramificação exige um conhecimento prévio da teoria algébrica dos números. O Capítulo 1 deste trabalho traz alguns resultados importantes de teoria algébrica dos números, para que no Capítulo 2, a teoria da ramificação seja apresentada ao leitor com mais clareza.

Apesar de garantir que todo corpo de números abeliano $\mathbb{K}$ é um subcorpo de um corpo ciclotômico $\mathbb{Q}(\zeta_n)$, o teorema de Kronecker-Weber não apresenta explicitamente a

fórmula para o cálculo de n, o qual é chamado de condutor de $\mathbb{K}$ se for o menor com esta propriedade. A Seção 3.3, tem o objetivo de ajudar no cálculo do condutor de um corpo de números abeliano. Em [4] é possível ver um estudo detalhado do cálculo deste condutor. O condutor de uma extensão abeliana é muito útil para o cálculo do discriminante de um corpo de números abeliano, que pode ser encontrado em [5].

Os anéis considerados neste trabalho são anéis comutativos com unidade.

Capítulo 1

Resultados básicos de teoria algébrica dos números

Neste capítulo abordamos alguns conceitos básicos da teoria algébrica dos números necessários para o entendimento e desenvolvimento dos próximos capítulos. Os objetivos principais deste capítulo são definir e estudar módulos Noetherianos, anel de inteiros, norma, traço e discriminante. Além disso, mostrar que todo grupo abeliano finito é produto de grupos ciclícos e também que o anel de inteiros é um anel integralmente fechado, Noetheriano e um módulo finitamente gerado. A última seção traz resultados importantes sobre corpos quadráticos e ciclotômicos que serão úteis para a demonstração do Teorema de Kronecker-Weber.

1.1 Módulos

Vemos nesta seção que o conceito de módulo sobre um anel é o mesmo de um espaço vetorial sobre um corpo. Porém, alguns resultados sobre módulos merecem um pouco mais de cuidado. O Teorema Fundamental de Grupos Abelianos Finitos é o principal resultado desta seção. As principais referências desta seção são [6], [7] e [8].

Definição 1.1 *Seja A um anel. Dizemos que um conjunto não vazio M é um A-módulo se:*

i) $(M,+)$ *é um grupo abeliano;*

ii) Existe uma aplicação $\varphi : A \times M \longrightarrow M$ *dada por* $\varphi(a,x) = ax$*, que satisfaz*

a) $a(x+y) = ax + ay$*;*

b) $(a+b)x = ax + bx$*;*

c) $(ab)x = a(bx)$*;*

d) $1x = x$*,*

para todo $a,\ b \in A$ *e* $x,\ y \in M$*.*

Exemplo 1.1 *Todo anel* A *é um* A*-módulo, todo espaço vetorial* V *sobre um corpo* $\mathbb{K}$ *é um* $\mathbb{K}$*-módulo e todo grupo abeliano é um* $\mathbb{Z}$*-módulo.*

Definição 1.2 *Um subconjunto não vazio* N *de um* A*-módulo* M *é um* A*-submódulo de* M *se* N *é um subgrupo de* $(M,+)$ *e* $an \in N$*, para todo* $a \in A$ *e* $n \in N$*. Se* M *é um* A*-módulo, tem-se que* $(M,+)$ *é um grupo abeliano. Assim, se* N *é um* A*-submódulo de* M*, então* N *é um subgrupo normal de* M*. Logo, está definido o grupo quociente de* M *por* N*, e denotado por* $\dfrac{M}{N}$*, onde a soma de* $\overline{x} = x + N$ *e* $\overline{y} = y + N$ *é dada por* $\overline{x} + \overline{y} = (x+y) + N \in \dfrac{M}{N}$*. A multiplicação de* $\overline{x} \in \dfrac{M}{N}$ *por* $a \in A$ *é definida por* $a\overline{x} = a(x+N) = ax + N \in \dfrac{M}{N}$*. Com essas duas operações tem-se que* $\dfrac{M}{N}$ *é um* A*-módulo, chamado módulo quociente de* M *por* N*.*

Definição 1.3 *Sejam* M *e* M' *A-módulos. Uma aplicação* $f : M \longrightarrow M'$ *tal que*

a) $f(x+y) = f(x) + f(y)$*;*

b) $f(ax) = af(x)$*;*

para todo $x,\ y \in M$ *e* $a \in A$*, é chamada um homomorfismo de* A*-módulos.*

Consideramos M um A-módulo e N um A-submódulo de M. Notemos que a aplicação $f : M \longrightarrow \dfrac{M}{N}$, dada por $f(x) = \overline{x} = x + N$, é um homomorfismo sobrejetor. Assim, como

uma consequência desta aplicação existe um isomorfismo entre os A-submódulos de M que contém N e os A-submódulos de $\frac{M}{N}$. Além disso, notemos que se A é um corpo, então M e N são espaços vetoriais sobre A, e assim, um homomorfismo de A-módulos é uma transformação linear entre espaços vetoriais.

Definição 1.4 *Um A-módulo M é livre se M é isomorfo a um A-módulo da forma $\bigoplus_{i\in I} M_i$, onde cada $M_i \simeq A$, para todo $i \in I$.*

Da Definição 1.4, tem-se que um A-módulo M é livre se existe um subconjunto $\{x_i\}_{i\in I}$ de M tal que cada $x \in M$ é escrito de forma única como $x = \sum_{i\in I} a_i x_i$, onde $a_i \in A$ para $i \in I$, ou seja, o conjunto $\{x_i\}_{i\in I}$ é um conjunto de geradores linearmente independentes de M. O número de elementos de I é chamado de posto de M. No caso em que I é finito e $\{x_i\}_{i\in I}$ não é necessariamente linearmente independente, ou seja, $x = \sum_{i\in I} a_i x_i$ mas não de forma única, M é dito um A-módulo finitamente gerado.

Proposição 1.1 *Se M é um A-módulo, então M é finitamente gerado se, e somente se, M é isomorfo a um quociente de A^n, para algum $n \in \mathbb{N}$.*

Demonstração. Suponhamos que M é finitamente gerado por $\{x_1, x_2, \ldots, x_n\}$ e consideramos a aplicação $\varphi : A^n \longrightarrow M$ dada por $\varphi(a_1, a_2, \ldots, a_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n$. Tem-se que φ é um homomorfismo sobrejetor de A-módulos, e assim, $\frac{A^n}{Ker(\varphi)} \simeq M$. Reciprocamente, consideramos ψ o homomorfismo de A^n no A-módulo M. Tem-se que o conjunto $\{e_1, e_2, \ldots, e_n\}$ gera A^n, onde $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, com a i-ésima coordenada igual a 1. Assim, $\psi(e_i)$ gera M, pois M é isomorfo a um quociente de A^n. Portanto, M é finitamente gerado. ■

Definição 1.5 *Dizemos que um A-módulo M é um A-módulo Noetheriano se satisfaz uma das seguintes condições equivalentes:*

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

ii) Toda sequência crescente de A-submódulos de M é estacionária

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

Um anel A é chamado de um anel Noetheriano se A é um A-módulo Noetheriano.

Exemplo 1.2 *Seja A um anel principal. Os A-submódulos de A são os ideais do anel A. Assim, qualquer A-submódulo de A é finitamente gerado. Portanto, A é um anel Noetheriano.*

Teorema 1.1 *Se M um A-módulo e N um A-submódulo de M, então M é Noetheriano se, e somente se, N e $\frac{M}{N}$ são Noetherianos.*

Demonstração. Suponhamos que M é um A-módulo Noetheriano. Se F é um A-submódulo de N, então F é um A-submódulo de M. Assim, qualquer sequência crescente de A-submódulos de N é estacionária. De forma análoga, se E é um A-submódulo de $\frac{M}{N}$ então E é um A-submódulo de M que contém N. Portanto, qualquer sequência crescente de A-submódulos de $\frac{M}{N}$ é estacionária. Reciprocamente, suponhamos que N e $\frac{M}{N}$ são A-módulos Noetherianos. Seja $(R_n)_{n\in\mathbb{N}}$ uma sequência crescente de A-submódulos de M. Consideramos a aplicação $\varphi : M \longrightarrow N \times \frac{M}{N}$ dada por $\varphi(R_n) = \left(R_n \cap N, \frac{R_n + N}{N}\right)$. Tem-se que φ está bem definida, pois $R_n \cap N$ é um A-submódulo de N e $\frac{R_n + N}{N}$ é um A-submódulo de $\frac{M}{N}$. Tem-se que $R_n \subseteq R_{n+1}$ e mostramos que $R_{n+1} \subseteq R_n$, para algum n. Para isso mostremos que φ é injetiva. Suponhamos que $R_n \cap N = R_{n+1} \cap N$ e $\frac{R_n + N}{N} = \frac{R_{n+1} + N}{N}$. Seja $x \in R_{n+1}$. Assim, existem $u, v \in N$ e $y \in R_n$ tal que $y + u = x + v$. Logo, $x - y = u - v \in R_{n+1} \cap N = R_n \cap N$. Como $x - y \in R_n$ e $y \in R_n$ segue que $x \in R_n$. Portanto, $R_{n+1} = R_n$. Pelo fato de N e $\frac{M}{N}$ serem A-módulos Noetherianos, segue que existem $n_1, n_2 \in \mathbb{N}$ tais que dadas sequências crescentes $(F_n)_{n\in\mathbb{N}}$ em N e $(E_n)_{n\in\mathbb{N}}$ em $\frac{M}{N}$, tem-se que $E_n = E_{n+1}$, para todo $n \geq n_1$ e $F_n = F_{n+1}$, para todo $n \geq n_2$. Se $n_0 = sup\{n_1, n_2\}$, então $R_n = R_{n+1}$, para todo $n \geq n_0$. Portanto, M é um A-módulo Noetheriano. ■

Corolário 1.1 *Se $M_1, M_2, \ldots, M_n$ são A-módulos Noetherianos, então $\prod_{i=1}^{n} M_i$ é um A-módulo Noetheriano.*

Demonstração. Mostramos por indução sobre n. Para $n = 2$, tem-se que $M_1 \simeq M_1 \times \{0\} \subseteq M_1 \times M_2$. Seja a aplicação $\varphi : M_1 \times M_2 \longrightarrow M_2$ dada por $\varphi(x, y) =$

y. Tem-se que φ é um homomorfismo sobrejetor, e assim, $\dfrac{M_1 \times M_2}{Ker(\varphi)} \simeq M_2$. Como $Ker(\varphi) = M_1 \times \{0\} \simeq M_1$, segue que $\dfrac{M_1 \times M_2}{M_1 \times \{0\}} \simeq \dfrac{M_1 \times M_2}{M_1} \simeq M_2$. Como M_1 e M_2 são Noetherianos, segue pelo Teorema 1.1, que $M_1 \times M_2$ é Noetheriano. Agora, suponhamos que $\prod_{i=1}^{n-1} M_i$ é Noetheriano e mostramos que $\prod_{i=1}^{n} M_i$ é Noetheriano. Se $N = \prod_{i=1}^{n-1} M_i$, então $N \times M_n$ é Noetheriano pela primeira parte. Portanto, $\prod_{i=1}^{n} M_i$ é Noetheriano. ■

Corolário 1.2 *Se A é um anel Noetheriano e M um A-módulo finitamente gerado, então M é um A-módulo Noetheriano.*

Demonstração. Como M é um A-módulo finitamente gerado, segue que M é isomorfo ao módulo quociente $\dfrac{A^n}{Ker(\varphi)}$ (Proposição 1.1). Pelo Corolário 1.1, segue que A^n é Noetheriano e pelo Teorema 1.1, segue que $\dfrac{A^n}{Ker(\varphi)}$ é Noetheriano. Portanto, M é Noetheriano. ■

Proposição 1.2 *Se A é um anel Noetheriano, então todo ideal de A contém um produto de ideais primos de A. Se A é um domínio de integridade Noetheriano, então todo ideal não nulo de A contém um produto de ideais primos não nulos de A.*

Demonstração. Suponhamos que a família $\mathfrak{F}$ de ideais de A que não contém um produto de ideais primos é não vazia. Como A é Noetheriano, segue que $\mathfrak{F}$ tem um elemento maximal $\mathfrak{b}$. Tem-se que $\mathfrak{b}$ não é um ideal primo, pois caso contrário $\mathfrak{b} \notin \mathfrak{F}$. Assim, existem $x, y \in A - \mathfrak{b}$ tal que $xy \in \mathfrak{b}$. Consideramos $\mathfrak{b}' = \mathfrak{b} + \langle x \rangle$ e $\mathfrak{b}'' = \mathfrak{b} + \langle y \rangle$. Logo, $\mathfrak{b} \subset \mathfrak{b}'$ e $\mathfrak{b} \subset \mathfrak{b}''$, e assim $\mathfrak{b}'$, $\mathfrak{b}'' \notin \mathfrak{F}$, pois $\mathfrak{b}$ é maximal. Assim, $\mathfrak{b}'$ e $\mathfrak{b}''$ contém produtos de ideais primos de A. Como $\mathfrak{b}'\mathfrak{b}'' = \left\{ \sum_{i=1}^{n} a_i b_i ; a_i \in \mathfrak{b}', b_i \in \mathfrak{b}'' \right\}$, segue que $\mathfrak{b}'\mathfrak{b}'' \subset \mathfrak{b}$. Deste modo, $\mathfrak{b}$ contém um produto de ideais primos de A, o que contraria o fato de $\mathfrak{b} \in \mathfrak{F}$. Portanto, $\mathfrak{F}$ é uma família vazia. ■

Teorema 1.2 *Se A é um anel principal, M um A-módulo livre de posto n e N um A-submódulo de M, então*

a) N é livre de posto m, onde $0 \leq m \leq n$;

b) Se $N \neq \{0\}$, existe uma base $\{e_1, \ldots, e_n\}$ de M e elementos não nulos $a_1, \ldots, a_m \in A$ tal que $\{a_1e_1, \ldots, a_me_m\}$ é uma base de N com $a_i|a_{i+1}$, para $1 \leq i \leq m-1$.

Demonstração. a) Se $N = \{0\}$, então o resultado é válido. Assim, podemos supor $N \neq \{0\}$. Seja $\mathcal{L}(M, A)$ o conjunto dos funcionais lineares sobre M. Se $f \in \mathcal{L}(M, A)$, então $f(N)$ é um A-submódulo de A, ou seja, é um ideal de A. Como A é principal, segue que $f(N) = \langle a_f \rangle$, com $a_f \in A$. Pelo Exemplo 1.2, segue que existe $f \in \mathcal{L}(M, A)$ tal que $\langle a_f \rangle$ é maximal sobre $\langle a_g \rangle$, para qualquer $g \in \mathcal{L}(M, A)$. Como M é livre de posto n, segue, pela Proposição 1.1, que $M \simeq A^n$. Seja $\pi_i : M \longrightarrow A$ a projeção sobre a i-ésima coordenada. Logo, $\pi_i(x_j) = \delta_{ij}$, para $1 \leq i, j \leq n$. Pelo fato de $N \neq \{0\}$, tem-se que existe pelo menos um i, $1 \leq i \leq n$, tal que $\pi_i(N) \neq \{0\}$, e assim, $\langle a_f \rangle \neq \langle 0 \rangle$. Como $f(N) = \langle a_f \rangle$, segue que existe $e' \in N$ tal que $f(e') = a_f$. Mostramos que $a_f | g(e')$ para qualquer $g \in \mathcal{L}(M, A)$. De fato, se $d = mdc(a_f, g(e'))$, então existem $a,\ b \in A$ tal que $d = aa_f + bg(e')$. Logo, $d = af(e') + bg(e') = (af + bg)(e')$, que é um funcional linear sobre M. Assim, $\langle a_f \rangle \subseteq \langle d \rangle \subseteq f(N)$. Porém, como $\langle a_f \rangle$ é maximal, segue que $\langle a_f \rangle = \langle d \rangle$, o que implica que $a_f | g(e')$. Em particular, $a_f | \pi_i(e')$. Assim, $\pi_i(e') = a_f b_i$, com $b_i \in A$. Se $\{x_1, \ldots, x_n\}$ é uma base de M, então podemos escrever $e = \sum_{i=1}^{n} b_i x_i$, e assim, $e' = a_f e$. Como $f(e') = a_f = a_f f(e)$, segue que $f(e) = 1$, pois $a_f \neq 0$. Mostramos que $M = Ker(f) \oplus \langle e \rangle$ e $N = (N \cap Ker(f)) \oplus \langle e' \rangle$, onde $e' = a_f e$. De fato, se $x \in M$, então $x = f(x)e + (x - f(x)e)$. Assim, $f(x - f(x)e) = f(x) - f(x)f(e) = 0$, pois $f(e) = 1$. Logo, $x - f(x)e \in Ker(f)$, o que implica que $Ker(f) + \langle e \rangle = M$. Como $f(e) \neq 0$, segue que $Ker(f) \cap \langle e \rangle = \langle 0 \rangle$. Agora, se $y \in N$, então $f(y) = ba_f$, com $b \in A$. Assim, $y = ba_f e + (y - ba_f e) = be' + (y - f(y)e)$. De modo análogo ao anterior, $y - f(y)e \in Ker(f)$ e também $y - f(y)e = y - be' \in N$, ou seja, $y - f(y)e \in N \cap Ker(f)$ e $be' \in \langle e' \rangle$. Agora, provamos (a) por indução sobre m. Se $m = 0$, então $N = \{0\}$ e a prova é direta. Se $m > 0$, então $N \cap Ker(f)$ tem posto $m-1$, e assim, pela hipótese de indução $N \cap Ker(f)$ é livre. Logo, adicionando e' a uma base de $N \cap Ker(f)$ obtemos uma base de N. Portanto, N é livre de posto m.

b) Provamos (b) por indução sobre n. Se $n = 0$ a prova é trivial. Tem-se por (a) que $Ker(f)$ é livre de posto $n - 1$, pois $M = Ker(f) \oplus \langle e \rangle$. Logo, aplicando a hipótese de

indução sobre $Ker(f)$ e seu submódulo $N \cap Ker(f)$, tem-se que se $N \cap Ker(f) \neq \langle 0 \rangle$, então existem $m \leq n$, uma base $\{e_2, \ldots, e_n\}$ do $Ker(f)$ e elementos não nulos $a_2, \ldots, a_m$ de A tal que $\{a_2e_2, \ldots, a_me_m\}$ é uma base para $N \cap Ker(f)$, com $a_i | a_{i+1}$, para $2 \leq i \leq m-1$. Tomando a mesma notação dada acima e colocando $a_f = a_1$ e $e = e_1$, tem-se que $\{e_1, \ldots, e_n\}$ é uma base de M e $\{a_1e_1, \ldots, a_me_m\}$ é uma base de N, pois $M = Ker(f) \oplus \langle e \rangle$ e $N = (N \cap Ker(f)) \oplus \langle e' \rangle$, com $e' = a_1e_1$. Resta mostrar que $a_1 | a_2$. De fato, se $g \in \mathcal{L}(M, A)$ tal que $g(e_1) = g(e_2) = 1$ e $g(e_i) = 0$, para $i \geq 3$, então $a_1 = a_f = g(a_fe_1) = g(e') \in g(N)$. Assim, $\langle a_f \rangle = g(N) = \langle a_1 \rangle$. Como $a_2 = g(a_2e_2) \in g(N)$, segue que $a_2 \in \langle a_1 \rangle$, o que implica que $a_1 | a_2$. ■

Corolário 1.3 *Se A é um anel principal e M um A-módulo finitamente gerado, então M é isomorfo ao produto $\frac{A}{\mathfrak{a}_1} \times \frac{A}{\mathfrak{a}_2} \times \ldots \times \frac{A}{\mathfrak{a}_n}$, onde $\mathfrak{a}_i$'s são ideais de A tal que $\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \ldots \supseteq \mathfrak{a}_n$.*

Demonstração. Seja $\{x_1, \ldots, x_n\}$ um conjunto de geradores de M. Pela Proposição 1.1, segue que $M \simeq \frac{A^n}{Ker(\varphi)}$ e pelo Teorema 1.2, segue que existe uma base $\{e_1, \ldots, e_n\}$ de A^n e elementos não nulos $a_1, \ldots, a_q \in A$ tal que $\{a_1e_1, \ldots, a_qe_q\}$ é uma base de $Ker(\varphi)$ e que $a_i | a_{i+1}$, para $1 \leq i \leq q-1$. Notemos que se colocarmos $a_j = 0$, para $q \leq j \leq n$, então $\frac{A^n}{Ker(\varphi)} \simeq \prod_{i=1}^{n} \frac{e_iA}{a_ie_iA}$. Assim, $\frac{A^n}{Ker(\varphi)} \simeq \prod_{i=1}^{n} \frac{A}{\mathfrak{a}_i} \simeq M$. ■

Definição 1.6 *Seja A um domínio de integridade. Um A-módulo M é dito livre de torsão se $ax = 0$ implicar que $a = 0$ ou $x = 0$, com $a \in A$ e $x \in M$.*

Corolário 1.4 *Se A é um anel principal e M é um A-módulo finitamente gerado e livre de torsão, então M é um A-módulo livre.*

Demonstração. Pelo Corolário 1.3 tem-se que $M \simeq \frac{A}{\mathfrak{a}_1} \times \ldots \times \frac{A}{\mathfrak{a}_n}$, onde os $\mathfrak{a}_i$'s são ideais de A tal que $\mathfrak{a}_1 \supseteq \ldots \supseteq \mathfrak{a}_n$. Eliminando os fatores que são iguais a zero, podemos supor que $\mathfrak{a}_i \neq A$, para $1 \leq i \leq n$. Se $\mathfrak{a}_1 \neq \langle 0 \rangle$, $a \in \mathfrak{a}_1$, $x_1 \in \frac{A}{\mathfrak{a}_1}$ são não nulos, então $ax = 0$, onde $x = (x_1, \ldots, 0)$, o que contradiz o fato de M ser livre de torsão. Assim, $\mathfrak{a}_1 = \langle 0 \rangle$, e consequentemente, $\mathfrak{a}_i = \langle 0 \rangle$, para todo $1 \leq i \leq n$. Portanto, $M \simeq A^n$. ■

Lema 1.1 *Se A é um anel e $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_r\}$ é um conjunto de ideais de A tal que $\mathfrak{a}_i + \mathfrak{a}_j = A$, para $i \neq j$, então* $\dfrac{A}{\mathfrak{a}_1\mathfrak{a}_2 \ldots \mathfrak{a}_r} \simeq \prod_{i=1}^{r} \dfrac{A}{\mathfrak{a}_i}$.

Demonstração. Mostramos o resultado por indução sobre r. Se $r = 2$, mostramos que $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{a}_2$ e o homomorfismo canônico $\varphi : A \longrightarrow \dfrac{A}{\mathfrak{a}_1} \times \dfrac{A}{\mathfrak{a}_2}$ induz um isomorfismo $\theta : \dfrac{A}{\mathfrak{a}_1\mathfrak{a}_2} \longrightarrow \dfrac{A}{\mathfrak{a}_1} \times \dfrac{A}{\mathfrak{a}_2}$. De fato, tem-se que $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}_1$ e $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}_2$, e assim, $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}_1 \cap \mathfrak{a}_2$. Como $\mathfrak{a}_1 + \mathfrak{a}_2 = A$, segue que existem $a \in \mathfrak{a}_1$ e $b \in \mathfrak{a}_2$ tal que $a + b = 1$. Assim, se $x \in \mathfrak{a}_1 \cap \mathfrak{a}_2$, então $x = ax + bx \in \mathfrak{a}_1\mathfrak{a}_2$, ou seja, $\mathfrak{a}_1 \cap \mathfrak{a}_2 \subseteq \mathfrak{a}_1\mathfrak{a}_2$. Deste modo, $\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{a}_1 \cap \mathfrak{a}_2$. Seja $(\overline{y}, \overline{z}) \in \dfrac{A}{\mathfrak{a}_1} \times \dfrac{A}{\mathfrak{a}_2}$. Tomamos $x = az + by$, com a e b como antes. Notemos $x \equiv by \equiv (y - ay) \equiv y(mod\ \mathfrak{a}_1)$ e $x \equiv az \equiv (z - bz) \equiv z(mod\ \mathfrak{a}_2)$. Logo, $\varphi(x) = (\overline{y}, \overline{z})$. Portanto, φ é sobrejetora. Claramente, $Ker(\varphi) = \mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{a}_2$, e consequentemente, $\theta : \dfrac{A}{\mathfrak{a}_1\mathfrak{a}_2} \longrightarrow \dfrac{A}{\mathfrak{a}_1} \times \dfrac{A}{\mathfrak{a}_2}$ é um isomorfismo. Agora seja $r > 2$. Tomamos $\mathfrak{b} = \mathfrak{a}_2 \ldots \mathfrak{a}_r$. Mostramos que $\mathfrak{a}_1 + \mathfrak{b} = A$. De fato, tem-se que $\mathfrak{a}_1 + \mathfrak{a}_i = A$, para todo $i \geq 2$, e assim, existem $c_i \in \mathfrak{a}_1$ e $a_i \in \mathfrak{a}_i$ tal que $c_i + a_i = 1$, e consequentemente, $1 = \prod_{i=2}^{r}(c_i + a_i) = c + \mathfrak{b}$, onde $c = \prod_{i=2}^{r} c_i \in \mathfrak{a}_1$. Logo, $\mathfrak{a}_1 + \mathfrak{b} = A$. Portanto, o resultado segue pela primeira parte. ■

Como consequência do Lema 1.1 tem-se que se $mdc(n, m) = 1$, então $\dfrac{\mathbb{Z}}{nm\mathbb{Z}} \simeq \dfrac{\mathbb{Z}}{n\mathbb{Z}} \times \dfrac{\mathbb{Z}}{m\mathbb{Z}}$.

Corolário 1.5 *Se A é um anel principal e M um A-módulo finitamente gerado, então M é isomorfo a um produto finito de A-módulos M_i, onde $M_i = A$ ou $M_i = \dfrac{A}{p^s A}$, com p primo.*

Demonstração. Pelo Corolário 1.3, tem-se que $M \simeq \dfrac{A}{a_1 A} \times \ldots \times \dfrac{A}{a_n A}$. Se $a_i = p_1^{s_1} \ldots p_r^{s_r}$, para cada $1 \leq i \leq n$, é a fatoração de a_i em primos, então, pelo Lema 1.1, segue que $\dfrac{A}{a_i A} \simeq \prod_{i=1}^{r} \dfrac{A}{p_i^{s_i} A}$, o prova o corolário. ■

Corolário 1.6 *(Teorema Fundamental de Grupos Abelianos Finitos) Se G é um grupo abeliano finito, então $G \simeq \prod_{i=1}^{r} G_i$, onde os G_i's são grupos ciclícos de ordem $p_i^{s_i}$, com p_i primo, $s_i \in \mathbb{N}$ e $1 \leq i \leq r$.*

Demonstração. Como todo grupo abeliano é um $\mathbb{Z}$-módulo e $\mathbb{Z}$ é um anel principal, segue, pelo Corolário 1.5, que $G \simeq \prod_{i=1}^{r} G_i$, onde $G_i = \mathbb{Z}$ ou $G_i = \frac{\mathbb{Z}}{p_i^{s_i}\mathbb{Z}}$, com p_i primo. No caso em que $G_i = \frac{\mathbb{Z}}{p_i^{s_i}\mathbb{Z}}$, tem-se que G_i é ciclíco de ordem $p_i^{s_i}$, pois a aplicação $f : \frac{\mathbb{Z}}{n\mathbb{Z}} \longrightarrow G_i$ dada por $f(\bar{s}) = a_i^s$, onde a_i é um gerador de G_i, é um isomorfismo. No caso em que $G_i = \mathbb{Z}$, tem-se que G_i é ciclíco infinito, pois a aplicação $h : \mathbb{Z} \longrightarrow G_i$ dada por $h(m) = a_i^m$, onde a_i é um gerador de G_i, é um isomorfismo. Pelo fato de G ser finito, segue que $G \simeq \prod_{i=1}^{r} G_i$, onde $G_i = \frac{\mathbb{Z}}{p_i^{s_i}\mathbb{Z}}$, com p_i primo. ■

Corolário 1.7 *Se G é um grupo abeliano finito, então existe $g \in G$ tal que $o(g) = mmc\{o(h);\ h \in G\}$.*

Demonstração. Como todo grupo abeliano é um $\mathbb{Z}$-módulo e $\mathbb{Z}$ é um anel principal, segue, pelo Corolário 1.3, que $G \simeq \frac{\mathbb{Z}}{a_1\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{a_n\mathbb{Z}}$, onde $a_i | a_{i+1}$, para todo $1 \leq i \leq n-1$. Como G é finito, segue que $a_i \neq 0$ para $1 \leq i \leq n$. Seja $g = (0, \ldots, 0, \overline{1})$, onde $\overline{1} = 1 + a_n\mathbb{Z}$. Tem-se que $a_n g = (0, \ldots, 0, a_n + a_n\mathbb{Z}) = (0, \ldots, 0)$ o que torna a_n a ordem de g. Pelo fato de $a_i | a_{i+1}$, tem-se que $a_n h = 0$, para todo $h \in G$, ou seja, a_n é mútiplo de $o(h)$, para todo $h \in G$. Portanto, g é o elemento de G cuja ordem é $mmc\{o(h);\ h \in G\}$. ■.

1.2 Elementos inteiros

Nesta seção, o objetivo é definir elementos inteiros sobre um anel, anel de inteiros e suas propriedades, sendo que uma delas é de que o anel de inteiros é integralmente fechado. A principal referência desta seção é [7].

Definição 1.7 *Sejam $A \subseteq B$ anéis e $\alpha \in B$. Dizemos que α é inteiro sobre A se α é raiz de um polinômio mônico com coeficientes em A, ou seja, se existem $a_0, a_1, \ldots, a_{n-1} \in A$, não todos nulos, tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$. No caso, em que $A = \mathbb{Z}$ diremos que α é um inteiro algébrico.*

Exemplo 1.3 *Se $\alpha = \sqrt{2} + \sqrt{5} \in \mathbb{R}$, então α é raiz de $f(x) = x^4 - 14x^2 + 9 \in \mathbb{Z}[x]$. Portanto, α é um inteiro algébrico.*

Teorema 1.3 *Sejam $A \subseteq B$ anéis e $\alpha \in B$. As seguintes afirmações são equivalentes:*

a) α é inteiro sobre A.

b) O anel $A[\alpha] = \left\{ \sum_i a_i \alpha^i,\ a_i \in A \right\}$ é um A-módulo finitamente gerado.

c) Existe um subanel R de B que é um A-módulo finitamente gerado contendo A e α.

Demonstração. $(a) \Rightarrow (b)$ Seja M um A-submódulo de B gerado por $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Como α é inteiro sobre A, segue que existem $a_0, a_1, \ldots, a_{n-1} \in A$, não todos nulos, tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$. Assim, $\alpha^n = -\sum_{i=0}^{n-1} a_i \alpha^i$ o que implica que $\alpha^n \in M$. Para provar que $M = A[\alpha]$, devemos provar que $\alpha^j \in M$, para todo $j \in \mathbb{N}$, que será feito por indução sobre j. Para $j \leq n$, já vimos que $\alpha^j \in M$. Suponhamos que $\alpha^j \in M$ e mostramos que $\alpha^{j+1} \in M$. Por hipótese de indução, tem-se que $\alpha^j = \sum_{i=0}^{n-1} s_i \alpha^i$, $s_i \in A$. Assim,

$$\begin{aligned}
\alpha^{j+1} &= \left(\sum_{i=0}^{n-1} s_i \alpha^i \right) \alpha = (s_{n-1}\alpha^{n-1} + \ldots + s_0)\alpha = s_{n-1}\alpha^n + s_{n-2}\alpha^{n-1} + \ldots + s_0\alpha \\
&= s_{n-1}(-a_{n-1}\alpha^{n-1} - \ldots - a_1\alpha - a_0) + s_{n-2}\alpha^{n-1} + \ldots + s_0\alpha \\
&= (s_{n-2} - a_{n-1}s_{n-1})\alpha^{n-1} + (s_{n-3} - a_{n-2}s_{n-1})\alpha^{n-2} + \ldots + (s_0 - a_1 s_{n-1})\alpha - a_0 s_{n-1}.
\end{aligned}$$

Logo, $\alpha^{j+1} \in M$, para todo $j \in \mathbb{N}$, o que implica que $A[\alpha] \subseteq M$. Como M é gerado por $\{1, \ldots, \alpha^{n-1}\}$ segue que $M \subseteq A[\alpha]$. Portanto, $M = A[\alpha]$ o que torna $A[\alpha]$ um A-módulo finitamente gerado.

$(b) \Rightarrow (c)$ Basta colocar $R = A[\alpha]$. Assim R é um subanel de B que é um A-módulo finitamente gerado contendo A e α.

$(c) \Rightarrow (a)$ Como R é um A-módulo finitamente gerado, segue que existe um conjunto $\{r_1, r_2, \ldots, r_n\} \subseteq R$ tal que $R = \sum_{i=1}^{n} A r_i$. Assim, $\alpha r_i \in R$, para $i = 1, 2, \ldots, n$, pois $\alpha \in R$ por hipótese. Deste modo, $\alpha r_i = \sum_{j=1}^{n} a_{ij} r_j$, com $a_{ij} \in A$, para $1 \leq i \leq n$, ou seja, $\alpha r_i - \sum_{j=1}^{n} a_{ij} r_j = 0$, com $a_{ij} \in A$, para $1 \leq i \leq n$. Portanto, $\sum_{j=1}^{n} (\delta_{ij}\alpha - a_{ij}) r_j = 0$,

com $a_{ij} \in A$, para $1 \leq i \leq n$, onde $\delta_{ij} = \begin{cases} 1, & se \;\; i = j \\ 0, & se \;\; i \neq j \end{cases}$. Seja $d = det(\delta_{ij}\alpha - a_{ij}) = \alpha^n + \ldots + a_0$. Pela Regra de Cramer, segue que $dr_i = 0$, para $i = 1, 2, \ldots, n$. Assim $dr = 0$, para todo $r \in R$ e em particular, $d1 = d = 0$. Portanto, $d = \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$, o que torna α inteiro sobre A. ■

Proposição 1.3 *Sejam $A \subseteq B$ anéis e $\{b_1, b_2, \ldots, b_n\} \subseteq B$. Se b_i é inteiro sobre $A[b_1, b_2, \ldots, b_{i-1}]$, para $1 \leq i \leq n$, então $A[b_1, b_2, \ldots, b_n]$ é um A-módulo finitamente gerado.*

Demonstração. Provamos por indução sobre n. Para $n = 1$, o resultado segue pelo Teorema 1.3. Assumimos que $R = A[b_1, b_2, \ldots, b_{n-1}]$ é um A-módulo finitamente gerado. Assim, existe $\{r_1, r_2, \ldots, r_p\} \subseteq R$ tal que $R = \sum_{i=1}^{p} Ar_i$. Como b_n é inteiro sobre R, pelo Teorema 1.3, segue que $R[b_n]$ é um R-módulo finitamente gerado. Logo, existe $\{s_1, s_2, \ldots, s_q\} \subseteq R[b_n]$ tal que

$$R[b_n] = \sum_{j=1}^{q} Rs_j = \sum_{j=1}^{q} \left(\sum_{i=1}^{p} Ar_i \right) s_j = \sum_{i,j} Ar_i s_j.$$

Portanto, $R[b_n] = A[b_1, b_2, \ldots, b_n]$ é um A-módulo finitamente gerado por $\{r_i s_j\}$, onde $1 \leq i \leq p$ e $1 \leq j \leq q$. ■

Definição 1.8 *Sejam $A \subseteq B$ anéis. O conjunto $\mathcal{O}_B = \{b \in B; b$ é inteiro sobre $A\}$ é chamado de fecho inteiro de B sobre A, ou simplesmente de anel de inteiros de B sobre A. Se A é um domínio de integridade e $\mathbb{K}$ seu corpo de frações, o fecho inteiro de $\mathbb{K}$ sobre A é chamado de fecho inteiro de A. Dizemos que B é inteiro sobre A se para todo $b \in B$, b é inteiro sobre A.*

Notemos que $\mathcal{O}_B$ é um subanel de B que contém A, pois qualquer $\alpha \in A$ é raiz de $f(x) = x - \alpha \in A[x]$. Além disso, se $x,\ y \in \mathcal{O}_\mathcal{B}$, então $x + y,\ x - y$ e $xy \in A[x, y]$. Assim, pela Proposição 1.3, $A[x, y]$ é um A-módulo finitamente gerado. Logo, pelo item (c) do Teorema 1.3, tem-se que $x + y,\ x - y$ e $xy \in \mathcal{O}_B$.

Proposição 1.4 *Sejam $A \subseteq B \subseteq C$ anéis. Assim, C é inteiro sobre A se, e somente se, C é inteiro sobre B e B é inteiro sobre A.*

Demonstração. Suponhamos que C é inteiro sobre A. Assim, se $\alpha \in C$, então existem $a_0, a_1, \ldots, a_{n-1} \in A$, não todos nulos, tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$. Como $A \subseteq B$ segue que $a_i \in B$, para $i = 1, 2, \ldots, n$, o que torna α inteiro sobre B. Portanto, C é inteiro sobre B. Seja $\alpha \in B$. Como $B \subseteq C$, segue que $\alpha \in C$. Por hipótese, tem-se que $\alpha \in C$ é inteiro sobre A, e portanto, B é inteiro sobre A. Reciprocamente, se $\alpha \in C$, então existem $b_0, b_1, \ldots, b_{n-1} \in B$ tal que $\alpha^n + b_{n-1}\alpha^{n-1} + \ldots + b_0 = 0$. Assim, α é inteiro sobre $A[b_0, b_1, \ldots, b_{n-1}]$, e como B é inteiro sobre A, segue que cada b_i, para $i = 0, 1, \ldots, n-1$, é inteiro sobre A. Logo, pela Proposição 1.3, segue que $A[b_0, b_1, \ldots, b_{n-1}, \alpha]$ é um A-módulo finitamente gerado. Assim, pelo Teorema 1.3, segue que α é inteiro sobre A. Portanto, C é inteiro sobre A. ■

Proposição 1.5 *Sejam B um domínio de integridade, A um subanel de B e B inteiro sobre A. Para que B seja um corpo é necessário e suficiente que A seja um corpo.*

Demonstração. Se B é um corpo e $a \in A$ é não nulo, então $a^{-1} \in B$. Como B é inteiro sobre A, segue que existem $c_0, \ldots, c_{n-1} \in A$ tal que

$$(a^{-1})^n + c_{n-1}(a^{-1})^{n-1} + \ldots + c_0 = 0. \tag{1.1}$$

Multiplicando a Equação (1.1) por a^{n-1}, obtemos $a^{-1} = -c_{n-1} - c_{n-2}a - \ldots - c_0 a^{n-1}$. Logo, $a^{-1} \in A$. Portanto, A é um corpo. Reciprocamente, se A é um corpo e $b \in B$ é não nulo, então, pelo Teorema 1.3, segue que $A[b]$ é um A-espaço vetorial de dimensão finita. Consideramos a aplicação $f : A[b] \longrightarrow A[b]$ dada por $f(y) = by$, a qual é uma transformação A-linear. Como $A[b]$ é um domínio de integridade e $b \neq 0$, segue que $Ker(f) = \{0\}$. Além disso, f é sobrejetiva, pois é uma transformação A-linear injetiva entre espaços vetoriais de mesma dimensão. Logo, existe $b' \in A[b]$ tal que $bb' = 1$, ou seja, b é inversível em $A[b]$. Portanto, B é um corpo. ■

Definição 1.9 *Seja A é um domínio de integridade. Dizemos que A é integralmente fechado se o fecho inteiro de A é o próprio A.*

Exemplo 1.4 *Todo anel principal A é integralmente fechado, pois A é um domínio de integridade e se $\alpha \in Q(A)$ (corpo de frações de A) é inteiro sobre A, então existem*

$a_0, a_1, \ldots, a_{n-1} \in A$, não todos nulos, tal que

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0. \tag{1.2}$$

Como $\alpha \in Q(A)$, segue que podemos escrever $\alpha = \frac{a}{b}$, com $a, b \in A, b \neq 0$ e $mdc(a, b) = 1$. Substituindo $\alpha = \frac{a}{b}$ na Equação (1.2), tem-se que

$$\frac{a^n}{b^n} + a_{n-1}\frac{a^{n-1}}{b^{n-1}} + \ldots + a_1\frac{a}{b} + a_0 = 0. \tag{1.3}$$

Multiplicando a Equação (1.3) por b^n tem-se que $a^n + a_{n-1}ba^{n-1} + \ldots + a_1b^{n-1}a + b^n a_0 = a^n + b(a_{n-1}a^{n-1} + \ldots + a_1b^{n-2}a + b^{n-1}a_0) = 0$ o que implica que $a^n = -b(a_{n-1}a^{n-1} + \ldots + b^{n-1}a_0)$. Assim, b divide a^n, e como $mdc(a, b) = 1$, segue que $b|a^{n-1}$. Repetindo este processo, segue que $b|a$, ou seja, $a = bk$, para algum $k \in \mathbb{Z}$. Logo, $a = bk$ e existem $x, y \in A$ tal que $ax + by = 1$. Assim, $bkx + by = 1$ o que implica que $b(kx + y) = 1$. Portanto, b é um elemento inversível de A, e deste modo $\alpha = \frac{a}{b} = ab^{-1} \in A$ o que torna A um anel integralmente fechado.

Exemplo 1.5 *Se $A \subseteq B$ são anéis, então $\mathcal{O}_B$ (o fecho inteiro de B sobre A) é integralmente fechado. Seja $x \in \mathbb{M} = Q(\mathcal{O}_B)$ tal que x é inteiro sobre $\mathcal{O}_B$. Como $\mathcal{O}_B$ é inteiro sobre A, segue pela Proposição 1.4, que x é inteiro sobre A. Assim, o conjunto dos elementos de $\mathbb{M}$ que são inteiros sobre $\mathcal{O}_B$ está contido em $\mathcal{O}_B$. Portanto, $\mathcal{O}_B$ é integralmente fechado.*

1.3 Extensões de corpos e teoria de Galois

Nesta seção, apresentamos alguns resultados de extensões de corpos e extensões de Galois. O principal resultado é o Teorema de Irracionalidade Natural, além é claro de resultados clássicos da Teoria de Galois como o Teorema da Correspondência de Galois. Utilizamos as referências [8], [11], [12], [13], [14] e [15].

Definição 1.10 *Dizemos que um corpo $\mathbb{L}$ é uma extensão de um corpo $\mathbb{K}$ se $\mathbb{K} \subseteq \mathbb{L}$. Podemos considerar $\mathbb{L}$ como um $\mathbb{K}$-espaço vetorial e assim chamamos $dim_{\mathbb{K}}\mathbb{L} = [\mathbb{L} : \mathbb{K}]$ de grau da extensão $\mathbb{L}$ sobre $\mathbb{K}$. Denotamos a extensão $\mathbb{L}$ de $\mathbb{K}$ por $\mathbb{L}|\mathbb{K}$.*

Exemplo 1.6 *Como $\mathbb{R} \subset \mathbb{C}$, segue que $\mathbb{C}$ é uma extensão de $\mathbb{R}$ e $dim_{\mathbb{R}}\mathbb{C} = [\mathbb{C} : \mathbb{R}] = 2$, pois $\{1, i\}$ é uma base de $\mathbb{C}$ sobre $\mathbb{R}$.*

Definição 1.11 *Sejam A um anel e $\mathbb{K}$ um corpo contido em A. Dizemos que $x \in A$ é algébrico sobre $\mathbb{K}$ se existem $a_0, a_1, \ldots, a_n \in \mathbb{K}$, não todos nulos, tal que*

$$a_n x^n + \ldots + a_1 x + a_0 = 0. \tag{1.4}$$

Se x não é algébrico sobre $\mathbb{K}$ chamamos x de transcendente sobre $\mathbb{K}$.

Como $\mathbb{K}$ é um corpo, segue que assumindo que $a_n \neq 0$, podemos multiplicar a Equação (1.4) por $a_n^{-1} \in \mathbb{K}$. Assim, x é inteiro sobre $\mathbb{K}$. Portanto, sobre um corpo x é inteiro se, e somente se, x é algébrico.

Definição 1.12 *Sejam A um anel, $\mathbb{K}$ um corpo contido em A e $\alpha \in A$ algébrico sobre $\mathbb{K}$. O polinômio $p(x) \in \mathbb{K}[x]$ mônico de menor grau tal que α é raiz é chamado polinômio minimal de α sobre $\mathbb{K}$ e denotado por $min_{\mathbb{K}}\alpha$.*

Proposição 1.6 *Sejam $\mathbb{L}|\mathbb{K}$ uma extensão de corpos, $\alpha \in \mathbb{L}$ algébrico sobre $\mathbb{K}$ e $\mathbb{K}(\alpha)$ o menor corpo que contém $\mathbb{K}$ e α.*

a) O polinômio $min_{\mathbb{K}}\alpha$ é irredutível sobre $\mathbb{K}$;

b) Se $f(x) \in \mathbb{K}[x]$, então $f(\alpha) = 0$ se, e somente se, $min_{\mathbb{K}}\alpha$ divide $f(x)$;

c) Se $n = gr(min_{\mathbb{K}}\alpha)$, então $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base de $\mathbb{K}(\alpha)$ sobre $\mathbb{K}$. Assim $[\mathbb{K}(\alpha) : \mathbb{K}] = gr(min_{\mathbb{K}}\alpha)$ e $\mathbb{K}(\alpha) = \mathbb{K}[\alpha]$.

Demonstração. ([8], pág. 15) ■

Observação 1.1 *Pelo Teorema 1.3 tem-se que α é algébrico sobre $\mathbb{K}$ se, e somente se, $\mathbb{K}[\alpha]$ é um $\mathbb{K}$-espaço vetorial de dimensão finita.*

No caso de $\mathbb{K} \subset \mathbb{L}$ ser uma extensão de corpos e todo $\alpha \in \mathbb{L}$ ser algébrico sobre $\mathbb{K}$, dizemos que $\mathbb{K} \subset \mathbb{L}$ é uma extensão algébrica. Pelo Teorema 1.3, se $[\mathbb{L} : \mathbb{K}]$ é finita, então $\mathbb{K} \subset \mathbb{L}$ é uma extensão algébrica.

Proposição 1.7 *Sejam $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ extensões de corpos. Se $\mathbb{K} \subseteq \mathbb{L}$ e $\mathbb{L} \subseteq \mathbb{M}$ são extensões algébricas, então $\mathbb{K} \subseteq \mathbb{M}$ é algébrica e $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.*

Demonstração. Pela Proposição 1.4, tem-se que $\mathbb{K} \subseteq \mathbb{M}$ é algébrica. Consideramos $\{x_i\}_{i\in I}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$ e $\{y_j\}_{j\in J}$ uma base de $\mathbb{M}$ sobre $\mathbb{L}$. De modo análogo a demonstração da Proposição 1.3, tem-se que $\{x_i y_j\}_{(i,j)\in I\times J}$ gera $\mathbb{M}$ sobre $\mathbb{K}$. Agora, se $\sum_{(i,j)\in I\times J} a_{ij}x_i y_j = 0$, com $a_{ij} \in \mathbb{K}$, então $\sum_{j\in J}\left(\sum_{i\in I} a_{ij}x_i\right) y_j = 0$. Como $\{y_j\}_{j\in J}$ é linearmente independente, segue que $\sum_{i\in I} a_{ij}x_i = 0$, para todo $j \in J$. Como $\{x_i\}_{i\in I}$ é linearmente independente, segue que $a_{ij} = 0$, para todo $i \in I$ e $j \in J$. Portanto, $\{x_i y_j\}_{(i,j)\in IxJ}$ é uma base de $\mathbb{M}$ sobre $\mathbb{K}$ e $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$. ■

Proposição 1.8 *Se $\mathbb{K}$ é um corpo e $p(x) \in \mathbb{K}[x]$ é um polinômio não constante, então existe uma extensão finita $\mathbb{L}$ de $\mathbb{K}$ tal que $p(x)$ fatora em $\mathbb{L}[x]$ em produto de polinômios de grau 1.*

Demonstração. Provamos por indução sobre $n = gr(p(x))$. Se $n = 1$, então o resultado é válido. Suponhamos que o resultado é válido para $n-1$ e provamos para n. Considere $p(x) = f(x)g(x)$, com $f(x) \in \mathbb{K}[x]$ irredutível. Seja α uma raiz de $p(x)$ e $f(x)$ é o polinômio minimal de α sobre $\mathbb{K}$. Consideramos o homomorfismo sobrejetor $\psi : \mathbb{K}[x] \longrightarrow \mathbb{K}[\alpha]$ dado por $\psi(q(x)) = q(\alpha)$. Pela Proposição 1.6, segue que o núcleo de ψ é $\langle f(x)\rangle$, e assim $\frac{\mathbb{K}[x]}{\langle f(x)\rangle} \simeq \mathbb{K}[\alpha]$. Como $x - \alpha \in \mathbb{K}(\alpha)[x]$ é o polinômio minimal de α em $\mathbb{K}(\alpha)$, segue que $x - \alpha$ divide $f(x)$ em $\mathbb{K}(\alpha)[x]$. Logo, existe $g_1(x) \in \mathbb{K}(\alpha)[x]$ tal que $p(x) = (x-\alpha)g_1(x)$. Como $gr(g_1(x)) = n-1$, segue, pela hipótese de indução, que existe uma extensão $\mathbb{L}$ de $\mathbb{K}(\alpha)$ tal que $g_1(x)$ fatora em $\mathbb{L}[x]$ em produto de polinômios de grau 1. Logo, em $\mathbb{L}[x]$, tem-se que $p(x)$ fatora em um produto de polinômios de grau 1. ■

Definição 1.13 *O menor corpo que contém $\mathbb{K}$ e as raízes de $p(x)$ é chamado de corpo de raízes de $p(x)$. Denotamos $\mathbb{K}(R_p)$ o corpo de raízes de $p(x)$. A Proposição 1.8 garante a existência de $\mathbb{K}(R_p)$.*

Definição 1.14 *Sejam $\mathbb{M}$ e $\mathbb{L}$ corpos contendo $\mathbb{K}$. Dizemos que $\mathbb{M}$ e $\mathbb{L}$ são conjugados sobre $\mathbb{K}$ (ou $\mathbb{K}$-isomorfos) se existe um isomorfismo $\varphi : \mathbb{M} \longrightarrow \mathbb{L}$ tal que $\varphi|_{\mathbb{K}} = id$. Se*

$\alpha \in \mathbb{M}$, $\beta \in \mathbb{L}$ e existe um isomorfismo $\varphi : \mathbb{M} \longrightarrow \mathbb{L}$ tal que $\varphi|_{\mathbb{K}} = id$ e $\varphi(\alpha) = \beta$, dizemos que α e β são conjugados sobre $\mathbb{K}$. Neste caso, α e β têm o mesmo polinômio minimal sobre $\mathbb{K}$.

Exemplo 1.7 *Se $f(x) \in \mathbb{K}[x]$ é um polinômio irredutível de grau n e se $x_1, x_2, \ldots, x_n$ são suas raízes em $\mathbb{K}(R_f)$, então as raízes $x_i's$ são duas a duas conjugadas, e os corpos $\mathbb{K}(x_i)'s$ são dois a dois conjugados.*

Proposição 1.9 *Se $\mathbb{K}$ é um corpo de característica zero, $f(x) \in \mathbb{K}[x]$ um polinômio mônico e irredutível sobre $\mathbb{K}$ e $f(x) = \prod_{i=1}^{n}(x - x_i)$ sua decomposição em produtos de fatores lineares em $\mathbb{K}(R_f)$, então as n raízes de $f(x)$ são distintas.*

Demonstração. Suponhamos que as n raízes de $f(x)$ não sejam distintas. Assim $f(x)$ e $f'(x)$ (derivada de $f(x)$) têm pelo menos uma raíz α em comum. Como $f(x)$ é um polinômio mônico e irredutível podemos supor que $f(x)$ é o polinômio minimal de α. Assim , se $f'(\alpha) = 0$ então $f(x)$ divide $f'(x)$. Como $gr(f'(x)) = n - 1$ segue que $f'(x) \equiv 0$, ou seja, dado $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$, com $a_i \in \mathbb{K}$, tem-se $f'(x) = nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1 = 0$ o que implica que $n1 = 0$, para todo $n \in \mathbb{N}$ e $ja_j = 0$, para todo $j = 1, 2, \ldots, n-1$, o que é impossível, pois $car(\mathbb{K}) = 0$. ■

Teorema 1.4 *Se $\mathbb{K}$ é um corpo de caracterítica zero, $\mathbb{L}$ uma extensão de grau n de $\mathbb{K}$ e $\mathbb{F}$ um corpo algebricamente fechado contendo $\mathbb{K}$, então existem n $\mathbb{K}$-monomorfismos distintos de $\mathbb{L}$ em $\mathbb{F}$.*

Demonstração. Se $\mathbb{L}$ é uma extensão simples de $\mathbb{K}$, ou seja, $\mathbb{L} = \mathbb{K}(\alpha)$ e $f(x) \in \mathbb{K}[x]$ o polinômio minimal de α sobre $\mathbb{K}$, então pela Proposição 1.9, segue que $f(x)$ tem n raízes distintas $\alpha_1, \alpha_2, \ldots, \alpha_n$ que pertencem a $\mathbb{F}$. Logo existem n $\mathbb{K}$-monomorfimos $\sigma_i : \mathbb{L} \longrightarrow \mathbb{F}$ tal que $\sigma_i(\alpha) = \alpha_i$, para $i = 1, 2, \ldots, n$. Agora, se $\mathbb{L}$ não é uma extensão simples de $\mathbb{K}$, mostremos o resultado por indução sobre n. Consideremos para cada $\alpha \in \mathbb{L}$, os corpos $\mathbb{K} \subseteq \mathbb{K}(\alpha) \subseteq \mathbb{L}$. Seja $q = [\mathbb{K}(\alpha) : \mathbb{K}]$ e assumimos $q > 1$. Pela primeira parte existem $\sigma_1, \sigma_2, \ldots, \sigma_q$ $\mathbb{K}$-monomorfismos distintos de $\mathbb{K}(\alpha)$ em $\mathbb{F}$. Como α e $\sigma_i(\alpha)$ têm o mesmo polinômio minimal, segue que os corpos $\mathbb{K}(\alpha)$ e $\mathbb{K}(\sigma_i(\alpha))$ são isomorfos. Consideramos $\mathbb{L}_i$

uma extensão de $\mathbb{K}(\sigma_i(\alpha))$ que é isomorfo a $\mathbb{L}$, onde ψ é tal isomorfismo. Assim, $\mathbb{K}(\sigma_i(\alpha))$ é de característica zero e $[\mathbb{L}_i : \mathbb{K}(\sigma_i(\alpha))] = [\mathbb{L} : \mathbb{K}(\alpha)] = \dfrac{n}{q} < n$. Logo, por hipótese de indução, existem $\dfrac{n}{q}$ $\mathbb{K}(\sigma_i(\alpha))$-monomorfismos τ_{ij} de $\mathbb{L}_i$ em $\mathbb{F}$, para $1 \leq j \leq \frac{n}{q}$, todos distintos. Portanto, a composição $\tau_{ij} \circ \psi_i : \mathbb{L} \longrightarrow \mathbb{F}$ é um $\mathbb{K}$-monomorfismo e como existem $q\,\dfrac{n}{q} = n$ aplicações $\tau_{ij} \circ \psi_i$, segue que existem n $\mathbb{K}$-monomorfismos de $\mathbb{L}$ em $\mathbb{F}$. Além disso, são todos distintos, pois para $i \neq i'$, tem-se que $\tau_{i'j} \circ \psi_{i'} \neq \tau_{ij} \circ \psi_i$ e para $i = i'$ e $j \neq j'$, tem-se que $\tau_{ij} \neq \tau_{ij'}$. ■

Corolário 1.8 *(Teorema do elemento primitivo) Se $\mathbb{K}$ é um corpo de característica zero e $\mathbb{L}$ é uma extensão de grau n sobre $\mathbb{K}$, então existe $\alpha \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\alpha)$, onde α é chamado de elemento primitivo.*

Demonstração. Pelo Teorema 1.4 existem n $\mathbb{K}$-monomorfismos distintos $\sigma_i : \mathbb{L} \longrightarrow \mathbb{F}$, onde $\mathbb{F}$ é um corpo algebricamente fechado. Consideramos o conjunto $V_{ij} = \{\beta \in \mathbb{L}; \sigma_i(\beta) = \sigma_j(\beta),\ i \neq j\}$. Tem-se que V_{ij} é um $\mathbb{K}$-subespaço vetorial de $\mathbb{L}$ e $V_{ij} \subsetneq \mathbb{L}$, pois em $\mathbb{L}$ tem-se que $\sigma_i(\gamma) \neq \sigma_j(\gamma)$, para algum $\gamma \in \mathbb{L}$. Como $\mathbb{K}$ é infinito, segue que $\bigcup_{i,j} V_{ij} \subsetneq \mathbb{L}$. Consideramos $\alpha \in \mathbb{L} - \bigcup_{i,j} V_{ij}$. Assim, os $\sigma_i(\alpha)'s$ são dois a dois distintos, e deste modo, o polinômio minimal de α sobre $\mathbb{K}$ tem no minímo n raízes distintas em $\mathbb{F}$. Logo, $[\mathbb{K}(\alpha) : \mathbb{K}] \geq n$ com $\mathbb{K}(\alpha) \subseteq \mathbb{L}$ e $[\mathbb{L} : \mathbb{K}] = n$. Portanto $\mathbb{L} = \mathbb{K}(\alpha)$. ■

Definição 1.15 *Seja $\mathbb{L}|\mathbb{K}$ uma extensão finita de corpos. O grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$ é o conjunto de todos os $\mathbb{K}$-automorfismos de $\mathbb{L}$, ou seja, é o conjunto $\{\sigma \in Aut(\mathbb{L});\ \sigma|_{\mathbb{K}} = id\}$. Denotamos este grupo por $Gal(\mathbb{L}|\mathbb{K})$.*

Definição 1.16 *Uma extensão finita $\mathbb{L}$ de $\mathbb{K}$ é dita uma extensão Galoisiana, ou simplesmente de Galois, se $[\mathbb{L} : \mathbb{K}] = |Gal(\mathbb{L}|\mathbb{K})|$. Uma extensão de Galois é dita abeliana (ou ciclíca) se o grupo de Galois é abeliano (ou ciclíco).*

Para os casos em que a extensão é abeliana ou ciclíca, ou seja, o grupo de Galois é abeliano ou ciclíco, faremos alguns resultados sobre grupos abelianos e ciclícos os quais são úteis para a demonstração do Teorema de Kronecker-Weber.

Lema 1.2 *Se G é um grupo ciclíco de ordem n, então existe um único subgrupo H de G de ordem d para cada d que divide n.*

Demonstração. Se G é ciclíco, então $G = \langle a \rangle$, para algum $a \in G$. Consideramos $H = \langle a^{\frac{n}{d}} \rangle$. Tem-se que H é um subgrupo de G de ordem d, pois se $b \in H$, então $b = (a^{\frac{n}{d}})^k$, o que implica que $b^d = (a^{\frac{n}{d}})^{kd} = a^{nk} = e^k = 1$, onde e é o elemento neutro de G. Suponhamos que exista um outro subgrupo S de G de ordem d. Como G é ciclíco, segue que S é ciclíco, ou seja, $S = \langle c \rangle$, para algum $c \in G$. Como $c \in G$, segue que $c = a^m$, para algum $m \in \mathbb{N}$. Tem-se que $c^d = a^{md} = 1$. Logo, $md = nk$, para algum $k \in \mathbb{N}$. Assim, $c = a^m = (a^{\frac{n}{d}})^k$. Logo, $S = \langle c \rangle$ é um subgrupo de $H = \langle a^{\frac{n}{d}} \rangle$, ambos com ordem d. Portanto, $H = S$. ■

Lema 1.3 *Se n é inteiro positivo, então $n = \sum_{d|n} \varphi(d)$, com $1 \leq d \leq n$.*

Demonstração. Se H é um subgrupo ciclíco de um grupo G e $gen(H)$ é o conjunto de todos os geradores de H, então $G = \dot{\bigcup} gen(H)$, onde H percorre todos os subgrupos ciclícos de G. Se G é ciclíco de ordem n, então para cada $d|n$ existe um único subgrupoH_d de G que é ciclíco. Portanto, $n = |G| = \sum_{d|n} gen(H_d) = \sum_{d|n} \varphi(d)$, pois se $H_d = \langle h \rangle$, então h^k é gerador de H_d se, e somente se, $mdc(k, d) = 1$. ■

Lema 1.4 *Um grupo G de ordem n é ciclíco se, e somente se, para cada d divisor de n, existe no máximo um subgrupo ciclíco de G com ordem d.*

Demonstração. Se G é ciclíco, então o resultado segue pelo Lema 1.2. Reciprocamente, tem-se pelo Lema 1.3 que $G = \dot{\bigcup} gen(H)$, onde H percorre todos os subgrupos ciclícos de G. Assim, $n = |G| = \sum |gen(H)| \leq \sum_{d|n} \varphi(d) = n$ (Lema 1.3). Logo, G tem um subgrupo ciclíco de ordem d para cada $d|n$. Em particular, $d = n$. Portanto, G é ciclíco. ■

Lema 1.5 *Seja G um grupo abeliano de ordem p^m, com p primo e $m \in \mathbb{N}$.*

a) Se H é um subgrupo de G de ordem p^r, com $r < r' \leq m$, então existe um subgrupo H' de G de ordem $p^{r'}$ tal que $H \leq H'$.

b) Se existe um único subgrupo H de G de índice p, ou seja, de ordem p^{m-1}, então G é ciclíco.

Demonstração. a) Mostramos o Lema para $r' = r+1$, e para o caso geral basta repetir o processo. Como $|H| = p^r < p^m$, segue que existe $x \in G$ tal que $x \notin H$, ou seja, existe um $\overline{x} \in \dfrac{G}{H}$ não nulo. Pelo fato de que $\left|\dfrac{G}{H}\right| = p^{m-r}$ e $p|p^{m-r}$, com $r < m$, tem-se que existe $\overline{x} \in \dfrac{G}{H}$ tal que $o(x) = p$, ou seja, $x^p \in H$. Consideramos H' o subgrupo de G gerado por H e x, isto é, $H' = H \cup Hx \cup \ldots \cup Hx^{p-1}$. Tem-se que H' é um subgrupo de G de ordem p^{r+1}. Portanto, H' é um subgrupo de G de ordem $p^{r'}$ tal que $H \leq H'$.

b) Como $|H| = p^{m-1}$, segue que existe $x \in G$ tal que $x \notin H$. Suponhamos que $\langle x \rangle \lneq G$. Como $x \notin H$, segue que $o(x) < p^{m-1}$, pois caso contrário $\langle x \rangle = H$. Assim, pelo item (a), como $o(x) < p^{m-1} < p^m$, segue que existe um subgrupo H' de G de ordem p^{m-1} que contém $\langle x \rangle$. Logo, $H' = H$, o que contraria o fato de $x \notin H$. Portanto, $G = \langle x \rangle$. ■

Definição 1.17 *Sejam $\mathbb{L}|\mathbb{K}$ uma extensão de corpos e G um subgrupo do grupo $Aut(\mathbb{L})$. O corpo*

$$\mathbb{L}^G = \{\alpha \in \mathbb{L}; \sigma(\alpha) = \alpha, \text{ para todo } \sigma \in G\}$$

é chamado corpo fixo de G.

Definição 1.18 *Uma extensão $\mathbb{L}|\mathbb{K}$ é dita normal se todo polinômio irredutível sobre $\mathbb{K}$ que tem uma raíz em $\mathbb{L}$ fatora em $\mathbb{L}$.*

Definição 1.19 *Uma extensão $\mathbb{L}|\mathbb{K}$ é dita separável sobre $\mathbb{K}$ se para todo elemento $\alpha \in \mathbb{L}$, o polinômio minimal de α sobre $\mathbb{K}$ não têm raiz múltipla no seu corpo de raízes.*

Teorema 1.5 *Seja $\mathbb{L}|\mathbb{K}$ uma extensão finita de grau n com $Gal(\mathbb{L}|\mathbb{K}) = G$. São equivalentes:*

i) $|G| = n$;

ii) $\mathbb{L}|\mathbb{K}$ é normal e separável;

iii) $\mathbb{L}$ é o corpo de raízes de um conjunto de polinômios separáveis sobre $\mathbb{K}$.

Demonstração. ([8], pág 42, Teorema 4.9) ■

Exemplo 1.8 *Toda extensão de grau 2 é uma extensão de Galois.*

Proposição 1.10 *Se* $\mathbb{L}|\mathbb{K}$ *é uma extensão de Galois e* $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$*, então a extensão* $\mathbb{L}|\mathbb{M}$ *é Galois. Além disso,* $\mathbb{M}|\mathbb{K}$ *é Galois se, e somente se,* $Gal(\mathbb{L}|\mathbb{M})$ *é um subgrupo normal de* $Gal(\mathbb{L}|\mathbb{K})$*. Neste caso,* $\dfrac{Gal(\mathbb{L}|\mathbb{K})}{Gal(\mathbb{L}|\mathbb{M})} \simeq Gal(\mathbb{M}|\mathbb{K})$.

Demonstração. ([8], pág 51, Teorema 5.1) ■

Teorema 1.6 *(Correspondência de Galois) Sejam* $\mathbb{L}|\mathbb{K}$ *uma extensão de Galois e* $G = Gal(\mathbb{L}|\mathbb{K})$*. Considerando os seguintes diagramas,*

$$\begin{array}{ccc} \mathbb{L} & \longrightarrow & \{id\} \\ | & & \\ \mathbb{M} & \longrightarrow & Gal(\mathbb{L}|\mathbb{M}) \\ | & & \\ \mathbb{K} & \longrightarrow & Gal(\mathbb{L}|\mathbb{K}) = G \end{array} \qquad \begin{array}{ccc} \mathbb{L} & \longleftarrow & \{e\} \\ | & & \\ \mathbb{L}^H & \longleftarrow & \{H\} \\ | & & \\ \mathbb{L}^G & \longleftarrow & G \end{array}$$

tem-se que existe uma correspondência entre os corpos intermediários entre $\mathbb{K}$ *e* $\mathbb{L}$ *e os subgrupos de* G*, ou seja,*

i) $\mathbb{M} = \mathbb{L}^H \Longleftrightarrow Gal(\mathbb{L}|\mathbb{M}) = H$

ii) $[\mathbb{L}^H : \mathbb{K}] = (G : H)$ *(índice de* G *sobre* H*).*

Demonstração. ([8], pág 51, Teorema 5.1) ■

Teorema 1.7 *Se* $\mathbb{L}|\mathbb{K}$ *é uma extensão finita, então existe um corpo* $\mathbb{M}$ *tal que:*

i) $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$*;*

ii) $\mathbb{K} \subseteq \mathbb{M}$ *é normal e finita;*

iii) $\mathbb{M}$ *é o menor corpo com as propriedades* (i) *e* (ii)

Demonstração. Como $\mathbb{L}|\mathbb{K}$ é finita, segue que existe uma base $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ de $\mathbb{L}$ sobre $\mathbb{K}$. Consideramos $p_i(x) = min_{\mathbb{K}}\alpha_i \in \mathbb{K}[x]$, para $i = 1, 2, \ldots, n$. Sejam $f(x) = \prod_{i=1}^{n} p_i(x)$ e $\mathbb{M}$ o corpo de raízes de $f(x)$ sobre $\mathbb{L}$ e consequentemente sobre $\mathbb{K}$. Assim, a extensão $\mathbb{M}|\mathbb{K}$ é normal, finita e $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$. Agora, suponhamos que existe um corpo $\mathbb{F}$ tal que $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{F} \subseteq \mathbb{M}$, com $\mathbb{F}|\mathbb{K}$ normal e finita. Como $\alpha_i \in \mathbb{F}$ segue que $p_i(x)$ tem uma raíz em $\mathbb{F}$. Portanto, $p_i(x)$ se fatora em $\mathbb{F}$. Mas como $\mathbb{M}$ é o corpo de raízes de $f(x)$, segue que $\mathbb{F} = \mathbb{M}$. ■

Definição 1.20 *O corpo $\mathbb{M}$ do Teorema 1.7 é chamado de fecho normal da extensão $\mathbb{L}|\mathbb{K}$.*

Teorema 1.8 *Se $\mathbb{L}|\mathbb{K}$ é uma extensão finita, então são equivalentes:*

i) $\mathbb{L}|\mathbb{K}$ *é normal;*

ii) Para toda extensão $\mathbb{M}|\mathbb{K}$, onde $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$, tem-se que todo $\mathbb{K}$-monomorfismo de $\mathbb{L}$ em $\mathbb{M}$ é um $\mathbb{K}$-automorfismo de $\mathbb{L}$;

iii) Existe uma extensão normal $\mathbb{M}|\mathbb{K}$, onde $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$, tal que todo $\mathbb{K}$-monomorfismo de $\mathbb{L}$ em $\mathbb{M}$ é um $\mathbb{K}$-automorfismo de $\mathbb{L}$.

Demonstração. $(i) \Longrightarrow (ii)$ Sejam $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ extensões de corpos e $\varphi : \mathbb{L} \longrightarrow \mathbb{M}$ um $\mathbb{K}$-monomorfismo. Como $\mathbb{L}|\mathbb{K}$ é normal, segue que $\mathbb{L}$ é o fecho normal de $\mathbb{L}$ sobre $\mathbb{K}$. Seja $\alpha \in \mathbb{L}$ e $p(x) = min_{\mathbb{K}}\alpha$. Como $\varphi(\alpha)$ e α têm o mesmo polinômio minimal sobre $\mathbb{K}$, segue que $\varphi(\alpha) \in \mathbb{L}$. Assim, $\mathbb{L}|\mathbb{K}$ é finita e $\varphi(\mathbb{L}) \subseteq \mathbb{L}$, pois se $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ e $p_i(x) = min_{\mathbb{K}}\alpha_i$, então $p_i(x)$ fatora em $\mathbb{L}$, isto é, $\varphi(\alpha_i) \in \mathbb{L}$, para $i = 1, 2, \ldots, n$. Como $\varphi : \mathbb{L} \longrightarrow \mathbb{M}$ é injetiva, segue que $\mathbb{L} \simeq \varphi(\mathbb{L}) \subseteq \mathbb{L}$. Assim, $\varphi : \mathbb{L} \longrightarrow \mathbb{L}$ é uma bijeção. Portanto, $\varphi : \mathbb{L} \longrightarrow \mathbb{L}$ é um $\mathbb{K}$-automorfismo.

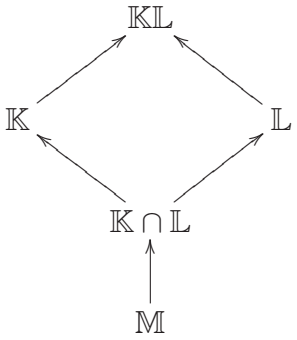
$(ii) \Longrightarrow (iii)$ Como $\varphi : \mathbb{L} \longrightarrow \mathbb{M}$ é um $\mathbb{K}$-automorfismo de $\mathbb{L}$, para qualquel $\mathbb{M}$ tal que $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$, segue que quando $\mathbb{M}$ for uma extensão normal tem-se que $\varphi : \mathbb{L} \longrightarrow \mathbb{M}$ é um $\mathbb{K}$-automorfismo de $\mathbb{L}$.

$(iii) \Longrightarrow (i)$ Sejam $\{\alpha_1, \ldots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$ e $p_i(x) = min_{\mathbb{K}}\alpha_i$. Por hipótese $p_i(x)$ se fatora em $\mathbb{M}$, para $i = 1, 2, \ldots, n$. Como α_i e $\varphi(\alpha_i)$ são conjugados, segue que existe $\varphi : \mathbb{M} \longrightarrow \mathbb{M}$ um $\mathbb{K}$-automorfismo. Por hipótese, $\varphi|_{\mathbb{L}} : \mathbb{L} \longrightarrow \mathbb{L}$ é

um $\mathbb{K}$-automorfismo, e portanto, $\varphi(\alpha_i) \in \mathbb{L}$, para $i = 1, 2, \ldots, n$. Portanto, $\mathbb{K} \subseteq \mathbb{L}$ é normal. ■

Definição 1.21 *Sejam $\mathbb{L}_1$ e $\mathbb{L}_2$ extensões de um corpo $\mathbb{K}$. O menor corpo que contém $\mathbb{L}_1$ e $\mathbb{L}_2$ é chamado de corpo composto de $\mathbb{L}_1$ e $\mathbb{L}_2$, e denotado por $\mathbb{L}_1\mathbb{L}_2$.*

Teorema 1.9 *(Irracionalidade Natural) Se $\mathbb{K}|\mathbb{M}$ é uma extensão de Galois e $\mathbb{L}|\mathbb{M}$ é uma extensão arbitrária, então $\mathbb{KL}|\mathbb{L}$ é Galois e $Gal(\mathbb{KL}|\mathbb{L}) \simeq Gal(\mathbb{K}|\mathbb{K} \cap \mathbb{L})$.*



Demonstração. Consideramos a aplicação

$$\varphi : Gal(\mathbb{KL}|\mathbb{L}) \longrightarrow Gal(\mathbb{K}|\mathbb{M})$$
$$\sigma \longmapsto \sigma|_{\mathbb{K}}$$

e mostramos que φ está bem definida. Se $\sigma \in Gal(\mathbb{KL}|\mathbb{L})$ então $\sigma|_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{KL}$ é um $\mathbb{M}$-monomorfismo. Como $\mathbb{K}|\mathbb{M}$ é normal, segue pelo Teorema 1.8, que $\sigma|_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{K}$ é um $\mathbb{M}$-automorfismo. Portanto $\sigma|_{\mathbb{K}} \in Gal(\mathbb{K}|\mathbb{M})$. Se $\sigma \in Ker(\varphi)$, então $\sigma|_{\mathbb{K}} = id_{\mathbb{K}}$. Agora, se $\sigma \in Gal(\mathbb{KL}|\mathbb{L})$, então $\sigma|_{\mathbb{L}} = id_{\mathbb{L}}$. Assim, o fato de $\sigma \in Ker(\varphi)$ significa que o corpo fixo de σ contém $\mathbb{K}$ e $\mathbb{L}$. Assim, $\sigma|_{\mathbb{KL}} = id$. Portanto, φ é um homomorfismo de grupos injetivo. Assim, $Gal(\mathbb{KL}|\mathbb{L}) \simeq Im(\varphi)$. Mostramos que $Im(\varphi) = Gal(\mathbb{K}|\mathbb{K}\cap\mathbb{L})$, ou seja, que o corpo fixo da $Im(\varphi)$ é igual $\mathbb{K} \cap \mathbb{L}$. Se $x \in \mathbb{K} \cap \mathbb{L}$, então $\sigma|_{\mathbb{K}}(x) = x$, para todo $\sigma \in Gal(\mathbb{KL}|\mathbb{L})$. Assim, x pertence ao corpo fixo da $Im(\varphi)$. Agora, se x pertencente ao corpo fixo da $Im(\varphi)$, então $x \in \mathbb{K}$ e $\sigma|_{\mathbb{K}}(x) = x$, para todo $\sigma \in Gal(\mathbb{KL}|\mathbb{L})$. Logo, $\sigma(x) = x$, para todo $\sigma \in Gal(\mathbb{KL}|\mathbb{L})$. Portanto, $x \in \mathbb{L}$. Assim, $Gal(\mathbb{KL}|\mathbb{L}) \simeq Im(\varphi) = Gal(\mathbb{K}|\mathbb{K} \cap \mathbb{L})$, e portanto, $[\mathbb{KL} : \mathbb{L}] = [\mathbb{K} : \mathbb{K} \cap \mathbb{L}]$. ■

Teorema 1.10 *Se $\mathbb{K}|\mathbb{M}$ e $\mathbb{L}|\mathbb{M}$ são extensões de Galois, então $\mathbb{KL}|\mathbb{M}$ é uma extensão de Galois.*

Demonstração. Por hipótese $\mathbb{K}$ e $\mathbb{L}$ são extensões de Galois de $\mathbb{M}$. Assim, pelo Teorema 1.5, segue que $\mathbb{K}$ e $\mathbb{L}$ são corpos de raízes de polinômios separáveis sobre $\mathbb{M}$. Sejam $f(x),\ g(x) \in \mathbb{M}[x]$ separáveis. Seja $p(x) = f(x)g(x) \in \mathbb{M}[x]$. Como $p(x)$ tem as mesmas raízes de $f(x)$ e $g(x)$, segue que o corpo de raízes de $p(x)$ é $\mathbb{KL}$. Portanto, $\mathbb{KL}|\mathbb{M}$ é uma extensão de Galois. ■

Teorema 1.11 *Sejam $\mathbb{K}|\mathbb{M}$ e $\mathbb{L}|\mathbb{M}$ extensões de Galois. Se $G = Gal(\mathbb{K}|\mathbb{M})$ e $H = Gal(\mathbb{L}|\mathbb{M})$, então a aplicação*

$$\begin{aligned} \varphi : Gal(\mathbb{KL}|\mathbb{M}) &\longrightarrow G \times H \\ \rho &\longmapsto (\rho|_{\mathbb{K}}, \rho|_{\mathbb{L}}) \end{aligned}$$

é um homomorfismo injetor. Em particular, se $\mathbb{K} \cap \mathbb{L} = \mathbb{M}$, então φ é um isomorfismo.

Demonstração. Se $\rho \in Gal(\mathbb{KL}|\mathbb{M})$ então $\rho : \mathbb{KL} \longrightarrow \mathbb{KL}$ é um automorfismo e $\rho|_{\mathbb{M}} = id$. Como $\mathbb{K}$ e $\mathbb{L}$ são extensões normais de $\mathbb{M}$ segue que $\rho|_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{KL}$ e $\rho|_{\mathbb{L}} : \mathbb{L} \longrightarrow \mathbb{KL}$ são $\mathbb{M}$-monomorfismos. Pelo Teorema 1.8, segue que $\rho|_{\mathbb{K}}$ e $\rho|_{\mathbb{L}}$ são $\mathbb{M}$-automorfismos de $\mathbb{K}$ e $\mathbb{L}$, respectivamente. Portanto, φ está bem definida. Agora, se $\rho \in Ker(\varphi)$, então $\rho|_{\mathbb{K}} = id_{\mathbb{K}}$ e $\rho|_{\mathbb{L}} = id_{\mathbb{L}}$. Assim, $\rho \in Ker(\varphi)$ se, e somente se, ρ é a aplicação identidade. Portanto, φ é injetiva. Se $\mathbb{K} \cap \mathbb{L} = \mathbb{M}$, mostremos que φ é sobrejetiva. Se $\sigma_1 \in G$, pelo Teorema 1.9, segue que existe $\sigma \in Gal(\mathbb{KL}|\mathbb{L})$ tal que $\varphi(\sigma) = (\sigma|_{\mathbb{K}}, \sigma|_{\mathbb{L}}) = (\sigma_1, id_{\mathbb{L}})$. Se $\tau_2 \in H$, pelo Teorema 1.9, segue que existe $\tau \in Gal(\mathbb{KL}|\mathbb{K})$ tal que $\varphi(\tau) = (\tau|_{\mathbb{K}}, \tau|_{\mathbb{L}}) = (id_{\mathbb{K}}, \tau_2)$. Assim, $Im(\varphi) = G \times H$. Portanto, φ é um isomorfismo, se $\mathbb{K} \cap \mathbb{L} = \mathbb{M}$. ■

Exemplo 1.9 *Sejam $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(i)$ extensões dos números racionais $\mathbb{Q}$. Como $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(i) : \mathbb{Q}] = 2$ segue, pelo Exemplo 1.8, que estas extensões são de Galois. Assim, pelo Teorema 1.11, segue que $\mathbb{Q}(\sqrt{2}, i)$ é uma extensão de Galois de $\mathbb{Q}$ e se $G = Gal(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q})$, então $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.*

1.4 Norma, traço e discriminante

Os conceitos de norma, traço, polinômio característico e discriminante são originários de conceitos de álgebra linear. Nesta seção, apresentamos definições e resultados envolvendo tais conteúdos, onde os dois últimos teoremas garantem propriedades importantes sobre o anel de inteiros. A principal referência desta seção é [7].

Sejam $A \subseteq B$ anéis e B um A-módulo livre de posto n. Consideramos para cada $x \in B$ o endomorfismo

$$\begin{aligned} \sigma_x : & B \longrightarrow B \\ & y \longmapsto xy. \end{aligned}$$

Pela álgebra linear sabemos que σ_x tem uma representação matricial $[a_{ij}]$, ou seja, se $\{e_1, e_2, \ldots, e_n\}$ é uma base de B sobre A, então

$$\begin{cases} \sigma_x(e_1) = a_{11}e_1 + a_{12}e_2 + \ldots + a_{1n}e_n \\ \sigma_x(e_2) = a_{21}e_1 + a_{22}e_2 + \ldots + a_{2n}e_n \\ \vdots \\ \sigma_x(e_n) = a_{n1}e_1 + a_{n2}e_2 + \ldots + a_{nn}e_n. \end{cases}$$

Assim,

$$\begin{bmatrix} \sigma_x(e_1) \\ \sigma_x(e_2) \\ \vdots \\ \sigma_x(e_n) \end{bmatrix} = \begin{bmatrix} \ a_{ij} \ \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{bmatrix}.$$

Definição 1.22 *Sejam $A \subseteq B$ anéis, B um A-módulo livre de posto n e $x \in B$. O traço de $x \in B$ é definido por $Tr_{B|A}(x) = Tr_{B|A}(\sigma_x) = \sum_{i=1}^{n} a_{ii}$, a norma de $x \in B$ por $N_{B|A}(x) = \det([a_{ij}])$ e o polinômio característico de $x \in B$ por $p_{B|A}(x) = \det(xId - \sigma_x)$.*

Assim dados $x, y \in B$ tem-se

$$Tr_{B|A}(x+y) = Tr_{B|A}(x) + Tr_{B|A}(y),$$
$$N_{B|A}(xy) = N_{B|A}(x)N_{B|A}(y),$$
$$p_{B|A}(x) = \det(xId - \sigma_x) = x^n + Tr_{B|A}(\sigma_x)x^{n-1} + \ldots + (-1)^n \det \sigma_x.$$

Propriedades 1.1 *Sejam $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L}$ corpos, onde $\mathbb{K} \subseteq \mathbb{L}$ é uma extensão finita. Se $x, y \in \mathbb{L}$ e $a \in \mathbb{K}$ valem as seguintes propriedades:*

a) $Tr_{\mathbb{L}|\mathbb{K}}(ax) = aTr_{\mathbb{L}|\mathbb{K}}(x)$

b) $Tr_{\mathbb{L}|\mathbb{K}}(a) = [\mathbb{L} : \mathbb{K}]a$

c) $N_{\mathbb{L}|\mathbb{K}}(a) = a^{[\mathbb{L}:\mathbb{K}]}$

d) $N_{\mathbb{L}|\mathbb{K}}(ax) = a^{[\mathbb{L}:\mathbb{K}]}N_{\mathbb{L}|\mathbb{K}}(x)$

e se $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ tem-se que

e) $N_{\mathbb{L}|\mathbb{K}}(x) = N_{\mathbb{M}|\mathbb{K}}(N_{\mathbb{L}|\mathbb{M}}(x))$

f) $Tr_{\mathbb{L}|\mathbb{K}}(x) = Tr_{\mathbb{M}|\mathbb{K}}(Tr_{\mathbb{L}|\mathbb{M}}(x))$. ■

Proposição 1.11 *Se $\mathbb{K}$ é um corpo de característica zero, $\mathbb{L}$ uma extensão de grau n de $\mathbb{K}$, $\alpha \in \mathbb{L}$ e $\alpha_1, \alpha_2, \ldots, \alpha_n$ raízes do polinômio minimal de α sobre $\mathbb{K}$, então $Tr_{\mathbb{L}|\mathbb{K}}(\alpha) = \alpha_1 + \alpha_2 + \ldots + \alpha_n$, $N_{\mathbb{L}|\mathbb{K}}(\alpha) = \alpha_1\alpha_2 \ldots \alpha_n$ e o polinômio característico de α sobre $\mathbb{K}$ é $p_{\mathbb{L}|\mathbb{K}}(x) = (x - \alpha_1) \ldots (x - \alpha_n)$.*

Demonstração. Se α é um elemento primitivo de $\mathbb{L}$ sobre $\mathbb{K}$, então $\mathbb{L} = \mathbb{K}(\alpha)$. Assim, $\mathbb{L} \simeq \dfrac{\mathbb{K}[x]}{\langle f(x) \rangle}$, onde $f(x)$ é o polinômio minimal de α sobre $\mathbb{K}$. Logo, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é base de $\mathbb{L}$ sobre $\mathbb{K}$. Seja $\sigma_\alpha : \mathbb{L} \longrightarrow \mathbb{L}$ dada por $\sigma_\alpha(x) = \alpha x$. Consideramos M a matriz de σ_α em relação a base $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Logo,

$$M = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}.$$

Como $p_{\mathbb{L}|\mathbb{K}}(\alpha) = \det(\alpha Id - M)$, segue que

$$p_{\mathbb{L}|\mathbb{K}}(x) = det \begin{bmatrix} \alpha & 0 & \cdots & 0 & -a_0 \\ 1 & \alpha & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}.$$

Por definição tem-se que, $p_{\mathbb{L}|\mathbb{K}}(x) = x^n + (TrM)\alpha^{n-1} + \ldots + (-1)^n detM$. Como α é primitivo, segue que $p_{\mathbb{L}|\mathbb{K}}(x) = (x-\alpha_1)\ldots(x-\alpha_n) = x^n - \left(\sum_{i=1}^{n} \alpha_i\right) x^{n-1} + \ldots + \left(\prod_{i=1}^{n} \alpha_i\right)$. Logo, $Tr_{\mathbb{L}|\mathbb{K}}(\alpha) = \sum_{i=1}^{n} \alpha_i$ e $N_{\mathbb{L}|\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \alpha_i$ e $p_{\mathbb{L}|\mathbb{K}}(x) = f(x) = (x - \alpha_1)\ldots(x - \alpha_n)$. Agora, se α não é um elemento primitivo, consideremos $r = [\mathbb{L} : \mathbb{K}(\alpha)]$. Mostramos que se $\overline{M}$ é a matriz do endomorfismo $\overline{\sigma}_\alpha : \mathbb{L} \longrightarrow \mathbb{L}$ definida por $\overline{\sigma}_\alpha(\beta) = \alpha\beta$, então $\overline{M}$ é uma matriz formada por blocos na diagonal, onde cada um desses blocos é igual a M. Sejam $\{y_i\}_{1\leq i\leq q}$ uma base de $\mathbb{K}(\alpha)$ sobre $\mathbb{K}$ e $\{z_j\}_{1\leq j\leq r}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}(\alpha)$. Logo, $\{y_i z_j\}_{(i,j)\in I\times J}$, onde $I = \{1, 2, \ldots, q\}$ e $J = \{1, 2, \ldots, r\}$, é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Seja $M = [a_{ih}]$ a matriz de multiplicação por α em $\mathbb{K}(\alpha)$. Assim, $\alpha y_i = \sum_{h=1}^{q} a_{ih} y_h$ e $\alpha y_i z_j = \left(\sum_{h=1}^{q} a_{ih} y_h\right) z_j = \sum_{h=1}^{q} a_{ih}(y_h z_j)$. Logo,

$$\overline{M} = \begin{bmatrix} M & 0 & \cdots & 0 \\ 0 & M & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & M \end{bmatrix}.$$

Como $n = qr$, segue que a matriz M aparece r-vezes na diagonal de $\overline{M}$. Logo, $det(xId_n - \overline{M}) = (det(xId_q - M))^r$. Portanto, o polinômio característico de α é uma r-ésima potência do polinômio minimal de α. ■

Observação 1.2 *Pelas Propriedades 1.1, se* $r = [\mathbb{L} : \mathbb{K}(\alpha)]$ *então*

1) $Tr_{\mathbb{L}|\mathbb{K}}(\alpha) = rT_{\mathbb{K}(\alpha)|\mathbb{K}}(\alpha)$,

2) $N_{\mathbb{L}|\mathbb{K}}(\alpha) = (N_{\mathbb{K}(\alpha)|\mathbb{K}}(\alpha))^r$,

3) $p_{\mathbb{L}|\mathbb{K}}(x) = (p_{\mathbb{K}(\alpha)|\mathbb{K}}(x))^r$.

Exemplo 1.10 *Seja* $\mathbb{L} = \mathbb{Q}(\sqrt{2})$ *extensão de* $\mathbb{Q}$. *Como* $\{1, \sqrt{2}\}$ *é uma base de* $\mathbb{L}$ *sobre* $\mathbb{Q}$, *segue que*

$$[a_{ij}] = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}.$$

Assim, $Tr_{\mathbb{L}|\mathbb{Q}}(\sqrt{2}) = 0, N_{\mathbb{L}|\mathbb{Q}}(\sqrt{2}) = -2$ *e* $p_{\mathbb{L}|\mathbb{Q}}(\sqrt{2}) = x^2 - 2$. *Agora, se* $\mathbb{L} = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$, $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ *e* $\alpha = 3 + \sqrt{2}$, *então* $Tr_{\mathbb{L}|\mathbb{Q}}(\alpha) = [\mathbb{L} : \mathbb{K}]Tr_{\mathbb{K}|\mathbb{Q}}(\alpha) = 12$, $N_{\mathbb{L}|\mathbb{Q}}(\alpha) = (N_{\mathbb{K}|\mathbb{Q}}(\alpha))^2 = 7^2 = 49$ *e* $p_{\mathbb{L}|\mathbb{Q}}(x) = (p_{\mathbb{K}|\mathbb{Q}}(x))^2 = (x^2 - 6x + 7)^2$.

Proposição 1.12 *Sejam* A *um domínio de integridade,* $\mathbb{K}$ *seu corpo de frações,* $\mathbb{L}$ *uma extensão finita de* $\mathbb{K}$ *e* $\alpha \in \mathcal{O}_{\mathbb{L}}$. *Se* $\mathbb{K}$ *é de característica zero, então os coeficientes do polinômio característico* $p_{\mathbb{L}|\mathbb{K}}(x)$, *em particular, o* $Tr_{\mathbb{L}|\mathbb{K}}(\alpha)$ *e* $N_{\mathbb{L}|\mathbb{K}}(\alpha)$, *são inteiros sobre* A. *No caso de* A *ser integralmente fechado, tem-se que* $Tr_{\mathbb{L}|\mathbb{K}}(\alpha)$ *e* $N_{\mathbb{L}|\mathbb{K}}(\alpha)$ *são elementos de* A.

Demonstração. Pela Proposição 1.11, tem-se que $p_{\mathbb{L}|\mathbb{K}}(x) = (x - \alpha_1)\ldots(x - \alpha_n)$. Assim, os coeficientes de $p_{\mathbb{L}|\mathbb{K}}(x)$ são somas e produtos dos $\alpha_i's$. Logo, basta mostrar que $\alpha_i \in \mathcal{O}_{\mathbb{L}}$, para $i = 1, 2, \ldots, n$. Como α e α_i tem o mesmo polinômio minimal segue que existe um $\mathbb{K}$-isomorfismo

$$\sigma_i : \mathbb{K}(\alpha) \longrightarrow \mathbb{K}(\alpha_i)$$
$$\alpha \longmapsto \alpha_i$$

para $i = 1, 2, \ldots, n$. Se $\alpha \in \mathcal{O}_{\mathbb{L}}$, então existem $a_0, a_1, \ldots, a_{n-1} \in A$, não todos nulos, tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$. Aplicando σ_i tem-se que $\sigma_i(\alpha^n) + a_{n-1}\sigma_i(\alpha^{n-1}) + \ldots + a_0 = 0$, ou seja, $(\sigma_i(\alpha))^n + a_{n-1}(\sigma(\alpha))^{n-1} + \ldots + a_0 = 0$. Portanto $\sigma_i(\alpha) = \alpha_i \in \mathcal{O}_{\mathbb{L}}$, para $i = 1, 2, \ldots, n$. ■

Definição 1.23 *Sejam* $A \subseteq B$ *anéis e* B *um* A*-módulo livre de posto* n. *Para* $\{x_1, x_2, \ldots, x_n\} \subseteq B$ *chamamos de discriminante do conjunto* $\{x_1, \ldots, x_n\}$ *o elemento de* A *dado por*

$$D(x_1, x_2, \ldots, x_n) = det(Tr_{B|A}(x_i x_j)).$$

Definição 1.24 *Sejam $A \subseteq B$ anéis, B um A-módulo livre de posto n e $\{x_1, x_2, \ldots, x_n\}$ base de B sobre A. Chamamos de discriminante de B sobre A o ideal de A gerado por $D(x_1, x_2, \ldots, x_n)$ e denotamos por $\mathfrak{D}_{B|A}$.*

Lema 1.6 *(Lema de Dedekind) Sejam G um grupo e $\mathbb{K}$ um corpo. Se $\sigma_1, \sigma_1, \ldots, \sigma_n$ são os homomorfismos distintos de G no grupo multiplicativo $\mathbb{K}^*$, então os $\sigma_i's$ são linearmente independentes sobre $\mathbb{K}$.*

Demonstração. Suponhamos que os $\sigma_i's$ sejam linearmente dependentes, ou seja, que existam $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{K}$, não todos nulos, tal que $\sum_{i=1}^{n} \alpha_i\sigma_i = 0$. Suponhamos que o número q dos $\sigma_i's$ não nulos seja o menor possível. Assim,

$$\alpha_1\sigma_1(g) + \ldots + \alpha_q\sigma_q(g) = 0, \text{ para todo } g \in G, \tag{1.5}$$

onde $q \geq 2$, pois $\alpha_i's$ são não nulos. Como, $\sigma_i \neq \sigma_j$, para todo $i \neq j$, segue que existe $h \in G$ tal que $\sigma_i(h) \neq \sigma_j(h)$, para todo $i \neq j$. Assim,

$$\alpha_1\sigma_1(g)\sigma_1(h) + \ldots + \alpha_q\sigma_q(g)\sigma_q(h) = 0, \text{ para todo } g \in G. \tag{1.6}$$

Multiplicando a Equação (1.5) por $\sigma_1(h)$ e subtraindo da Equação (1.6), tem-se que

$$\alpha_2(\sigma_1(h) - \sigma_2(h))\sigma_2(g) + \ldots + \alpha_q(\sigma_1(h) - \sigma_q(h))\sigma_q(g) = 0.$$

Logo, existe $p = q - 1$ tal que $\sum_{j=1}^{p} \beta_j\sigma_j = 0$, onde $\beta_j = \alpha_{j+1}(\sigma_1(h) - \sigma_{j+1}(h))$. Pela minimalidade de q, segue que $\beta_j = 0$. Como $\alpha_{j+1} \neq 0$, para todo j, segue que $\sigma_1(h) = \sigma_{j+1}(h)$, para todo j, o que contraria o fato de $\sigma_1(h) \neq \sigma_2(h)$. Portanto, os $\sigma_i's$ são linearmente independentes. ■

Proposição 1.13 *Se $\mathbb{K}$ é um corpo de característica zero, $\mathbb{L}$ uma extensão de grau n sobre $\mathbb{K}$ e $\sigma_1, \ldots, \sigma_n$ $\mathbb{K}$-monomorfismos distintos de $\mathbb{L}$ em um corpo algebricamente fechado $\mathbb{F}$ contendo $\mathbb{K}$, então*

$$D(x_1, x_2, \ldots, x_n) = det(\sigma_i(x_j))^2 \neq 0,$$

onde $\{x_1, x_2, \ldots, x_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$.

Demonstração. Tem-se que

$$D(x_1, x_2, \ldots, x_n) = det(Tr_{\mathbb{L}|\mathbb{K}}(x_i x_j)) = det\left(\sum_{k=1}^{n} \sigma_k(x_i x_j)\right) = det\left(\sum_{k=1}^{n} \sigma_k(x_i)\sigma_k(x_j)\right).$$

Como

$$\left[\begin{array}{c} \sum_{k=1}^{n} \sigma_k(x_i x_j) \end{array}\right] = \left[\begin{array}{cccc} \sigma_1(x_1) & \sigma_2(x_1) & \cdots & \sigma_n(x_1) \\ \sigma_1(x_2) & \sigma_2(x_2) & \cdots & \sigma_n(x_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(x_n) & \sigma_2(x_n) & \cdots & \sigma_n(x_n) \end{array}\right] \left[\begin{array}{cccc} \sigma_1(x_1) & \sigma_1(x_2) & \cdots & \sigma_1(x_n) \\ \sigma_2(x_1) & \sigma_2(x_2) & \cdots & \sigma_2(x_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(x_1) & \sigma_n(x_2) & \cdots & \sigma_n(x_n) \end{array}\right],$$

segue que $D(x_1, x_2, \ldots, x_n) = det(\sigma_k(x_i))det(\sigma_k(x_j)) = (det(\sigma_i(x_j)))^2$. Agora, suponhamos que $det(\sigma_i(x_j)) = 0$. Assim, existem $c_1, c_2, \ldots, c_n \in \mathbb{F}$, não todos nulos, tal que $\sum_{i=1}^{n} c_i\sigma_i(x_j) = 0$, para algum $j = 1, 2, \ldots, n$. Logo, para qualquer $\alpha \in \mathbb{L}$, tem-se que $\sum_{i=1}^{n} c_i\sigma_i(\alpha) = \sum_{i=1}^{n} c_i\sigma_i\left(\sum_{j=1}^{n} a_j x_j\right) = \sum_{i,j=1}^{n} c_i a_j \sigma_i(x_j) = 0$, ou seja, os $\sigma_i's$ são linearmente dependentes, o que contraria o Lema de Dedekind. ■

Proposição 1.14 *Se $\mathbb{K}$ é um corpo de característica zero, $\mathbb{L} = \mathbb{K}(\alpha)$ uma extensão de grau n de $\mathbb{K}$ e $p(x) = min_{\mathbb{K}}\alpha$,então*

$$D(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{L}|\mathbb{K}}(p'(\alpha)),$$

onde $p'(x)$ é a derivada de $p(x)$.

Demonstração. Como $\mathbb{L} = \mathbb{K}[\alpha]$ e $[\mathbb{L} : \mathbb{K}] = n$, segue que $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Assim, pela Proposição 1.13, segue que $D(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = det(\sigma_i(\alpha^j))^2$, onde os σ_i's são os $\mathbb{K}$-monomorfismos de $\mathbb{L}$, para $1 \leq i \leq n$. Como $det(\sigma_i(\alpha^j))$ é um determinante de Vardermonde, segue que $det(\sigma_i(\alpha^j)) = \prod_{i<j}(\alpha^j - \alpha^i)$. Logo, $D(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = \prod_{i<j}(\alpha^j - \alpha^i)^2$, onde os α^i são os conjugados de α, para $1 \leq i \leq n$. Como $p(x) = min_{\mathbb{K}}\alpha = \prod_{i=1}^{n}(x - \alpha^i)$, segue que $p'(x) = \sum_{i=1}^{n}(\prod_{i=1,\ i\neq j}^{n}(x - \alpha^i))$. Logo, $p'(\alpha) = \prod_{i=1}^{n}(\alpha^i - \alpha^j)$. Assim,

$$\prod_{j=1}^{n} p'(\alpha) = \prod_{j=1}^{n}\prod_{i=1}^{n}(\alpha^j - \alpha^i) = \prod_{i=1,\ i\neq j}^{n}(\alpha^j - \alpha^i). \tag{1.7}$$

Observemos que $N(p'(x)) = \prod_{j=1}^{n} \sigma_j(p'(\alpha)) = \prod_{j=1}^{n} p'(\alpha^j)$, onde $p'(\alpha^j)$ são conjugados de $p'(\alpha)$. Como cada fator $\alpha^j - \alpha^i$ aparece duas vezes, uma como $\alpha^j - \alpha^i$ e outra como $\alpha^i - \alpha^j$, segue que o produto desses fatores é $-(\alpha^j - \alpha^i)^2$. Assim, $\prod_{i=1,\ i\neq j}^{n} (\alpha^j - \alpha^i) = \prod_{i=1,\ i\neq j}^{n} -(\alpha^j - \alpha^i)^2 = (-1)^k \prod_{i<j} (\alpha^j - \alpha^i)^2$, onde $k = \frac{n(n-1)}{2}$ é o número de pares (i, j). Logo, pela Equação (1.7), obtemos $D(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{L}|\mathbb{K}}(p'(\alpha))$. ■

Observação 1.3 *Nas hipóteses da Proposição 1.13, o fato de* $D(x_1, \ldots, x_n) \neq 0$ *significa que a aplicação bilinear* $\varphi : \mathbb{L} \times \mathbb{L} \longrightarrow \mathbb{K}$ *tal que* $\varphi(x, y) = Tr_{\mathbb{L}|\mathbb{K}}(xy)$ *é não degenerada, ou seja, que para cada* $x \neq 0$ *o funcional linear* $\varphi(x, \bullet) : \mathbb{L} \longrightarrow \mathbb{K}$ *é tal que* $\varphi(x, y) = Tr_{\mathbb{L}|\mathbb{K}}(xy) \neq 0$. *Logo, a aplicação* $\psi : \mathbb{L} \longrightarrow \mathcal{L}(\mathbb{L}, \mathbb{K}) = \mathbb{L}^*$ *tal que* $\psi(x) = \varphi(x, \bullet)$ *é injetiva. Como* $dim_{\mathbb{K}}\mathbb{L} = dim_{\mathbb{K}}\mathbb{L}^*$, *segue que* ψ *é um isomorfismo. Assim, se* $\{x_1, \ldots, x_n\}$ *é uma base de* $\mathbb{L}$ *sobre* $\mathbb{K}$, *então existe uma única base dual* $\{x_1^*, \ldots, x_n^*\} = \{y_1, \ldots, y_n\}$ *tal que* $Tr_{\mathbb{L}|\mathbb{K}}(x_i y_j) = \delta_{ij}$, *para* $1 \leq i, j \leq n$.

Teorema 1.12 *Sejam* A *um anel integralmente fechado,* $\mathbb{K}$ *seu corpo de frações,* $\mathbb{L}$ *uma extensão finita de* $\mathbb{K}$ *e* $\mathcal{O}_{\mathbb{L}}$ *o anel de inteiro de* $\mathbb{L}$ *sobre* A. *Se* $\mathbb{K}$ *é de característica zero, então* $\mathcal{O}_{\mathbb{L}}$ *é um* A*-submódulo de um* A*-módulo livre de posto* n.

Demonstração. Como $\mathbb{L}|\mathbb{K}$ é finita, segue que existe uma base $\{x_1, x_2, \ldots, x_n\}$ de $\mathbb{L}$ sobre $\mathbb{K}$, onde cada x_i é algébrico sobre $\mathbb{K}$. Assim, para cada x_i existe uma equação da forma

$$a_{in}x_i^n + a_{in-1}x_i^{n-1} + \ldots + a_{i0} = 0, \text{ onde } a_{ij} \in \mathbb{K}, \text{ para } 0 \leq j \leq n. \tag{1.8}$$

Assumimos $a_{in} \neq 0$, e multiplicamos a Equação 1.8 por $a_{in}^{n-1} \in \mathbb{K}$. Logo,

$$(a_{in}x_i)^n + a_{in-1}(a_{in}x_i)^{n-1} + \ldots + a_{i1}a_{in}^{n-2}(a_{in}x_i) + a_{i0}a_{in}^{n-1} = 0,$$

ou seja, $a_{in}x_i$ é inteiro sobre A. Assim, se $y_i = a_{in}x_i$, então $\{y_1, \ldots, y_n\} \subseteq \mathcal{O}_{\mathbb{L}}$. Mostramos que $\{y_1, \ldots, y_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Se $b_1y_1 + \ldots + b_ny_n = 0$, então $b_1a_{in}x_i + \ldots + b_na_{nn}x_n = 0$, e como $\{x_1, \ldots, x_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, segue que $b_ia_{in} = 0$, para $i = 1, 2, \ldots, n$. Como $a_{in} \neq 0$, segue que $b_i = 0$, para $i = 1, 2, \ldots, n$. Logo, $\{y_1, \ldots, y_n\}$

é um conjunto linearmente independente com n elementos, e portanto é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Pela Observação 1.3, segue que existe uma base $\{z_1, \ldots, z_n\}$ de $\mathbb{L}$ sobre $\mathbb{K}$ tal que $Tr(y_i z_j) = \delta_{ij}$. Se $w \in \mathcal{O}_{\mathbb{L}} \subseteq \mathbb{L}$, então $w = \sum_{j=1}^{n} c_j z_j$, onde $c_j \in \mathbb{K}$. Como $y_i \in \mathcal{O}_{\mathbb{L}}$, para $i = 1, 2, \ldots, n$, segue que $y_i w \in \mathcal{O}_{\mathbb{L}}$, para $i = 1, 2, \ldots, n$. Assim, pela Proposição 1.12, segue que $Tr_{\mathbb{L}|\mathbb{K}}(y_i w) \in A$. Logo, $Tr_{\mathbb{L}|\mathbb{K}}(y_i w) = Tr_{\mathbb{L}|\mathbb{K}}\left(\sum_{j=1}^{n} c_j y_i z_j\right) = \sum_{j=1}^{n} c_j Tr_{\mathbb{L}|\mathbb{K}}(y_i z_j) = \sum_{j=1}^{n} c_j \delta_{ij} = c_i \in A$, para $i = 1, 2, \ldots, n$. Portanto, $\mathcal{O}_{\mathbb{L}}$ é um A-submódulo do A-módulo livre M de posto n, onde M é gerado por $\{z_1, \ldots, z_n\}$. ■

Corolário 1.9 *Sejam A um anel integralmente fechado, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiro de $\mathbb{L}$ sobre A. Se A é principal e $\mathbb{K}$ tem característica zero, então $\mathcal{O}_{\mathbb{L}}$ é um A-módulo livre de posto n.*

Demonstração. Como A é principal, segue pelo Teorema 1.2 que todo A-submódulo de um A-módulo livre de posto n é livre e tem posto menor ou igual a n. Pela demonstração do Teorema 1.12, tem-se que $\mathcal{O}_{\mathbb{L}}$ contém uma base de $\mathbb{L}$ sobre $\mathbb{K}$, o que implica que o posto de $\mathcal{O}_{\mathbb{L}}$ é n. ■

Teorema 1.13 *Sejam A um anel integralmente fechado e Noetheriano, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de $\mathbb{L}$ sobre A. Se $\mathbb{K}$ tem característica zero, então $\mathcal{O}_{\mathbb{L}}$ é um A-módulo finitamente gerado e Noetheriano.*

Demonstração. Pelo Teorema 1.12, tem-se que $\mathcal{O}_{\mathbb{L}}$ é um A-submódulo de um A-módulo livre de posto n. Pelo Corolário 1.2, segue que este A-módulo livre de posto n é Noetheriano, e assim, $\mathcal{O}_{\mathbb{L}}$ é finitamente gerado. Pelo Corolario 1.2, tem-se que $\mathcal{O}_{\mathbb{L}}$ é um A-módulo Noetheriano. Agora, consideramos $\mathcal{O}_{\mathbb{L}}$ como um $\mathcal{O}_{\mathbb{L}}$-módulo. Tem-se que os $\mathcal{O}_{\mathbb{L}}$-submódulo de $\mathcal{O}_{\mathbb{L}}$ são os ideais de $\mathcal{O}_{\mathbb{L}}$. Como $A \subseteq \mathcal{O}_{\mathbb{L}}$, segue que os $\mathcal{O}_{\mathbb{L}}$-submódulos de $\mathcal{O}_{\mathbb{L}}$ são também A-submódulos de $\mathcal{O}_{\mathbb{L}}$, e assim, qualquer sequência crescente de $\mathcal{O}_{\mathbb{L}}$-submódulos é estacionária. Portanto, $\mathcal{O}_{\mathbb{L}}$ é um anel Noetheriano. ■

1.5 Corpos quadráticos e ciclotômicos

Nesta seção, apresentamos casos particulares de extensões dos números racionais. Explicitamos o anel de inteiros e os discriminantes dessas extensões. Os discriminantes serão de grande utilidade no Capítulo 2 e na demonstração do Teorema de Kronecker-Weber. As principais referências desta seção são [2], [7], [12], [14] e [16].

Definição 1.25 *Um corpo $\mathbb{K}$ é chamado corpo de números se $\mathbb{K}$ é uma extensão finita de $\mathbb{Q}$. Se $[\mathbb{K}:\mathbb{Q}]=2$, dizemos que $\mathbb{K}$ é um corpo quadrático.*

Observação 1.4 *1) Pelo Teorema do Elemento Primitivo, segue que existe $\alpha \in \mathbb{K}$ tal que $\mathbb{Q}(\alpha)=\mathbb{K}$. Assim, se $\mathbb{K}$ é um corpo quadrático, então $min_{\mathbb{K}}\alpha = x^2+bx+c \in \mathbb{Q}[x]$. Como $\alpha = \dfrac{-b \pm \sqrt{b^2-4c}}{2}$, segue que $\mathbb{K}=\mathbb{Q}(\sqrt{b^2-4c})$. Como $b,c \in \mathbb{Q}$, segue que $b^2-4c \in \mathbb{Q}$. Assim, existem $\alpha,\beta \in \mathbb{Z}$, $\beta \neq 0$, tal que $b^2-4c = \dfrac{\alpha}{\beta} = \dfrac{\alpha\beta}{\beta^2}$. Logo $\mathbb{K}=\mathbb{Q}(\sqrt{b^2-4c})=\mathbb{Q}(\sqrt{\alpha\beta})$. Decompondo $\alpha\beta$ em fatores primos tem-se que $\alpha\beta=\omega^2 d$, onde d é livre de quadrados. Portanto, podemos considerar $\mathbb{K}=\mathbb{Q}(\sqrt{d})$, onde $d \in \mathbb{Z}$ é livre de quadrados.*

2) As raízes do polinômio irredutível $x^2-d \in \mathbb{Q}[x]$ são $\sqrt{d}$ e $-\sqrt{d}$. Logo, existe um $\mathbb{Q}$-automorfismo de $\mathbb{K}$, $\varphi : \mathbb{K} \longrightarrow \mathbb{K}$, tal que $\varphi(\sqrt{d})=-\sqrt{d}$.

3) Se $\mathbb{K}=\mathbb{Q}(\sqrt{d})$, onde $d \in \mathbb{Z}$ é livre de quadrados, então $[\mathbb{K}:\mathbb{Q}]=2$ e assim a extensão $\mathbb{K}|\mathbb{Q}$ é uma extensão de Galois.

Teorema 1.14 *Seja $\mathbb{K}=\mathbb{Q}(\sqrt{d})$, onde $d \in \mathbb{Z}$ é livre de quadrados. Se $\alpha = a+b\sqrt{d}$, onde $a,b \in \mathbb{Q}$, é um inteiro algébrico, então $2a$, a^2-db^2 e $2b \in \mathbb{Z}$.*

Demonstração. Se α é inteiro algébrico, então existem $a_0,\ldots,a_{n-1} \in \mathbb{Z}$ tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$. Seja $\sigma \in Aut(\mathbb{K})$ tal que $\sigma(a+b\sqrt{d}) = a-b\sqrt{d}$. Assim, $\sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \ldots + a_0 = 0$, ou seja, $\sigma(\alpha)$ é inteiro algébrico de $\mathbb{K}$. Portanto, $\alpha+\sigma(\alpha)=2a \in \mathbb{Q}$ e $\alpha\sigma(\alpha)=a^2-b^2d \in \mathbb{Q}$ são inteiros algébricos de $\mathbb{K}$. Como $\mathbb{Z}$ é um anel principal, segue que $\mathbb{Z}$ é integralmente fechado, e portanto, $2a$ e $a^2-b^2d \in \mathbb{Z}$. Assim, $4a^2-d4b^2=(2a)^2-d(2b)^2 \in \mathbb{Z}$. Como $2a \in \mathbb{Z}$, segue que $(2a)^2 \in \mathbb{Z}$, e assim $d(2b)^2 \in \mathbb{Z}$.

Se $2b \notin \mathbb{Z}$, então $b = \frac{q}{p}$, onde $mdc(q,p) = 1$. Logo, $d(2b)^2 = \frac{d4q^2}{p^2}$. Como d é livre de quadrados, segue que $d(2b)^2 \notin \mathbb{Z}$, o que é um absurdo. Portanto, $2b \in \mathbb{Z}$. ■

Teorema 1.15 *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, onde $d \in \mathbb{Z}$ é livre de quadrados e $d \notin 4\mathbb{Z}$.*

a) Se $d \equiv 2$ ou $d \equiv 3$ $(mod\ 4)$, então o anel dos inteiros algébricos de $\mathbb{K}$ é $\mathbb{Z}[\sqrt{d}]$.

b) Se $d \equiv 1$ $(mod\ 4)$, então o anel dos inteiros algébricos de $\mathbb{K}$ é $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

Demonstração. Seja $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ um inteiro algébrico e coloquemos $a = \frac{u}{2}$ e $b = \frac{v}{2}$. Pelo Teorema 1.14, segue que $2a = u,\ 2b = v \in \mathbb{Z}$ e $\frac{u^2}{4} - \frac{v^2}{4}d \in \mathbb{Z}$. Logo, $u, v \in \mathbb{Z}$ e $u^2 - v^2 d \in 4\mathbb{Z}$.

a) Para mostrar que $\alpha \in \mathbb{Z}[\sqrt{d}]$ devemos mostrar que $a, b \in \mathbb{Z}$, ou seja, u e v são pares (pertencem a $2\mathbb{Z}$). Suponhamos v ímpar. Assim $v = 2k + 1$, para algum $k \in \mathbb{N}$. Logo, $v^2 = 4(k^2 + k) + 1 \equiv 1(mod\ 4)$. Como $u^2 \equiv v^2 d(mod\ 4)$, segue que $u^2 \equiv d(mod\ 4)$. Assim, $d \equiv 1(mod\ 4)$ se u é ímpar ou $d \equiv 0(mod\ 4)$ se u é par, o que contraria a hipótese. Portanto, v é par. Logo $u^2 \equiv v^2 d(mod\ 4)$ implica que $u^2 \equiv 0(mod\ 4)$, ou seja, u é par. Portanto, u e v são pares e $\alpha \in \mathbb{Z}[\sqrt{d}]$. Seja $\alpha \in \mathbb{Z}[\sqrt{d}]$. Temos que α é raiz do polinômio $x^2 - 2ax + a^2 - b^2 d \in \mathbb{Z}[x]$, pois $2a$ e $a^2 - b^2 d \in \mathbb{Z}$. Deste modo, todo $\alpha \in \mathbb{Z}[\sqrt{d}]$ é um inteiro algébrico de $\mathbb{K}$. Portanto, $\mathbb{Z}[\sqrt{d}]$ é o anel de inteiros de $\mathbb{K}$.

b) Seja $d \equiv 1(mod\ 4)$. Logo $u^2 \equiv v^2(mod\ 4)$, e assim u e v tem a mesma paridade. Se u e v são pares, então $a,\ b \in \mathbb{Z}$. Logo, $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Se u e v são ímpares, então $\alpha = a + b\sqrt{d} = \frac{u}{2} + \frac{v}{2}\sqrt{d} = u\frac{1}{2} + v\frac{\sqrt{d}}{2} = u\frac{1}{2} - v\frac{1}{2} + v\frac{1}{2} + v\frac{\sqrt{d}}{2} = \frac{u-v}{2} + v\left(\frac{1}{2} + \frac{\sqrt{d}}{2}\right)$. Como u e v são ímpares, segue que $\frac{u-v}{2} \in \mathbb{Z}$, e assim $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Logo, $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Reciprocamente, se $\alpha = a + b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, então $2a + b \in \mathbb{Z}$ e $\left(a + \frac{b}{2}\right)^2 - d\left(\frac{b}{2}\right)^2 = a^2 + ab - (1-d)\frac{b^2}{4} \in \mathbb{Z}$, pois $d \equiv 1(mod\ 4)$. Assim, α é raíz do polinômio $x^2 - (2a+b)x + a^2 + ab + (1-d)\frac{b^2}{4} \in \mathbb{Z}[x]$. Deste modo, se $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$,

então α é um inteiro algébrico. Portanto, $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ é o anel de inteiros algébricos de $\mathbb{K}$. ■

Definição 1.26 *Sejam $\mathbb{K}$ um corpo de números e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros algébricos de $\mathbb{K}$. O anel $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto $[\mathbb{K}:\mathbb{Q}]$. Chamamos o discriminante de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$ de discriminante de $\mathbb{K}$, e denotamos por $D_{\mathbb{K}}$.*

Teorema 1.16 *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com $d \in \mathbb{Z}$ livre de quadrados.*

a) Se $d \equiv 2$ ou $d \equiv 3(mod\ 4)$, então $D_{\mathbb{K}} = 4d$.

b) Se $d \equiv 1(mod\ 4)$, então $D_{\mathbb{K}} = d$.

Demonstração. Seja $\sigma_i \in Gal(\mathbb{K}|\mathbb{Q})$.

a) Se $d \equiv 2$ ou $3(mod\ 4)$, então $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$. Logo, $\{1, \sqrt{d}\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$. Assim,

$$D_{\mathbb{K}} = D(1,\sqrt{d}) = det(\sigma_i(x_j))^2 = \begin{vmatrix} \sigma_1(1) & \sigma_1(\sqrt{d}) \\ \sigma_2(1) & \sigma_2(\sqrt{d}) \end{vmatrix}^2 = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = 4d.$$

b) Se $d \equiv 1(mod\ 4)$, então $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Logo, $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$. Assim,

$$D_{\mathbb{K}} = D\left(1, \frac{1+\sqrt{d}}{2}\right) = det(\sigma_i(x_j))^2 = \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = d,$$

o que prova o teorema. ■

Definição 1.27 *Sejam n um inteiro positivo e $\mathbb{K}$ um corpo.*

1) Uma raíz do polinômio $x^n - 1$ é chamada de raíz n-ésima da unidade e denotamos por ζ_n. Podemos escrever ζ_n da forma $\zeta_n = e^{\frac{2\pi i}{n}} = cos(\frac{2\pi}{n}) + isen(\frac{2\pi}{n})$.

2) Uma raíz n-ésima da unidade tal que $\zeta_n^m \neq 1$, para todo $1 \leq m \leq n-1$, é chamada de raíz n-ésima primitiva da unidade. Podemos escrever ζ_n da forma $\zeta_n = e^{\frac{2\pi i}{n}} = cos(\frac{2\pi}{n}) + isen(\frac{2\pi}{n})$.

3) Um corpo ciclotômico é uma extensão de $\mathbb{Q}$ da forma $\mathbb{Q}(\zeta_n)$, onde ζ_n é uma raíz n-ésima primitiva da unidade.

4) O polinômio $\phi_n(x) = \prod_{j=1}^{n}(x - \zeta_n^j)$, onde $mdc(j,n) = 1$, é chamado de n-ésimo polinômio ciclotômico. O grau de $\phi_n(x)$ é dado pela Função de Euler $\varphi(n) = \#\{0 < m < n;\ mdc(m,n) = 1\}$ e $\phi_n(x)$ é mônico irredutível sobre $\mathbb{Q}$.

Proposição 1.15 *Se $\zeta_n \in \mathbb{C}$ é uma raíz n-ésima primitiva da unidade e $k \in \mathbb{N}$, então ζ_n^k é uma n-ésima raíz primitiva da unidade se, e somente se, $mdc(k,n) = 1$.*

Demonstração. Suponhamos que $mdc(k,n) = d$, com $d \neq 1$ e $d \neq n$, e ζ_n^k uma raíz n-ésima primitiva da unidade. Logo, $n = dx$, com $x \in \mathbb{N}$. Assim, $(\zeta_n^k)^d = \zeta_n^{k\frac{n}{x}} = (\zeta_n)^{\frac{k}{x}} = 1$ o que é um absurdo, pois $d < n$ e ζ_n é uma raíz n-ésima primitiva da unidade. Reciprocamente, se $m \in \mathbb{N}$ tal que $(\zeta_n^k)^m = 1$, então $\zeta_n^{km} = 1$, e assim, $n|km$ o que implica que $n|m$, pois $mdc(k,n) = 1$. Portanto, ζ_n^k é uma raíz n-ésima primitiva da unidade. ■

Consideramos $U_n = \{\zeta_n^{k_1}, \zeta_n^{k_2}, \ldots, \zeta_n^{k_n}\}$ o conjunto das raízes distintas de $x^n - 1$. Tem-se que U_n é um grupo ciclíco com gerador ζ_n, e assim, podemos escrever $U_n = \{1, \zeta_n, \ldots, \zeta_n^{n-1}\}$, se ζ_n uma raíz n-ésima primitiva da unidade.

Proposição 1.16 *Se $mdc(m,n) = 1$, com $m,\ n \in \mathbb{N}$, então $U_m \times U_n \simeq U_{mn}$.*

Demonstração. Consideramos a aplicação $\Phi : U_m \times U_n \longrightarrow U_{mn}$ dada por $\Phi(\omega, \eta) = \omega\eta$. Mostramos que Φ é um isomorfismo. De fato, se $(\omega, \eta) = (\alpha, \beta)$, então $\Phi(\omega, \eta) = \omega\eta = \alpha\beta = \Phi(\alpha, \beta)$, ou seja, Φ está bem definida. Tem-se que Φ é um homomorfismo, pois $\Phi((\omega, \eta)(\alpha, \beta)) = \Phi(\omega\alpha, \eta\beta) = \omega\alpha\eta\beta = \omega\eta\alpha\beta = \Phi(\omega, \eta)\Phi(\alpha, \beta)$. Além disso, o $Ker(\Phi) = \{(\omega, \eta) \in U_m \times U_n;\ \omega\eta = 1\}$, e assim, $(\omega, \eta) \in Ker(\Phi)$ se, e somente se, $1 = \omega\eta = \zeta_m^k\zeta_n^l$, com $0 \leq k \leq m-1$ e $0 \leq l \leq n-1$. Assim, $\zeta_m^k = \zeta_n^{-l}$ o que implica que $\zeta_m^{nk} = \zeta_n^{-nl} = 1$, ou seja, $m|nk$. Como $mdc(m,n) = 1$, segue que $m|k$. De modo análogo, mostramos que $n|l$. Pelo fato de $0 \leq k \leq m-1$ e $0 \leq l \leq n-1$, tem-se que $k = l = 0$. Assim, $Ker(\Phi) = (1,1)$, isto é, Φ é injetora. Como $mdc(m,n) = 1$, segue que $|U_{mn}| = |U_m||U_n|$. Portanto, Φ é um isomorfismo. ■

Proposição 1.17 *Se ζ_m é uma raíz m-ésima da unidade e ζ_n uma raíz n-ésima da unidade, com $mdc(m,n) = 1$, então $\zeta_m^k \zeta_n^l$ é uma raíz mn-ésima primitiva da unidade, onde $0 \leq k \leq m-1$ e $0 \leq l \leq n-1$, se, e somente se, ζ_m^k e ζ_n^l são raízes m-ésima e n-ésima primitivas da unidade, respectivamente.*

Demonstração. Se ζ_m^k não é uma raiz m-ésima primitiva da unidade, então, pela Proposição 1.15, $mdc(k,m) = d > 1$. Assim, $(\zeta_m^k \zeta_n^l)^{\frac{mn}{d}} = (\zeta_m^m)^{\frac{kn}{d}} (\zeta_n^n)^{\frac{lm}{d}} = 1$, o que é um absurdo, pois $\frac{mn}{d} < mn$ e $\zeta_m^k \zeta_n^l$ é uma raíz mn-ésima primitiva da unidade. De modo análogo mostramos que ζ_n^l é uma raíz n-ésima primitiva da unidade. Por outro lado, se ζ_m^k e ζ_n^l são raizes m-ésima e n-ésima primitivas da unidades, então, pela Proposição 1.15, $mdc(k,m) = 1$ e $mdc(l,n) = 1$. Notamos que $(\zeta_m^k \zeta_n^l)^a = 1$ se, e somente se, $\zeta_m^{ka} = \zeta_n^{-la}$, e assim, $\zeta_m^{nka} = \zeta_n^{-nla} = 1$. Logo, $m|na$. Como $mdc(m,n) = 1$, segue que $m|a$. De modo análogo mostramos que $n|a$, e assim, $mn|a$, pois $mdc(m,n) = 1$. Pelo fato de que $(\zeta_m^k \zeta_n^l)^{mn} = 1$, tem-se que $mn = o(\zeta_m^k \zeta_n^l)$. Portanto, $\zeta_m^k \zeta_n^l$ é uma raíz mn-ésima primitiva da unidade. ■

Pela Proposição 1.17, tem-se que $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{mn})$ e se $mdc(m,n) = 1$, então vale a igualdade. Como $\varphi(mn) = \varphi(m)\varphi(n)$, com $mdc(m,n) = 1$, segue que $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

Proposição 1.18 *Para todo $n \geq 1$, tem-se $x^n - 1 = \prod_{d|n} \phi_d(x)$.*

Demonstração. Se $f(x) = x^n - 1$ e $\{1, \zeta_n, \ldots, \zeta_n^{n-1}\}$ são suas raízes, então podemos escrever $f(x) = (x-1)(x-\zeta_n)\ldots(x-\zeta_n^{n-1})$. Analisando as ordens de cada raíz de $f(x)$ e escrevendo todas as raízes de mesma ordem como um polinômio da forma $\phi_d(x) = \prod_{o(\zeta_n)=d} (x - \zeta_n)$, tem-se que $x^n - 1 = \prod_{d|n} \phi_d(x)$. ■

Como consequência da Proposição 1.18 basta conhecermos os polinômios ϕ_{p^r}, onde p é primo e $r \geq 1$. Assim,

$$\phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d<n} \phi_d(x)}. \tag{1.9}$$

Para $n = p$ primo, tem-se que

$$\phi_p(x) = \frac{x^p - 1}{\prod\limits_{q|p, q<p} \phi_q(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1.$$

Para $n = p^r$, com p primo e $r > 1$, tem-se que

$$\phi_{p^r}(x) = \frac{x^{p^r} - 1}{\prod\limits_{q|p^r, q<p^r} \phi_q(x)} = \frac{x^{p^r} - 1}{\phi_1(x) \ldots \phi_{p^{r-1}}(x)} = x^{p^{r-1}(p-1)} + \ldots + x^{p^{r-1}} + 1.$$

Exemplo 1.11 *Pela Equação (1.9) tem-se que* $\phi_1(x) = x - 1$, $\phi_2(x) = \dfrac{x^2 - 1}{x - 1}$, $\phi_3(x) = \dfrac{x^3 - 1}{x - 1}$ *e* $\phi_6(x) = \dfrac{x^6 - 1}{\phi_1(x)\phi_2(x)\phi_3(x)}$.

Proposição 1.19 *Se* ζ_n *é uma raíz n-ésima primitiva da unidade, então* $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ *e* $Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \simeq \mathbb{Z}_n^*$.

Demonstração. Se $f(x) = min_{\mathbb{Q}}\zeta_n$, então $x^n - 1 = f(x)g(x)$, com $g(x) \in \mathbb{Q}[x]$. Pelo Lema de Gauss, podemos considerar $f(x)$, $g(x) \in \mathbb{Z}[x]$. Se p é primo tal que $p \nmid n$, então $mdc(p, n) = 1$. Logo, pela Proposição 1.15, tem-se que ζ_n^p é uma raíz n-ésima primitiva da unidade. Assim, $(\zeta_n^p)^n - 1 = f(\zeta_n^p)g(\zeta_n^p) = 0$, o que implica que $f(\zeta_n^p) = 0$ ou $g(\zeta_n^p) = 0$. Se $g(\zeta_n^p) = 0$, então ζ_n é uma raíz de $g(x^p)$. Como $f(x)$ é o minimal de ζ_n, segue que $f(x)|g(x^p)$, ou seja, $g(x^p) = f(x)h(x)$, com $h(x) \in \mathbb{Z}[x]$. Pelo fato de que $a^p \equiv a(mod\ p)$, para todo $a \in \mathbb{Z}$, tem-se que $g(x^p) \equiv g(x)^p(mod\ p)$. Assim, $g(x)^p \equiv f(x)h(x)(mod\ p)$, o que implica que $\overline{g(\zeta_n)^p} = \overline{0}$, ou seja, $\overline{g}(\zeta_n) = 0$. Logo, $\overline{f}$ e $\overline{g}$ têm raízes em comum, e assim, $x^n - \overline{1} = \overline{f}(x)\overline{g}(x)$ tem uma raíz múltipla, a qual também é raíz de $\overline{n}x^{n-1}$. Se $\alpha \in \mathbb{Z}_p$ é raíz de $\overline{n}x^{n-1}$, então $\overline{n}\alpha^{n-1} = 0$. Como $car(\mathbb{Z}_p) = p$, segue que $p|n$ o que é um absurdo. Portanto, ζ_n^p é uma raíz de $f(x)$, para todo $p \nmid n$, e consequentemente, $gr(f(x)) \geq gr(\phi_n(x))$, pois toda raíz de $\phi_n(x)$ é raíz de $f(x)$. Por fim, como $f(x)|\phi_n(x)$, segue que $gr(f(x)) \leq gr(\phi_n(x))$. Portanto, $gr(f(x)) = gr(\phi_n(x)) = \varphi(n)$. Agora, consideramos $\Psi : \mathbb{Z}_n^* \longrightarrow Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ dada por $\Psi(\bar{i}) = \sigma_i(\zeta_n) = \zeta_n^i$. Esta aplicação é um homomorfismo injetivo entre grupos de mesma ordem. Portanto, Ψ é um isomorfismo. ■

Como consequência da Proposição 1.19 tem-se que $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ é de Galois. Além disso, $Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q}) = \{\sigma_i \in Aut(\mathbb{Q}(\zeta_n));\ mdc(i,n) = 1\ e\ \sigma_i(\zeta_n) = \zeta_n^i\}$. Como $\mathbb{Z}_n^*$ é abeliano, segue que $Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ é abeliano. Agora, como $\mathbb{Z}_n^*$ é ciclíco para $n = 2, 4, p^r$ ou $2p^r$, onde p é primo e $r \geq 1$, segue que $Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q})$ é ciclíco para $n = 2, 4, p^r$ ou $2p^r$, onde p é primo e $r \geq 1$. Caso, $\mathbb{Z}_n^*$ não seja ciclíco, segue que $\mathbb{Z}_n^*$ contém pelo menos dois subgrupos ciclícos de ordem 2.

Proposição 1.20 *Se $\mathbb{K} = \mathbb{Q}(\zeta_{2^r})$, com $r \geq 3$, então $Gal(\mathbb{K}|\mathbb{Q}) = G_1 \times G_2$, onde G_1 e G_2 são ciclícos e $|G_1| = 2^{r-2}$ e $|G_2| = 2$. Além disso, G_2 é gerado pelo automorfismo que aplica ζ em ζ^{-1}.* ■

Demonstração. [9], pág. 43.

Proposição 1.21 *Se ζ_n é uma raíz n-ésima primitiva da unidade, com $n \in \mathbb{N}^*$, e $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, então $\mathbb{K} \subset \mathbb{R}$ e $[\mathbb{Q}(\zeta_n) : \mathbb{K}] = 2$.*

Demonstração. Consideramos $f(x) = x^2 - (\zeta_n + \zeta_n^{-1})x + 1 \in \mathbb{K}[x]$. Notemos que $f(\zeta_n) = 0$ e $\zeta_n \notin \mathbb{K}$. Logo, $f(x)$ é irredutível sobre $\mathbb{K}$. Portanto, $[\mathbb{Q}(\zeta_n) : \mathbb{K}] = gr(f(x)) = 2$. ■

Definição 1.28 *O corpo $\mathbb{K}$ da Proposição 1.21 é chamado de subcorpo real maximal de $\mathbb{Q}(\zeta_n)$.*

Lema 1.7 *Se $\mathbb{K} = \mathbb{Q}(\zeta_p)$, onde ζ_p é uma raíz p-ésima primitiva da unidade e p um número primo, então*

a) $Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_p^j) = -1$, *para* $j = 1, 2, \ldots, p-1$;

b) $Tr_{\mathbb{K}|\mathbb{Q}}(1 - \zeta_p^j) = p$, *para* $j = 1, 2, \ldots, p-1$;

c) $N_{\mathbb{K}|\mathbb{Q}}(\zeta_p - 1) = (-1)^{p-1}p$;

d) $N_{\mathbb{K}|\mathbb{Q}}(1 - \zeta_p) = p$;

e) $p = (1 - \zeta_p)(1 - \zeta_p^2)\ldots(1 - \zeta_p^{p-1})$;

f) Se $\mathcal{O}_{\mathbb{K}}$ é o anel dos inteiros algébricos de $\mathbb{K}$, então $(1-\zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z} = \langle p \rangle$;

g) $Tr_{\mathbb{L}|\mathbb{K}}(y(1-\zeta_p)) \in p\mathbb{Z}$, para todo $y \in \mathcal{O}_{\mathbb{K}}$.

Demonstração. a) Tem-se que $\phi_p(x) = x^{p-1} + x^{p-2} + \ldots + 1$ o p-ésimo polinômio ciclotômico é o polinômio minimal de ζ_p sobre $\mathbb{Q}$. Como ζ_p^j é raíz de $\phi_p(x)$, segue que $Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_p^j) = -1$, para $1 \leq j \leq p-1$. Além disso, pelo item (b) das Propriedades 1.1, tem-se que $Tr_{\mathbb{K}|\mathbb{Q}}(1) = p-1$.

b) $Tr_{\mathbb{K}|\mathbb{Q}}(1-\zeta_p^j) = Tr_{\mathbb{K}|\mathbb{Q}}(1) - Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_p^j) = p-1+1 = p$, para $1 \leq j \leq p-1$.

c) Notemos que $1 = ((\zeta_p - 1) + 1)^p = \sum_{j=0}^{p} \begin{pmatrix} p \\ j \end{pmatrix} (\zeta_p - 1)^{p-j}$. Assim, $(\zeta_p - 1)((\zeta_p - 1)^{p-1} + p(\zeta_p - 1)^{p-2} + \ldots + p) = 0$, o que implica que $(\zeta_p - 1)^{p-1} + p(\zeta_p - 1)^{p-2} + \ldots + p = 0$, se $\zeta_p \neq 1$. Consideramos $f(x) = x^{p-1} + \sum_{j=p-1}^{1} \begin{pmatrix} p \\ j \end{pmatrix} x^{j-1} = x^{p-1} + px^{p-2} + \ldots + p$. Tem-se que $f(\zeta_p - 1) = (\zeta_p - 1)^{p-1} + p(\zeta_p - 1)^{p-2} + \ldots + p = 0$. Logo, $\zeta_p - 1$ é raíz de $f(x)$ e $f(x)$ é mônico irredutível, ou seja, $f(x) = min_{\mathbb{Q}}(\zeta_p - 1)$. Portanto, $N_{\mathbb{K}|\mathbb{Q}}(\zeta_p - 1) = (-1)^{p-1}p$.

d) Como $N_{\mathbb{K}|\mathbb{Q}}(1-\zeta_p) = N_{\mathbb{K}|\mathbb{Q}}(-1(\zeta_p - 1))$, segue que $N_{\mathbb{K}|\mathbb{Q}}(1-\zeta_p) = N_{\mathbb{K}|\mathbb{Q}}(-1)N_{\mathbb{K}|\mathbb{Q}}(\zeta_p - 1) = (-1)^{p-1}(-1)^{p-1}p = (-1)^{2(p-1)}p = p$.

e) Tem-se que $\phi_p(x) = x^{p-1} + x^{p-2} + \ldots + 1 = (x-\zeta_p)(x-\zeta_p^2)\ldots(x-\zeta_p^{p-1})$. Em particular, se tomarmos $x = 1$, tem-se que $(1-\zeta_p)\ldots(1-\zeta_p^{p-1}) = p$.

f) Como $p = (1-\zeta_p)\ldots(1-\zeta_p^{p-1})$, segue que $p \in (1-\zeta_p)\mathcal{O}_{\mathbb{K}}$. Logo, $\langle p \rangle = p\mathbb{Z} \subseteq (1-\zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z}$. Reciprocamente, suponhamos que $\langle p \rangle = p\mathbb{Z} \subsetneq (1-\zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} \subseteq \mathbb{Z}$. Como $p\mathbb{Z}$ é maximal, segue que $(1-\zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = \mathbb{Z}$. Assim, $1 = (1-\zeta_p)\alpha$, com $\alpha \in \mathcal{O}_{\mathbb{L}}$, ou seja, $1-\zeta_p$ é inversível. Logo, $1-\zeta_p^j$ é inversível, para $1 \leq j \leq p-1$. Deste modo, $p = (1-\zeta_p)(1-\zeta_p^2)\ldots(1-\zeta_p^{p-1})$ é inversível em $\mathbb{Z}$, o que é um absurdo. Portanto, $(1-\zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z} = \langle p \rangle$.

g) Sejam $y_i(1-\zeta_p^i)$ os conjugados de $y(1-\zeta_p)$, para $1 \leq i \leq p-1$. Tem-se que $(1-\zeta_p^i)$ e $(1-\zeta_p)$ são associados, ou seja, $(1-\zeta_p^i)|(1-\zeta_p)$ e $(1-\zeta_p)|(1-\zeta_p^i)$, pois se $1 \leq k, i \leq p-1$, então existe $1 \leq t \leq p-1$ tal que $i \equiv kt(mod\ p)$, e assim, $(1-\zeta_p^i) = 1-(\zeta_p^k)^t = (1-\zeta_p^k)(1+\zeta_p+\ldots+(\zeta_p^k)^{t-1})$. Assim, $1-\zeta_p^i$ é mútiplo de $1-\zeta_p$ em $\mathcal{O}_{\mathbb{K}}$. Logo, $Tr_{\mathbb{K}|\mathbb{Q}}(y(1-\zeta_p)) = y_1(1-\zeta_p) + y_2(1-\zeta_p^2) + \ldots + y_{p-1}(1-\zeta_P^{p-1}) = \alpha(1-\zeta_p)$,

com $\alpha \in \mathcal{O}_{\mathbb{K}}$. Deste modo, $Tr_{\mathbb{K}|\mathbb{Q}}(y(1-\zeta_p)) \in \mathcal{O}_{\mathbb{L}}$ e $Tr_{\mathbb{K}|\mathbb{Q}}(y(1-\zeta_p)) \in \mathbb{Z}$, pois $\mathbb{Z}$ é integralmente fechado. Portanto, $Tr_{\mathbb{K}|\mathbb{Q}}(y(1-\zeta_p)) \in (1-\zeta_p)\mathcal{O}_{\mathbb{L}} \cap \mathbb{Z} = p\mathbb{Z} = \langle p \rangle$. ■

Observação 1.5 *Se ζ_{p^r} é uma raíz p^r-ésima primitiva da unidade, com p primo e $r \in \mathbb{N}$, então o Lema 1.7 é análogo para ζ_{p^r}, e assim, $(1-\zeta_{p^r})\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$ é um ideal de $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$ acima de $p\mathbb{Z}$ e os conjugados de $1-\zeta_{p^r}$ são todos associados.*

Os próximos resultados explicitam os anéis de inteiros algébricos e discriminantes de corpos ciclotômicos. Neste trabalho é dado a demonstração para o caso $\mathbb{K} = \mathbb{Q}(\zeta_p)$, as demais podem ser encontradas em [16].

Teorema 1.17 *Se $\mathbb{K} = \mathbb{Q}(\zeta_p)$, onde ζ_p é uma raíz p-ésima primitiva da unidade e p um número primo, então o anel dos inteiros algébricos de $\mathbb{K}$ é $\mathbb{Z}[\zeta_p]$ e $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ é uma base de $\mathbb{Z}[\zeta_p]$ como $\mathbb{Z}$-módulo.*

Demonstração. Se $\alpha \in \mathbb{Z}[\zeta_p]$, então $\alpha \in \mathcal{O}_{\mathbb{K}} = \{\beta \in \mathbb{K};\ \beta \text{ é inteiro sobre } \mathbb{Z}\}$. Assim, basta mostrar que $\mathcal{O}_{\mathbb{K}} \subseteq \mathbb{Z}[\zeta_p]$. Se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então

$$\alpha = a_0 + a_1\zeta_p + \ldots + a_{p-2}\zeta_p^{p-2}, \text{ onde } a_i \in \mathbb{Q}, \text{ para } i = 0, 1 \ldots, p-2.$$

Multiplicando por $(1-\zeta_p)$ tem-se que

$$\alpha(1-\zeta_p) = a_0(1-\zeta_p) + a_1(\zeta_p - \zeta_p^2) + \ldots + a_{p-2}(\zeta_p^{p-2} - \zeta_p^{p-1}).$$

Assim,

$$Tr_{\mathbb{K}|\mathbb{Q}}(\alpha(1-\zeta_p)) = a_0 Tr_{\mathbb{K}|\mathbb{Q}}(1-\zeta_p) + a_1 Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_p - \zeta_p^2) + \ldots + a_{p-2} Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_p^{p-2} - \zeta_p^{p-1}).$$

Pelo Lema 1.7 e pelo fato de que $Tr_{\mathbb{K}|\mathbb{Q}}(\zeta_p^j - \zeta_p^{j+1}) = 0$, para $j = 1, 2, \ldots, p-1$, segue que

$$Tr_{\mathbb{K}|\mathbb{Q}}(\alpha(1-\zeta_p)) = a_0 Tr_{\mathbb{K}|\mathbb{Q}}(1-\zeta_p) = a_0 p \in p\mathbb{Z}, \text{ onde } a_0 \in \mathbb{Z}.$$

Como $\zeta_p^{-1} = \zeta_p^{p-1}$, segue que $\zeta_p^{-1} \in \mathcal{O}_{\mathbb{K}}$, e portanto

$$(\alpha - a_0)\zeta_p^{-1} = a_1 + a_2\zeta_p + \ldots + a_{p-1}\zeta_p^{p-3}.$$

Multiplicando por $(1-\zeta_p)$ tem-se que

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

Logo, $Tr_{\mathbb{K}|\mathbb{Q}}((\alpha - a_0)\zeta_p^{-1}(1-\zeta_p)) = a_1 Tr_{\mathbb{K}|\mathbb{Q}}(1-\zeta_p) = a_1 p \in p\mathbb{Z}$, onde $a_1 \in \mathbb{Z}$. Prosseguindo dessa forma tem-se que $a_0, a_1, \ldots, a_{p-2} \in \mathbb{Z}$. Portanto, $\alpha \in \mathbb{Z}[\zeta_p]$ e $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ é uma base de $\mathcal{O}_\mathbb{K}$ como um $\mathbb{Z}$-módulo. ■

Teorema 1.18 *Se $\mathbb{K} = \mathbb{Q}(\zeta_p)$, onde ζ_p é uma raíz p-ésima primitiva da unidade e p é um número primo ímpar, então o discriminante de $\mathbb{K}$ é dado por*

$$D_\mathbb{K} = D(1, \zeta_p, \ldots, \zeta_p^{p-2}) = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

Demonstração. Pelo Teorema 1.17 tem-se que $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ é uma base de $\mathcal{O}_\mathbb{K}$ como um $\mathbb{Z}$-módulo. Assim, pela Proposição 1.14, tem-se que

$$D_\mathbb{K} = (-1)^{\frac{(p-1)(p-2)}{2}} N_{\mathbb{K}|\mathbb{Q}}({\phi_p}'(\zeta_p)).$$

Como ${\phi_p}'(\zeta_p) = \dfrac{(\zeta_p - 1)p\zeta_p^{p-1} - (\zeta_p^p - 1)}{(\zeta_p - 1)^2} = \dfrac{-p\zeta_p^{p-1}}{1-\zeta_p}$, segue que $N_{\mathbb{K}|\mathbb{Q}}({\phi_p}'(\zeta_p)) = \dfrac{N_{\mathbb{K}|\mathbb{Q}}(-p)N_{\mathbb{K}|\mathbb{Q}}(\zeta_p^{p-1})}{N_{\mathbb{K}|\mathbb{Q}}(1-\zeta_p)} = \dfrac{p^{p-1}1^{p-1}}{p} = p^{p-2}$. Como p é ímpar, segue que $(-1)^{p-2} = -1$. Assim, $(-1)^{\frac{(p-1)(p-2)}{2}} = (-1)^{\frac{p-1}{2}}$. Portanto, $D_\mathbb{K} = (-1)^{\frac{p-1}{2}} p^{p-2}$. ■

Teorema 1.19 *Seja p um número primo e r um inteiro maior que 1.*

a) Se $\mathbb{K} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, onde ζ_p é uma raíz p-ésima primitiva da unidade, então o anel dos inteiros algébricos de $\mathbb{K}$ é $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ e $\{\zeta_p + \zeta_p^{-1}, \ldots, \zeta_p^{\frac{p-1}{2}} + \zeta_p^{\frac{1-p}{2}}\}$ é uma base de $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ como um $\mathbb{Z}$-módulo.

b) Se $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, onde ζ_{p^r} é uma raíz p^r-ésima primitiva da unidade, então o anel dos inteiros algébricos de $\mathbb{K}$ é $\mathbb{Z}[\zeta_{p^r}]$ e $\{1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{(p-1)p^{r-1}-1}\}$ é uma base de $\mathbb{Z}[\zeta_{p^r}]$ como um $\mathbb{Z}$-módulo.

c) Se $\mathbb{K} = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, onde ζ_{p^r} é uma raíz p^r-ésima primitiva da unidade, então o anel dos inteiros algébricos de $\mathbb{K}$ é $\mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$ e $\{\zeta_{p^r} + \zeta_{p^r}^{-1}, \ldots, \zeta_{p^r}^{\frac{(p-1)p^{r-1}}{2}} + \zeta_{p^r}^{\frac{(1-p)p^{r-1}}{2}}\}$ é uma base de $\mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$ como um $\mathbb{Z}$-módulo.

d) Se $\mathbb{K} = \mathbb{Q}(\zeta_n)$, onde ζ_n é uma raíz n-ésima primitiva da unidade, então o anel dos inteiros algébricos de $\mathbb{K}$ é $\mathbb{Z}[\zeta_n]$ e $\{1, \zeta_n, \ldots, \zeta_n^{\frac{\varphi(n)}{2}-1}\}$ é uma base de $\mathbb{Z}[\zeta_n]$ como um $\mathbb{Z}$-módulo.

Demonstração.

a) [16], pág 47, Proposição 1.9.4.

b) [16], pág 51, Teorema 1.9.4.

c) [16], pág 52, Proposição 1.9.6.

d) [16], pág 55, Teorema 1.9.6. ■

Teorema 1.20 *Se $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, onde ζ_{p^r} é uma raíz p^r-ésima primitiva da unidade e p é um número primo ímpar, então o discriminante de $\mathbb{K}$ é dado por*

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

Demonstração. [16], pág 65, Proposição 2.5.2. ■

Teorema 1.21 *Se $\mathbb{K} = \mathbb{Q}(\zeta_n)$, com n um inteiro maior que 1, então*

$$D_{\mathbb{Q}(\zeta_n)} = (1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}) = \pm \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\frac{\varphi(n)}{p-1}}}.$$

Demonstração. [16], pág 69, Teorema 2.5.1. ■

1.6 Considerações finais

O Capítulo 1 tem como objetivo fornecer uma base teórica para o desenvolvimento dos próximos capítulos. Para auxiliar na demonstração do Teorema de Kronecker-Weber podemos particularizar alguns resultados deste capítulo. Por exemplo, se $\mathbb{K}$ é uma extensão de $\mathbb{Q}$, então $\mathcal{O}_{\mathbb{K}}$ é integralmente fechado, um $\mathbb{Z}$-módulo Noetheriano e finitamente gerado. O Teorema Fundamental de Grupos Abelianos Finitos, o Teorema de Irracionalidade Natural e alguns resultados de extensões ciclícas são muito úteis na demonstração do Teorema de Kronecker-Weber.

Capítulo 2

Domínio de Dedekind, ramificação e valorização

Neste capítulo apresentamos o conceito de ramificação de ideais, o qual é de extrema importância na demonstração do Teorema de Kronecker-Weber. Antes precisamos definir domínios de Dedekind, anéis de frações e norma de ideais. A importante relação entre ramificação e discriminante é apresentada na seção 2.4.1 e na seção 2.4.2 são definidos e estudados os grupos de decomposição, inércia e ramificação de um ideal. Nas seções 2.5 e 2.6, breves conceitos de diferente e valorização são apresentados, apenas visando a demonstração do Teorema de Kronecker-Weber.

2.1 Domínio de Dedekind

Pela Proposição 1.2 do Capítulo 1, vimos que em um domínio de integridade Noetheriano qualquer ideal contém um produto de ideais primos. Nesta seção, apresentamos domínios de integridade em que qualquer ideal é igual a um produto de ideais primos. As principais referências desta seção são [2], [7] e [12].

Definição 2.1 *Um domínio de integridade A é chamado um domínio de Dedekind se:*

i) A é integralmente fechado

ii) A é um anel Noetheriano e

iii) todo ideal primo não nulo de A é um ideal maximal.

Exemplo 2.1 *Todo anel principal A é um domínio de Dedekind. De fato, pelos Exemplos 1.2 e 1.4, tem-se que A é um anel Noetheriano e integralmente fechado . Agora, se $\mathfrak{b}$ é um ideal primo não nulo de A, então $\mathfrak{b} = bA$, onde $b \neq 0$ e b é irredutível. Assim, se existir $\mathfrak{b}' = b'A$ ideal de A tal que $\mathfrak{b} \subset \mathfrak{b}'$, então $b'|b$ e $b \nmid b'$. Logo, b' é uma unidade de A. Portanto, $\mathfrak{b}' = A$.*

Proposição 2.1 *Se $A \subseteq B$ são anéis e $\mathfrak{p}$ ideal primo de B, então $\mathfrak{p} \cap A$ é ideal primo de A.*

Demonstração. Consideramos a aplicação $\varphi = \pi \circ i : A \longrightarrow B \longrightarrow \dfrac{B}{\mathfrak{p}}$, onde i é a inclusão e π e projeção, a qual é um homomorfismo de anéis. Tem-se que $Ker(\varphi) = \mathfrak{p} \cap A$. Logo, $\dfrac{A}{\mathfrak{p} \cap A}$ é isomorfo a um subanel de $\dfrac{B}{\mathfrak{p}}$. Como $\dfrac{B}{\mathfrak{p}}$ é um domínio de integridade, segue que $\dfrac{A}{\mathfrak{p} \cap A}$ também é um domínio de integridade. Portanto, $\mathfrak{p} \cap A$ é um ideal primo de A. ■

Teorema 2.1 *Se A é um domínio de Dedekind, $\mathbb{L}|\mathbb{K}$ uma extensão finita de grau n, onde $\mathbb{K} = Q(A)$ e $car(\mathbb{K}) = 0$, então $\mathcal{O}_{\mathbb{L}}$ é um domínio de Dedekind e um A-módulo finitamente gerado.*

Demonstração. Pelo Exemplo 1.5 e pelo Teorema 1.13, tem-se que $\mathcal{O}_{\mathbb{L}}$ é integralmente fechado, um anel Noetheriano e um A-módulo finitamente gerado. Agora, se $\mathfrak{p}$ é um ideal primo não nulo de $\mathcal{O}_{\mathbb{L}}$, então, pela Proposição 2.1, segue que $\mathfrak{p} \cap A$ é um ideal primo de A. Como $\mathfrak{p} \subseteq \mathcal{O}_{\mathbb{L}}$, segue que se $x \in \mathfrak{p}$, então x é inteiro sobre A. Logo, existem $a_0, a_1, \ldots, a_{n-1} \in A$ tal que $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$. Suponhamos que n seja mínimo. Assim, $a_0 \neq 0$, pois caso contrário n não seria mínimo. Tem-se que $a_0 \in x\mathcal{O}_{\mathbb{L}} \cap A \subseteq \mathfrak{p} \cap A$. Como $a_0 \neq 0$, segue que $\mathfrak{p} \cap A \neq \langle 0 \rangle$. Logo, $\mathfrak{p} \cap A$ é um ideal maximal de A. Deste modo, tem-se que $\dfrac{A}{\mathfrak{p} \cap A}$ é um corpo e $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}}$ é inteiro sobre $\dfrac{A}{\mathfrak{p} \cap A}$. Assim, pela Proposição 1.5, segue que $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}}$ é um corpo. Portanto, $\mathfrak{p}$ é um ideal maximal. ■

Definição 2.2 *Sejam A um domínio de integridade e $\mathbb{K}$ o corpo de frações de A. Um A-submódulo $\mathfrak{b}$ de $\mathbb{K}$ é chamado de ideal fracionário de A se existe $d \in A - \{0\}$ tal que $d\mathfrak{b} \subset A$. Chamamos d de um denominador comum dos elementos de $\mathfrak{b}$.*

Exemplo 2.2 *Todos os ideais de A são ideais fracionários de A, basta colocar $d = 1$. Chamamos os ideais de A de ideais inteiros.*

No conjunto $\mathcal{F}$ dos ideais fracionários de A estão definidas as operações de adição, multiplicação, interseção e quociente de ideais. Se $\mathfrak{b}$, $\mathfrak{b}' \in \mathcal{F}$, com d e d' seus denominadores comuns, então dd' é um denominador comum de $\mathfrak{b} + \mathfrak{b}'$ e $\mathfrak{b}\mathfrak{b}'$, e d ou d' é um denominador comum de $\mathfrak{b} \cap \mathfrak{b}'$. O quociente $(\mathfrak{b} : \mathfrak{b}') := \{x \in \mathbb{K};\ x\mathfrak{b}' \subset \mathfrak{b}\}$ tem denominador comum ad, onde d é o denominador de $\mathfrak{b}$ e $a \in \mathfrak{b}'$. O conjunto $(\mathcal{F}, \cdot)$ é um monóide comutativo, ou seja, satisfaz as propriedades associativa, comutativa e A é o elemento neutro.

Proposição 2.2 *Se A é um domínio de Dedekind, que não é corpo, e $\mathfrak{p}$ um ideal maximal de A, então $\mathfrak{p}' = (A : \mathfrak{p}) \neq A$.*

Demonstração. Se $y \in \mathfrak{p}$ e $y \neq 0$, então $Ay \supseteq \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n$ (Proposição 1.2), onde $\mathfrak{p}_i$ é um ideal primo, para $i = 1, 2, \dots, n$. Suponhamos n o menor possível. Assim, $\mathfrak{p} \supseteq \mathfrak{p}_i$, para algum $i = 1, 2, \dots, n$, pois caso contrário existiria $a_i \in \mathfrak{p}_i - \mathfrak{p}$, para $i = 1, 2, \dots, n$, tal que $a_1 a_2 \dots a_n \in \mathfrak{p}$, o que contraria o fato de $\mathfrak{p}$ ser primo. Suponhamos que $\mathfrak{p} \supseteq \mathfrak{p}_1$. Logo, $\mathfrak{p} = \mathfrak{p}_1$, pois $\mathfrak{p}_1$ é maximal. Se $\mathfrak{b} = \mathfrak{p}_2\mathfrak{p}_3 \dots \mathfrak{p}_n$, então $Ay \supseteq \mathfrak{p}\mathfrak{b}$ e $Ay \not\supseteq \mathfrak{b}$, pois n é o menor possível. Logo, existe $b \in \mathfrak{b}$ tal que $b \notin Ay$. Como $Ay \supseteq \mathfrak{p}\mathfrak{b}$, segue que $Ay \supseteq \mathfrak{p}b$. Assim, $A \supseteq \mathfrak{p}by^{-1}$, e deste modo, $by^{-1} \in \mathfrak{p}'$. Mas, como $b \notin Ay$, segue que $by^{-1} \notin A$. Portanto, $\mathfrak{p}' \neq A$. ■

Teorema 2.2 *Se A é um domínio de Dedekind, que não é corpo, então todo ideal maximal de A é invertível em $(\mathcal{F}, \cdot)$.*

Demonstração. Se $\mathfrak{p}$ é um ideal maximal de A, então $\mathfrak{p} \neq \langle 0 \rangle$, pois A é um corpo. Seja $\mathfrak{p}' = (A : \mathfrak{p}) = \{x \in \mathbb{K}; x\mathfrak{p} \subset A\}$. Tem-se que $\mathfrak{p}'\mathfrak{p} \subseteq A$. Se $a \in A$, então $a\mathfrak{p} \subseteq A$, pois $\mathfrak{p}$ é um ideal de A. Logo, $A \subset \mathfrak{p}'$. Assim, $\mathfrak{p} = A\mathfrak{p} \subseteq \mathfrak{p}'\mathfrak{p} \subseteq A$. Como $\mathfrak{p}$ é maximal, segue

que $\mathfrak{p} = \mathfrak{p}'\mathfrak{p}$ ou $\mathfrak{p}'\mathfrak{p} = A$. Suponhamos que $\mathfrak{p} = \mathfrak{p}'\mathfrak{p}$ e $x \in \mathfrak{p}'$. Assim, $x\mathfrak{p} \subseteq \mathfrak{p}$, $x^2\mathfrak{p} \subseteq \mathfrak{p}$ e $x^n\mathfrak{p} \subseteq \mathfrak{p}$, para $n \in \mathbb{N}$. Logo, para qualquer $y \in \mathfrak{p}$, tem-se $x^n y \subseteq \mathfrak{p} \subseteq A$, e assim, $A[x]$ é um ideal fracionário de A. Como A é Noetheriano, segue que $yA[x] \subseteq A$ é um A-módulo finitamente gerado, e portanto, $A[x]$ é um A-módulo finitamente gerado. Assim, pelo Teorema 1.3, segue que x é inteiro sobre A e $x \in \mathfrak{p}' \subseteq \mathbb{K}$. Como A é integralmente fechado, segue que $x \in A$, e assim, $\mathfrak{p}' = A$, o que contraria a Proposição 2.2. Portanto, $\mathfrak{p}'\mathfrak{p} = A$, ou seja, $\mathfrak{p}'$ é o inverso de $\mathfrak{p}$. ■

Teorema 2.3 *Sejam A um domínio de Dedekind e $\mathcal{P}$ o conjunto de todos os ideais primos não nulos de A.*

i) Todo ideal fracionário $\mathfrak{p}'$ não nulo de A pode ser expresso, de modo único, da forma

$$\mathfrak{p}' = \prod_{\mathfrak{p}_i \in \mathcal{P}} \mathfrak{p}_i^{e_i},$$

onde $e_i \in \mathbb{Z}$ e para quase todos os $\mathfrak{p}_i \in \mathcal{P}$ tem-se que $e_i = 0$;

ii) O conjunto $(\mathcal{F}, \cdot)$ é um grupo.

Demonstração. i) Provamos a existência desta fatoração. Se $\mathfrak{p}'$ é um ideal fracionário de A, então existe $d \in A - \{0\}$ tal que $d\mathfrak{p}' \subset A$. Logo, $d\mathfrak{p}'$ é um ideal inteiro de A. Assim, escrevendo $d\mathfrak{p}' = Ad\mathfrak{p}'$, tem-se que $\mathfrak{p}' = (Ad)^{-1}(d\mathfrak{p}')$. Se mostrarmos que $Ad = \prod_{\mathfrak{p}_i \in \mathcal{P}} \mathfrak{p}_i^{n_i}$ e $d\mathfrak{p}' = \prod_{\mathfrak{p}_i \in \mathcal{P}} \mathfrak{p}_i^{m_i}$, então $\mathfrak{p}' = \prod_{\mathfrak{p}_i \in \mathcal{P}} \mathfrak{p}_i^{m_i - n_i}$. Portanto, basta mostrarmos o resultado para ideais inteiros de A. Suponhamos que exista uma família não vazia de ideais de A que não são o produto de potências de ideais primos de A. Como A é Noetheriano, segue que esta família tem um elemento maximal $\mathfrak{m}$. Tem-se que $\mathfrak{m} \neq A$, pois A é o produto de uma coleção vazia de ideais primos. Assim, $\mathfrak{m} \subset \mathfrak{b}$, onde $\mathfrak{b}$ é maximal. Pelo Teorema 2.2, segue que existe $\mathfrak{b}' \in \mathcal{F}$ tal que $\mathfrak{b}'\mathfrak{b} = A$. Como $\mathfrak{m} \subset \mathfrak{b}$, segue que $\mathfrak{b}'\mathfrak{m} \subset \mathfrak{b}'\mathfrak{b} = A$. Como $A \subset \mathfrak{b}'$, segue que $\mathfrak{m} = A\mathfrak{m} \subset \mathfrak{b}'\mathfrak{m} \subset A$. Tem-se que $\mathfrak{m} \subsetneq \mathfrak{b}'\mathfrak{m}$, pois se $\mathfrak{m} = \mathfrak{b}'\mathfrak{m}$ e se $x \in \mathfrak{b}'$, então $x^n\mathfrak{m} \subset \mathfrak{m}$, para $n \in \mathbb{N}$. Agora, se $d \in \mathfrak{m} - \{0\}$, então $dx^n \subset \mathfrak{m} \subset A$, e portanto, $A[x]$ é um ideal fracionário de A. Analogamente, a demonstração do Teorema 2.2, tem-se que $A = \mathfrak{b}'$, o que contraria a Proposição 2.2. Portanto, os ideais inteiros de A são produtos

de potências de ideais primos. Provamos a unicidade desta fatoração. Suponhamos que $\mathfrak{p}$ seja um ideal inteiro de A tal que

$$\mathfrak{p} = \prod_{\mathfrak{p}_i \in \mathcal{P}} \mathfrak{p}_i^{n_i} \quad e \quad \mathfrak{p} = \prod_{\mathfrak{p}_i \in \mathcal{P}} \mathfrak{p}_i^{m_i},$$

com $n_i \neq m_i$ para algum i. Assim $\prod_{\mathfrak{p}_i \in \mathcal{P}} \mathfrak{p}_i^{n_i - m_i} = A$. Denotando por $-\beta_i = n_i - m_i$ se $n_i < m_i$ e por $\alpha_i = n_i - m_i$ se $n_i > m_i$, tem-se que

$$\mathfrak{p}_1^{\alpha_1}\mathfrak{p}_2^{\alpha_2} \dots \mathfrak{p}_r^{\alpha_r} = \mathfrak{q}_1^{\beta_1}\mathfrak{q}_2^{\beta_2} \dots \mathfrak{q}_s^{\beta_s},$$

onde $\mathfrak{p}_1,\ \mathfrak{q}_j \in \mathcal{P}$ e $\mathfrak{p}_i \neq \mathfrak{q}_j$, para $i = 1, \dots, r$ e $j = 1, \dots, s$. Como $\mathfrak{p}_1$ é primo e $\mathfrak{p}_1 \supseteq \mathfrak{p}_1^{\alpha_1}\mathfrak{p}_2^{\alpha_2} \dots \mathfrak{p}_r^{\alpha_r} = \mathfrak{q}_1^{\beta_1}\mathfrak{q}_2^{\beta_2} \dots \mathfrak{q}_s^{\beta_s}$, segue que $\mathfrak{p}_1 \supseteq \mathfrak{q}_j$, para algum $j = 1, \dots, s$. Suponhamos que $\mathfrak{p}_1 \supseteq \mathfrak{q}_1$. Logo, $\mathfrak{p}_1 = \mathfrak{q}_1$, pois $\mathfrak{q}_1$ é maximal, o que contraria o fato de $\mathfrak{p}_1 \neq \mathfrak{q}_j$, para $i = 1, \dots, r$ e $j = 1, \dots, s$. Portanto, a fatoração de $\mathfrak{p}$ é única.

ii) Como o conjunto dos ideais fracionários $\mathcal{F}$ é um monóide comutativo e para qualquer $\mathfrak{p}' \in \mathcal{F}$, tem-se por (i) que $\mathfrak{p}' = \prod_{\mathfrak{p}_i \in \mathcal{P}} \mathfrak{p}_i^{e_i}$, com $\mathfrak{p}_i$ primos em um domínio de Dedekind, e portanto, maximais, segue pelo Teorema 2.2, que $(\mathfrak{p}')^{-1} = \prod_{\mathfrak{p}_i \in \mathcal{P}} \mathfrak{p}_i^{-e_i} \in \mathcal{F}$. Portanto, $\mathcal{F}$ é um grupo. ■

Definição 2.3 *Dizemos que $\mathfrak{q}' \in \mathcal{F}$ divide $\mathfrak{b}' \in \mathcal{F}$ se existe um ideal inteiro $\mathfrak{a}$ tal que $\mathfrak{b}' = \mathfrak{a}\mathfrak{q}'$.*

Proposição 2.3 *Se A é um domínio de Dedekind e*

$$\mathfrak{b}' = \mathfrak{p}_1^{m_1} \dots \mathfrak{p}_r^{m_r} \ e\ \mathfrak{q}' = \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_r^{n_r} \in \mathcal{F},$$

então $\mathfrak{q}' \subseteq \mathfrak{b}' \Leftrightarrow \mathfrak{b}'|\mathfrak{p}' \Leftrightarrow m_1 \leq n_1, \dots, m_r \leq n_r$.

Demonstração. Se $\mathfrak{q}' \subseteq \mathfrak{b}'$, então $\mathfrak{q}'(\mathfrak{b}')^{-1} \subseteq \mathfrak{b}'(\mathfrak{b}')^{-1} = A$, pois $\mathfrak{b}' \in \mathcal{F}$ e $\mathcal{F}$ é um grupo. Deste modo, $\mathfrak{q}'(\mathfrak{b}')^{-1}$ é um ideal inteiro $\mathfrak{m}$ de A. Assim, $\mathfrak{q}' = \mathfrak{m}\mathfrak{b}'$, ou seja, $\mathfrak{b}'|\mathfrak{q}'$. Portanto, pela unicidade da fatoração de ideais em um domínio de Dedekind, tem-se que $m_1 \leq n_1, \dots, m_r \leq n_r$. ■

Teorema 2.4 *Todo domínio de Dedekind A que possui apenas um número finito de ideais primos é um domínio principal.*

Demonstração. Seja $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ o conjunto de ideais primos de A. Como A é um domínio de Dedekind, segue que, para qualquer ideal $\mathfrak{m}$ de A, tem-se $\mathfrak{m} = \prod_{i=1}^{q} \mathfrak{p}_i^{e_1}$. Logo, $1 \leq q \leq r$. Pela Proposição 2.3, segue que $\mathfrak{p}_j^2 \subsetneq \mathfrak{p}_j$, para $1 \leq j \leq r$. Assim, existe $a_j \in \mathfrak{p}_j$ tal que $a_j \notin \mathfrak{p}_j^2$. Além disso, $a_j \notin \mathfrak{p}_h$, para $h \neq j$ e $1 \leq h \leq r$. Logo, $\mathfrak{p}_j | Aa_j$, $\mathfrak{p}_j^2 \nmid Aa_j$ e $\mathfrak{p}_h \nmid Aa_j$, para $h \neq j$ e $1 \leq h, j \leq r$. Fazendo a decomposição de Aa_j em produto de ideais primos, tem-se que $Aa_j = \mathfrak{p}_j$. Deste modo, $\mathfrak{p}_j$ é principal, para $1 \leq j \leq r$. Como todo ideal está contido em um ideal maximal (primo), segue que todo ideal de A é principal.■

Proposição 2.4 *Se A é um domínio de Dedekind e $\mathfrak{b}$ um ideal de A, então o conjunto dos ideais que contém $\mathfrak{b}$ é finito e o conjunto dos ideais de A que estão contidos estritamente em $\mathfrak{b}$ tem seus elementos maximais da forma $\mathfrak{b}\mathfrak{p}$, onde $\mathfrak{p}$ é um ideal primo de A.*

Demonstração. Seja $\mathfrak{m} = \mathfrak{p}_1^{m_1} \ldots \mathfrak{p}_r^{m_r}$ um ideal de A que contém $\mathfrak{b} = \mathfrak{p}_1^{n_1} \ldots \mathfrak{p}_r^{n_r}$. Pela Proposição 2.3, tem-se que $m_j \leq n_j$, para $j = 1, \ldots, r$. Como existe um número finito de $m_j \in \mathbb{N}$ tal que $m_j \leq n_j$, segue que existe um número finito de ideais que contém $\mathfrak{b}$. Agora, se $\mathfrak{m} \subsetneq \mathfrak{b}$, então $\mathfrak{m} = \mathfrak{p}_1^{m_1} \ldots \mathfrak{p}_r^{m_r} = \mathfrak{p}_1^{n_1+k_1} \ldots \mathfrak{p}_r^{n_r+k_r}$, com $k_i \geq 1$, para $i = 1, \ldots, r$. Portanto, os elementos maximais do conjunto dos ideais que estão contidos estritamente em $\mathfrak{b}$ são da forma $\mathfrak{p}\mathfrak{b}$, com $\mathfrak{p}$ ideal primo. ■

2.2 Anéis de frações

O conceito de anel de frações é muito útil na teoria algébrica dos números. Nesta seção vemos o processo de localização, o qual facilita o estudo de alguns anéis, como vemos nos últimos resultados desta seção. A principal referência desta seção é [7].

Sejam A e B anéis e $f : A \longrightarrow B$ um homomorfismo de anéis. Se $\mathfrak{b}'$ é um ideal (primo) de B, então $f^{-1}(\mathfrak{b}') = \mathfrak{b}'^c$ é um ideal (primo) de A, chamado ideal contraído de $\mathfrak{b}'$. Além disso, se $A \subset B$ e f a inclusão, então $\mathfrak{b}'^c = A \cap \mathfrak{b}'$. Agora, se $\mathfrak{b}$ é um ideal de A, então $Bf(\mathfrak{b}) = \mathfrak{b}^e$ é um ideal de B, chamado ideal estendido de $\mathfrak{b}$.

Definição 2.4 *Sejam A um domínio de integridade e $S \subset A - \{0\}$ fechado para multiplicação e com $1 \in S$. Chamamos o anel $\left\{\frac{a}{s};\ a \in A,\ s \in S\right\}$ contido em $\mathbb{K} = Q(A)$ de anel de frações de A com respeito a S e denotamos por $S^{-1}A$.*

Proposição 2.5 *Sejam A um domínio de integridade, $S \subset A - \{0\}$ fechado para mulplicação com $1 \in S$, $f : A \longrightarrow S^{-1}A$ um homomorfismo de anéis dado por $f(a) = \frac{a}{1}$, $\mathcal{I}$ o conjunto de ideais de A e $\mathcal{J}$ o conjunto de ideais de $S^{-1}A$.*

i) Todo ideal de $S^{-1}A$ é um ideal estendido de A.

ii) Se $\theta : \mathcal{I} \longrightarrow \mathcal{J}$ é um homomorfismo dado por $\theta(\mathfrak{b}) = \mathfrak{b}S^{-1}A$, então θ é sobrejetiva.

iii) Se $\varphi : \mathcal{J} \longrightarrow \mathcal{I}$ é um homomorfismo dado por $\varphi(\mathfrak{b}') = \mathfrak{b}' \cap A$, então φ é injetiva.

iv) A composição $\theta \circ \varphi : \mathcal{J} \longrightarrow \mathcal{J}$ é a identidade.

Demonstração. i) Seja $\mathfrak{b}'$ é um ideal de $S^{-1}A$. Como $A \subset S^{-1}A$, segue que $\mathfrak{b}' \cap A \subset \mathfrak{b}' \cap S^{-1}A = \mathfrak{b}'$, e assim, $(\mathfrak{b}' \cap A)S^{-1}A \subset \mathfrak{b}'S^{-1}A \subset \mathfrak{b}'$. Agora, se $\frac{x}{s} \in \mathfrak{b}'$, então $\frac{s}{1}\frac{x}{s} = x \in \mathfrak{b}' \cap A$. Assim, $\frac{x}{s} = x\frac{1}{s} \in (\mathfrak{b}' \cap A)S^{-1}A$. Portanto, $\mathfrak{b}' = (\mathfrak{b}' \cap A)S^{-1}A$.

ii) Mostramos que $\mathcal{J} \subseteq \theta(\mathcal{I})$. Como para qualquer $\mathfrak{b}' \in \mathcal{J}$, podemos escever $\mathfrak{b}' = (\mathfrak{b}' \cap A)S^{-1}A$, segue que $\mathfrak{b}' = \theta(\mathfrak{b}' \cap A)$.

iii) Se $\mathfrak{b}' \neq \mathfrak{a}'$, então $(\mathfrak{b}' \cap A)S^{-1}A \neq (\mathfrak{a}' \cap A)S^{-1}A$. Portanto, $\varphi(\mathfrak{b}') \neq \varphi(\mathfrak{a}')$ o que torna φ injetiva.

iv) Tem-se que

$$\begin{aligned} \theta \circ \varphi : \mathcal{J} &\longrightarrow \quad \mathcal{I} \quad \longrightarrow \mathcal{J} \\ \mathfrak{b}' &\longmapsto \mathfrak{b}' \cap A \longmapsto (\mathfrak{b}' \cap A)S^{-1}A = \mathfrak{b}'. \end{aligned}$$

Portanto, $\theta \circ \varphi = id$. ■

Proposição 2.6 *Se $\mathfrak{b} \in \mathcal{I}$, então $\mathfrak{b}S^{-1}A = \left\{\frac{b}{s};\ b \in \mathfrak{b},\ s \in S\right\}$. Em particular, $\mathfrak{b}S^{-1}A = S^{-1}A$ se, e somente se, $\mathfrak{b} \cap S \neq \varnothing$.*

Demonstração. Tem-se que se $b_i \in \mathfrak{b},\ a_i \in A$ e $s_i \in S$, então

$$\sum_{i=1}^{k} b_i \frac{a_i}{s_i} = \frac{b_1 a_1(s_2 \dots s_k) + \dots + b_i a_i(s_1 \dots s_{i-1}s_{i+1} + \dots + s_k) + \dots + b_k a_k(s_1 \dots s_{k-1})}{s_1 \dots s_k}$$

pertence a $\left\{\frac{b}{s};\ b \in \mathfrak{b},\ s \in S\right\}$ e $\frac{b}{s} = b\frac{1}{s} \in \mathfrak{b}S^{-1}A$. Portanto, $\mathfrak{b}S^{-1}A = S^{-1}\mathfrak{b}$. Agora, se $S^{-1}\mathfrak{b} = S^{-1}A$, então existem $b \in \mathfrak{b}$ e $s \in S$ tal que $\frac{b}{s} = 1$. Assim, $b = s \in \mathfrak{b} \cap S$. Portanto, $\mathfrak{b} \cap S \neq \varnothing$. Por outro lado, se $\mathfrak{b} \cap S \neq \varnothing$, então existe $s \in \mathfrak{b} \cap S$. Logo, $1 = \frac{s}{s} \in S^{-1}\mathfrak{b}$. Portanto, $S^{-1}\mathfrak{b} = S^{-1}A$. ■

Proposição 2.7 *Se $\mathcal{P}$ é o conjunto dos ideais primos de A, $\mathcal{D}$ o conjunto dos ideais primos de $S^{-1}A$ e $\mathcal{P}_S$ o conjunto dos ideais primos de A que não interseptam S, então existe uma bijeção $\varphi : \mathcal{D} \longrightarrow \mathcal{P}_S$*

Demonstração. Se $\mathfrak{p}' \in \mathcal{D}$, então $\mathfrak{p}' \cap A = \mathfrak{p} \in \mathcal{P}$. Se $x \in \mathfrak{p} \cap S$, então $x \in \mathfrak{p}' \cap A = \mathfrak{p} \cap S$. Logo, $1 = x\frac{1}{x} \in \mathfrak{p}'S^{-1}A \subset \mathfrak{p}'$ o que um absurdo. Portanto, $\mathfrak{p} \cap S = \varnothing$. Por outro lado, se $\mathfrak{p} \in \mathcal{P}_S$, então, pela Proposição 2.6, $S^{-1}\mathfrak{p} \neq S^{-1}A$. Se existem $x, y \in A$ e $s, t \in S$ tal que $\frac{x}{s}\frac{y}{t} \in S^{-1}\mathfrak{p}$, então existe $w \in A$ e $z \in S$ tal que $xyz = stw \in \mathfrak{p}$. Como $\mathfrak{p} \cap S = \varnothing$, segue que $z \notin \mathfrak{p}$, e assim, $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$. Logo, $\frac{x}{s} \in S^{-1}\mathfrak{p}$ ou $\frac{y}{t} \in S^{-1}\mathfrak{p}$. Portanto, $S^{-1}\mathfrak{p} \in \mathcal{D}$. Pela Proposição 2.5, tem-se que $(\mathfrak{b}' \cap A)S^{-1}A = \mathfrak{b}'$, para qualquer $\mathfrak{b}' \in \mathcal{D}$. Mostramos que $S^{-1}\mathfrak{p} \cap A = \mathfrak{p}$, para qualquer $\mathfrak{p} \in \mathcal{P}_S$. Como $\mathfrak{p} \subset S^{-1}\mathfrak{p}$, segue que $\mathfrak{p} = \mathfrak{p} \cap A \subset S^{-1}\mathfrak{p} \cap A$. Agora, se $x \in S^{-1}\mathfrak{p} \cap A$, então $x = \frac{y}{s}$, $y \in \mathfrak{p}$ e $s \in S$. Como $sx = y \in \mathfrak{p}$ e $s \notin \mathfrak{p}$ (pois $\mathfrak{p} \cap S = \varnothing$), segue que $x \in \mathfrak{p}$. Portanto, $S^{-1}\mathfrak{p} \cap A = \mathfrak{p}$. ■

Proposição 2.8 *Sejam $A \subset B$ anéis e $S \subset A - \{0\}$ fechado pra multiplicação e com $1 \in S$. Se $\mathcal{O}_B$ é o fecho inteiro de B sobre A, então $S^{-1}\mathcal{O}_B$ é o fecho inteiro de $S^{-1}B$ sobre $S^{-1}A$, ou seja, $S^{-1}\mathcal{O}_B = \mathcal{O}_{S^{-1}B}$.*

Demonstração. Se $\frac{x}{s} \in S^{-1}\mathcal{O}_B$, então $x \in B$ é inteiro sobre A e $s \in S$. Assim, $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$, com $a_i \in A$ e $i = 0, 1, 2, \ldots, n-1$. Dividindo por s^n tem-se que $\left(\frac{x}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{x}{s}\right)^{n-1} + \ldots + \frac{a_0}{s^n} = 0$, com $\frac{a_{n-1}}{s}, \ldots, \frac{a_0}{s^n} \in S^{-1}A$, ou seja, $\frac{x}{s} \in S^{-1}\mathcal{O}_B \subset S^{-1}B$ é inteiro sobre $S^{-1}A$. Portanto, $S^{-1}\mathcal{O}_B \subset \mathcal{O}_{S^{-1}B}$. Por outro lado, se $\frac{x}{s} \in \mathcal{O}_{S^{-1}B}$, então $\frac{x}{s} \in S^{-1}B$ é inteiro sobre $S^{-1}A$. Assim, $\left(\frac{x}{s}\right)^n + \frac{a_{n-1}}{t_{n-1}}\left(\frac{x}{s}\right)^{n-1} + \ldots + \frac{a_0}{t_0} = 0$, com $\frac{a_i}{t_i} \in S^{-1}A$, para $i = 0, 1, 2, \ldots, n-1$. Multiplicando por $(t_0 t_1 \ldots t_{n-1}s)^n$, tem-se que $(t_0 t_1 \ldots t_{n-1}x)^n + a_{n-1}(t_0 t_1 \ldots t_{n-2}s)(t_0 \ldots t_{n-1}x)^{n-1} + \ldots + a_0 t_0^{n-1}(t_1 \ldots t_{n-1}s)^n = 0$, ou seja, $(t_0 t_1 \ldots t_{n-1}x) \in B$ é inteiro sobre A. Como $\frac{x}{s} = \frac{x\,(t_0 \ldots t_{n-1})}{s\,(t_0 \ldots t_{n-1})} \in S^{-1}\mathcal{O}_B$, segue que $\mathcal{O}_{S^{-1}B} \subset S^{-1}\mathcal{O}_B$. Portanto, $S^{-1}\mathcal{O}_B = \mathcal{O}_{S^{-1}B}$. ■

Proposição 2.9 *Se A é um domínio de Dedekind, então $S^{-1}A$ é um domínio de Dedekind.*

Demonstração. Colocando $B = \mathbb{K}$ o corpo de frações de A, pela Proposição 2.8, segue que $S^{-1}\mathcal{O}_{\mathbb{K}} = S^{-1}A = \mathcal{O}_{S^{-1}\mathbb{K}}$. Portanto, $S^{-1}A$ é integralmente fechado. Os ideais $\mathfrak{b}'$ de $S^{-1}A$ são da forma $(\mathfrak{b}' \cap A)S^{-1}A$. Como $\mathfrak{b}' \cap A$ é um ideal de A, segue que $\mathfrak{b}' \cap A$ é finitamente gerado, ou seja, $\mathfrak{b}' \cap A = \langle a_1 \dots a_n \rangle$. Logo, $(\mathfrak{b}' \cap A)S^{-1}A = \langle a_1 \dots a_n \rangle S^{-1}A$. Portanto, $\mathfrak{b}'$ é finitamente gerado. Se $\mathfrak{m}' \in \mathcal{D}$, $\mathfrak{m}' \neq \langle 0 \rangle$, então $\mathfrak{m}' \cap A = \mathfrak{m}$ é um ideal primo de A não nulo, pois $\mathfrak{m} \cap S = \varnothing$, e maximal, pois A é Dedekind. Como $\mathfrak{m}' = (\mathfrak{m}' \cap A)S^{-1}A = S^{-1}\mathfrak{m}$, segue que $\mathfrak{m}'$ é um ideal maximal de $S^{-1}A$. Portanto, $S^{-1}A$ é um domínio de Dedekind. ■

Definição 2.5 *Seja A um domínio de integridade. Dizemos que um elemento $p \in A$ é primo se o ideal principal $\langle p \rangle$ é um ideal primo.*

Proposição 2.10 *Se A é um domínio de Dedekind, $\mathfrak{p}$ um ideal primo não nulo de A e $S = A - \mathfrak{p}$, então $S^{-1}A$ é principal. Mais precisamente, existe um primo $p \in S^{-1}A$ tal que os ideais não nulos de $S^{-1}A$ são da forma $\langle p^n \rangle$, com $n \in \mathbb{N}$.*

Demonstração. Tem-se que $\mathfrak{p}$ é o único ideal primo de A tal que $\mathfrak{p} \cap S = \varnothing$. Assim, $\mathfrak{p}' = S^{-1}\mathfrak{p}$ é o único ideal primo não nulo de $S^{-1}A$. Portanto, $S^{-1}A$ é principal (Teorema 2.4). Como $S^{-1}A$ é um domínio de Dedekind, segue que todo ideal não nulo de $S^{-1}A$ é da forma $(\mathfrak{p}')^n$. Se $p \in \mathfrak{p}' - (\mathfrak{p}')^2$, então $\langle p \rangle \subset \mathfrak{p}' - (\mathfrak{p}')^2$. Logo, $\langle p \rangle = \mathfrak{p}'$, e assim, $\langle p^n \rangle = (\mathfrak{p}')^n$, para todo $n \in \mathbb{N}$. Como $\mathfrak{p}$ é um ideal primo, segue que p é um elemento primo. Portanto, $S^{-1}A$ é principal e seus ideais são da forma $\langle p^n \rangle$, para todo $n \in \mathbb{N}$. ■

Proposição 2.11 *Se $\mathfrak{m}$ é um ideal maximal de A que não intersepta S, então* $\dfrac{S^{-1}A}{S^{-1}\mathfrak{m}} \simeq \dfrac{A}{\mathfrak{m}}$.

Demonstração. Considere o homomorfismo

$$\varphi : A \longrightarrow S^{-1}A \longrightarrow \frac{S^{-1}A}{S^{-1}\mathfrak{m}},$$

cujo $Ker(\varphi) = A \cap S^{-1}\mathfrak{m} = \mathfrak{m}$. Assim, existe um homomorfismo injetor de $\dfrac{A}{\mathfrak{m}}$ em $\dfrac{S^{-1}A}{S^{-1}\mathfrak{m}}$. Agora, se $x = \dfrac{a}{s} \in S^{-1}A$, então $\bar{x} = x + S^{-1}\mathfrak{m} = \dfrac{a}{s} + S^{-1}\mathfrak{m}$. Como $\mathfrak{m} \cap S = \varnothing$ e $\mathfrak{m}$ é

maximal, segue que $A = \mathfrak{m} + \langle s \rangle$, para todo $s \in S$, ou seja, existe $m \in \mathfrak{m}$, $s \in S$ e $b \in A$ tal que $1 = m + bs$. Logo, $bs \equiv 1(mod\ \mathfrak{m})$. Assim, $\frac{a}{s} - ab = \frac{a}{s}(1 - sb) \in S^{-1}\mathfrak{m}$. Logo, $\varphi(ab) = \bar{x}$. Portanto, $\frac{A}{\mathfrak{m}} \simeq \frac{S^{-1}A}{S^{-1}\mathfrak{m}}$. ■

2.3 Norma de ideais

Na seção 1.4 estudamos norma de um elemento $x \in B$, onde B é um A-módulo livre e nesta seção apresentamos alguns resultados sobre norma de um ideal. A principal referência desta seção é [12].

Definição 2.6 *Seja A um anel, $\mathfrak{m}$ ideal maximal de A e B um A-módulo. Dizemos que B é anulado por $\mathfrak{m}$ se para todo $m \in \mathfrak{m}$ e para todo $b \in B$ tem-se $mb = 0$.*

Observação 2.1 *Se B é um A-módulo anulado por um ideal maximal $\mathfrak{m}$, então B pode ser considerado como um $\frac{A}{\mathfrak{m}}$-espaço vetorial, onde $\varphi : \frac{A}{\mathfrak{m}} \times B \longrightarrow B$ é dada por $\varphi(\bar{a}, x) = ax$. Agora, se C é um $\frac{A}{\mathfrak{m}}$-espaço vetorial, então C é um A-módulo com $\phi : A \times C \longrightarrow C$ dada por $\phi(a, c) = (a + \mathfrak{m})c$ e C é anulado por $\mathfrak{m}$. Portanto, os $\frac{A}{\mathfrak{m}}$-espaços vetoriais coincidem com os A-módulos anulados por $\mathfrak{m}$.*

Proposição 2.12 *Se A é um domínio de Dedekind, $\mathfrak{m}$ um ideal maximal de A e $\mathfrak{b}$ um ideal não nulo de A, então $\frac{\mathfrak{b}}{\mathfrak{m}\mathfrak{b}}$ é um $\frac{A}{\mathfrak{m}}$-espaço vetorial de dimensão 1.*

Demonstração. Se $\bar{x} \in \frac{\mathfrak{b}}{\mathfrak{m}\mathfrak{b}}$ e $m \in \mathfrak{m}$, então $m\bar{x} = mx + \mathfrak{m}\mathfrak{b}$, com $m \in \mathfrak{m}$ e $x \in \mathfrak{b}$. Logo, $m\bar{x} \in \mathfrak{m}\mathfrak{b}$, ou seja, $\mathfrak{m}$ é o anulador de $\frac{\mathfrak{b}}{\mathfrak{m}\mathfrak{b}}$. Portanto, $\frac{\mathfrak{b}}{\mathfrak{m}\mathfrak{b}}$ é um $\frac{A}{\mathfrak{m}}$-espaço vetorial. Os $\frac{A}{\mathfrak{m}}$-subespaços próprios de $\frac{\mathfrak{b}}{\mathfrak{m}\mathfrak{b}}$ são da forma, $\frac{\mathfrak{p}}{\mathfrak{m}\mathfrak{b}}$, onde $\mathfrak{p}$ é um ideal de A e $\mathfrak{m}\mathfrak{b} \subsetneq \mathfrak{p} \subsetneq \mathfrak{b}$ o que contraria a Proposição 2.4. Portanto, $\frac{\mathfrak{b}}{\mathfrak{m}\mathfrak{b}}$ é um $\frac{A}{\mathfrak{m}}$-espaço de dimensão 1. ■

Consideramos agora $\mathbb{L}|\mathbb{Q}$ uma extensão finita de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros algébricos de $\mathbb{L}$.

Proposição 2.13 *Se $\mathfrak{p}$ é um ideal primo não nulo de $\mathcal{O}_{\mathbb{L}}$, então*

i) $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, onde p é o único número primo de $\mathfrak{p}$;

ii) $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}}$ *é uma extensão finita de* $\mathbb{F}_p = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ *e* $\left[\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}} : \mathbb{F}_p\right] \leq n$.

Demonstração. i) Pela Proposição 2.1, tem-se que $\mathfrak{p} \cap \mathbb{Z}$ é um ideal primo de $\mathbb{Z}$. Logo, $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, com $p \in \mathbb{Z}$ primo. Como $\mathcal{O}_{\mathbb{L}}$ é inteiro sobre $\mathbb{Z}$, segue que $\mathfrak{p} \cap \mathbb{Z} \neq \langle 0 \rangle$, pois se $x \in \mathfrak{p} \subset \mathcal{O}_{\mathbb{L}}$, então x é inteiro sobre $\mathbb{Z}$, e assim, supondo n mínimo tem-se que $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$, com $a_i \in \mathbb{Z}$, $a_0 \neq 0$ e $a_0 \in \mathcal{O}_{\mathbb{L}}x \cap \mathbb{Z} \subset \mathfrak{p} \cap \mathbb{Z}$. Finalmente, se $q \in \mathbb{Z}$ é um primo e $q \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, então $q = p$. Assim, p é o único primo em $\mathfrak{p}$.

ii) Consideramos o homomorfismo canônico

$$\begin{aligned} \varphi : \mathcal{O}_{\mathbb{L}} &\longrightarrow \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}} \\ x &\longmapsto x + \mathfrak{p}. \end{aligned}$$

Restringindo φ a $\mathbb{Z}$ tem-se que $Ker(\varphi|_{\mathbb{Z}}) = \mathbb{Z} \cap \mathfrak{p} = p\mathbb{Z}$. Assim, pela demosntração do Teorema 1.12, tem-se que $\dfrac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{F}_p \simeq \varphi(\mathbb{Z})$, que é um subcorpo de $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}}$. Assim, existe uma base de $\mathbb{L}$ sobre $\mathbb{K}$ dada por $\{\beta_1, \ldots, \beta_n\}$ contida em $\mathcal{O}_{\mathbb{L}}$. Portanto, $\{\varphi(\beta_1), \ldots, \varphi(\beta_n)\}$ gera $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}}$ como $\mathbb{F}_p$-espaço vetorial. ■

Definição 2.7 *Seja* $\mathfrak{b}$ *um ideal não nulo de* $\mathcal{O}_{\mathbb{L}}$. *Chamamos de norma do ideal* $\mathfrak{b}$ *o número de elementos de* $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{b}}$ *e denotamos por* $N(\mathfrak{b})$.

Proposição 2.14 *Sejam* $\mathfrak{p}$ *um ideal primo não nulo de* $\mathcal{O}_{\mathbb{L}}$ *e* $\mathfrak{b}$, $\mathfrak{q}$ *ideais não nulos de* $\mathcal{O}_{\mathbb{L}}$.

a) $N(\mathfrak{p}) = p^f$, *onde* $f = \left[\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}} : \mathbb{F}_p\right]$ *e* p *o único primo em* $\mathfrak{p}$;

b) $N(\mathfrak{bq}) = N(\mathfrak{b})N(\mathfrak{q})$;

c) $N(\mathfrak{b}) \in \mathbb{N} - \{0\}$ *e* $N(\mathfrak{b}) = 1$ *se, e somente se,* $\mathfrak{b} = \mathcal{O}_{\mathbb{L}}$;

d) $N(\mathfrak{b}) \in \mathfrak{b}$;

e) Se $N(\mathfrak{b})$ *é um número primo, então* $\mathfrak{b}$ *é um ideal primo;*

f) Se $\mathfrak{b}$ *for múltiplo de* $\mathfrak{q}$ *e* $N(\mathfrak{b}) = N(\mathfrak{q})$, *então* $\mathfrak{b} = \mathfrak{q}$.

Demonstração. a) Pela Proposição 2.13, tem-se que $\mathfrak{p}$ aparece na fatoração de $p\mathcal{O}_{\mathbb{L}}$ em produto de ideais primos de $\mathcal{O}_{\mathbb{L}}$ e $\left[\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}} : \mathbb{F}_p\right] = f \leq n$. Assim, se $\overline{x} \in \dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}}$, então $x = a_1\alpha_1 + a_2\alpha_2 + \ldots + a_f\alpha_f$, com $\{\alpha_1, \ldots, \alpha_f\}$ é uma base de $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}}$ sobre $\mathbb{F}_p$ e $a_1, \ldots, a_f \in \mathbb{F}_p$. Portanto, $\#\left(\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}}\right) = p^f$.

b) Como $\mathfrak{q} = \mathfrak{p}_1 \ldots \mathfrak{p}_r$, onde os $\mathfrak{p}_i$'s são ideais primos não nulos de $\mathcal{O}_{\mathbb{L}}$, segue que basta mostrar que $N(\mathfrak{bp}) = N(\mathfrak{b})N(\mathfrak{p})$, com $\mathfrak{p} = \mathfrak{p}_i$, para algum $i = 1, \ldots, r$, ou seja, $\#\left(\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{bp}}\right) = \#\left(\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{b}}\right)\#\left(\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}}\right)$. Consideramos o homomorfismo $\phi : \dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{bp}} \longrightarrow \dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{b}}$ dado por $\phi(x + \mathfrak{bp}) = x + \mathfrak{b}$. Como $\mathfrak{bp} \subset \mathfrak{b}$, segue que ϕ é sobrejetivo. Além disso, $Ker(\phi) = \dfrac{\mathfrak{b}}{\mathfrak{bp}}$. Deste modo, $\#\left(\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{bp}}\right) = \#\left(\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{b}}\right)\#\left(\dfrac{\mathfrak{b}}{\mathfrak{bp}}\right)$, e assim, para mostrar que $N(\mathfrak{bp}) = N(\mathfrak{b})N(\mathfrak{p})$, basta mostrar que $\#\left(\dfrac{\mathfrak{b}}{\mathfrak{bp}}\right) = \#\left(\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}}\right)$. Notemos que $\dfrac{\mathfrak{b}}{\mathfrak{bp}}$ é um $\mathcal{O}_{\mathbb{L}}$-módulo anulado por $\mathfrak{p}$, pois se $x \in \mathfrak{b}$ e $p \in \mathfrak{p}$, então $xp \in \mathfrak{bp}$. Assim, pela Proposição 2.12, tem-se que $\dfrac{\mathfrak{b}}{\mathfrak{bp}}$ é um $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}}$ -espaço vetorial de dimensão 1. Deste modo, $\#\left(\dfrac{\mathfrak{b}}{\mathfrak{bp}}\right) = \#\left(\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}}\right)$. Portanto, $N(\mathfrak{bp}) = N(\mathfrak{b})N(\mathfrak{p})$.

c) Pelo item (b), tem-se que $N(\mathfrak{b}) = N(\mathfrak{p}_1 \ldots \mathfrak{p}_r) = N(\mathfrak{p}_1) \ldots N(\mathfrak{p}_r) \in \mathbb{N} - \{0\}$. Além disso, $N(\mathfrak{b}) = 1$ se, e somente se, $r = 0$ se, e somente se, $\mathfrak{b} = \mathcal{O}_{\mathbb{L}}$.

d) Tem-se que $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{b}}$ é um grupo aditivo com ordem $N(\mathfrak{b})$. Assim, $N(\mathfrak{b})\overline{1} = \overline{0}$, ou seja, $N(\mathfrak{b}) \in \mathfrak{b}$.

e) Suponhamos que $\mathfrak{b}$ não é um ideal primo de $\mathcal{O}_{\mathbb{L}}$. Assim, $\mathfrak{b} = \mathcal{O}_{\mathbb{L}}$ ou $\mathfrak{b} = \mathfrak{am}$, onde $\mathfrak{a}$ e $\mathfrak{m}$ são ideais não nulos e distintos de $\mathcal{O}_{\mathbb{L}}$. Logo, $N(\mathfrak{b}) = 1$ ou $N(\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{m})$, ou seja, em ambos os casos $N(\mathfrak{b})$ não é um número primo.

f) Por hipótese existe um ideal não nulo $\mathfrak{m}$ tal que $\mathfrak{b} = \mathfrak{qm}$. Logo, $N(\mathfrak{b}) = N(\mathfrak{q})N(\mathfrak{m}) = N(\mathfrak{q})$. Deste modo, $N(\mathfrak{m}) = 1$, ou seja, $\mathfrak{m} = \mathcal{O}_{\mathbb{L}}$. Portanto, $\mathfrak{b} = \mathfrak{q}$. ■

2.4 Ramificação

A teoria de ramificação é a principal ferramenta para a demonstração do Teorema de Kronecker-Weber. Por este fato esta seção é a mais importante do trabalho. As principais referências desta seção são [12], [17] e [18].

Consideramos, nesta seção, A um domínio de Dedekind, $\mathbb{K}$ o corpo de frações de A,

$\mathbb{L}|\mathbb{K}$ uma extensão finita de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de $\mathbb{L}$ sobre A. Pelo Teorema 2.1, tem-se que $\mathcal{O}_{\mathbb{L}}$ é um domínio de Dedekind. Denotamos por $\mathfrak{p},\ \mathfrak{q},\ \mathfrak{a},\ \mathfrak{b},\ \mathfrak{m}$ os ideais de anel A e por $\mathfrak{P}, \mathfrak{B},\ \mathfrak{M}$, os ideais do anel $\mathcal{O}_{\mathbb{L}}$.

Se considerarmos a aplicação $i : A \longrightarrow \mathcal{O}_{\mathbb{L}}$ (i inclusão) e $\mathfrak{p}$ um ideal primo não nulo de A, então $\mathcal{O}_{\mathbb{L}} i(\mathfrak{p}) = \mathcal{O}_{\mathbb{L}}\mathfrak{p} = \prod_{i=1}^{g} \mathfrak{P}_i{}^{e_i}$, onde $\mathfrak{P}_i$ é ideal primo não nulo de $\mathcal{O}_{\mathbb{L}}$ e $e_i \in \mathbb{N}$, para $i = 1, \ldots, g$.

Lema 2.1 *Sejam $\mathfrak{P}$ um ideal primo não nulo de $\mathcal{O}_{\mathbb{L}}$ e $\mathfrak{p}$ um ideal primo não nulo de A. Para que $\mathfrak{P} \cap A = \mathfrak{p}$, é necessário e suficiente, que $\mathcal{O}_{\mathbb{L}}\mathfrak{p} \subset \mathfrak{P}$.*

Demonstração. Se $x \in \mathcal{O}_{\mathbb{L}}\mathfrak{p}$, então $x = by$, com $y \in \mathfrak{p}$ e $b \in \mathcal{O}_{\mathbb{L}}$. Como $\mathfrak{P} \cap A = \mathfrak{p}$, segue que $y \in \mathfrak{P}$. Logo, $x \in \mathfrak{P}$, pois $\mathfrak{P}$ é ideal de $\mathcal{O}_{\mathbb{L}}$, ou seja, $by \in \mathcal{O}_{\mathbb{L}}\mathfrak{P} \subset \mathfrak{P}$. Reciprocamente, se $x \in \mathfrak{p} \subset A$, então $x \in \mathcal{O}_{\mathbb{L}}\mathfrak{p} \subset \mathfrak{P}$. Logo, $x \in \mathfrak{P} \cap A$, e assim, $\mathfrak{p} \subset \mathfrak{P} \cap A \subsetneq A$. Como $\mathfrak{p}$ é maximal, segue que $\mathfrak{p} = \mathfrak{P} \cap A$. ■

Proposição 2.15 *Os ideais primos $\mathfrak{P}_i$'s que aparecem na fatoração de $\mathcal{O}_{\mathbb{L}}\mathfrak{p}$ são exatamente aqueles ideais primos de $\mathcal{O}_{\mathbb{L}}$ tal que a interseção com A é $\mathfrak{p}$.*

Demonstração. Como $\mathcal{O}_{\mathbb{L}}\mathfrak{p} = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$, segue que $\mathcal{O}_{\mathbb{L}}\mathfrak{p} \subset \mathfrak{P}_i$, para $i = 1, \ldots, g$. Pelo Lema 2.1, segue que $\mathfrak{P}_i$ aparece na fatoração de $\mathcal{O}_{\mathbb{L}}\mathfrak{p}$ se, e somente se, $\mathfrak{P}_i \cap A = \mathfrak{p}$. ■

O homomorfismo $\varphi_i = \pi \circ i : A \longrightarrow \mathcal{O}_{\mathbb{L}} \longrightarrow \dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}_i}$, onde π é a projeção e i a inclusão, tem $Ker(\varphi_i) = A \cap \mathfrak{P}_i = \mathfrak{p}$. Logo, $\dfrac{A}{\mathfrak{p}}$ pode ser visto como um subanel de $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}_i}$, e como ambos são corpos, segue que $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}_i}$ é um $\dfrac{A}{\mathfrak{p}}$-espaço vetorial de dimensão finita, pois $\mathcal{O}_{\mathbb{L}}$ é um A-módulo finitamente gerado. Como $\mathcal{O}_{\mathbb{L}}\mathfrak{p} = \prod_{i=1}^{g} \mathfrak{P}_i{}^{e_i}$, segue que $\mathcal{O}_{\mathbb{L}}\mathfrak{p} \cap A = \mathfrak{p}$, pois $\mathfrak{p} \subset \mathcal{O}_{\mathbb{L}}\mathfrak{p}$ e $\mathfrak{p} \subset A$ implica que $\mathfrak{p} \subset \mathcal{O}_{\mathbb{L}} \cap A$ e $\mathcal{O}_{\mathbb{L}}\mathfrak{p} \subset \mathfrak{P}_i$, e assim, $\mathcal{O}_{\mathbb{L}}\mathfrak{p} \cap A \subset \mathfrak{P}_i \cap A = \mathfrak{p}$.

Definição 2.8 *Seja $\mathcal{O}_{\mathbb{L}}\mathfrak{p} = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$, onde $\mathfrak{P}_i$'s são ideais primos não nulos de $\mathcal{O}_{\mathbb{L}}$.*

1) *O grau $\left[\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}_i} : \dfrac{A}{\mathfrak{p}}\right] = dim_{A/\mathfrak{p}}(\mathcal{O}_{\mathbb{L}}/\mathfrak{P}_i)$ é chamado de grau de inércia de $\mathfrak{P}_i$ sobre $\mathfrak{p}$ e denotamos por $f_i = f(\mathfrak{P}_i|\mathfrak{p})$.*

2) O expoente $e_i = e(\mathfrak{P}_i|\mathfrak{p})$ *de* $\mathfrak{P}_i$ *é chamado de índice de ramificação de* $\mathfrak{P}_i$ *sobre* $\mathfrak{p}$.

3) Os ideais primos $\mathfrak{P}_i$*'s de* $\mathcal{O}_{\mathbb{L}}$ *são chamados ideais de* $\mathcal{O}_{\mathbb{L}}$ *que estão acima de* $\mathfrak{p}$.

Teorema 2.5 *(Igualdade Fundamental) Se* A *é um domínio de Dedekind,* $\mathbb{K}$ *seu corpo de frações,* $\mathbb{L}|\mathbb{K}$ *uma extensão finita de grau* n*,* $\mathcal{O}_{\mathbb{L}}$ *o anel de inteiros de* $\mathbb{L}$ *sobre* A *e* $\mathfrak{p}$ *um ideal primo não nulo de* A*, então* $\sum_{i=1}^{g} e_i f_i = \left[\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{O}_{\mathbb{L}}\mathfrak{p}} : \frac{A}{\mathfrak{p}}\right] = n$.

Demonstração. Primeiramente mostramos que $\sum_{i=1}^{g} e_i f_i = \left[\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{O}_{\mathbb{L}}\mathfrak{p}} : \frac{A}{\mathfrak{p}}\right]$. Para isto consideramos a sequência de ideais

$$\mathcal{O}_{\mathbb{L}} \supset \mathfrak{P}_1 \supset \mathfrak{P}_1^2 \supset \ldots \supset \mathfrak{P}_1^{e_1}\mathfrak{P}_2 \supset \ldots \supset \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2} \supset \ldots \supset \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\ldots\mathfrak{P}_g^{e_g} = \mathcal{O}_{\mathbb{L}}\mathfrak{p}.$$

Quaisquer dois elementos consecutivos desta sequência são da forma $\mathfrak{P}$ e $\mathfrak{P}\mathfrak{P}_i$ e pela Proposição 2.4, segue que não existe $\mathfrak{m}$ ideal de $\mathcal{O}_{\mathbb{L}}$ tal que $\mathfrak{P} \supset \mathfrak{m} \supset \mathfrak{P}\mathfrak{P}_i$. Assim, a sequencia é maximal. Além disso, pela Proposição 2.12, segue que $\frac{\mathfrak{P}}{\mathfrak{P}\mathfrak{P}_i}$ é um $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}_i}$-espaço vetorial de dimensão 1. Logo, $\left[\frac{\mathfrak{P}}{\mathfrak{P}\mathfrak{P}_i} : \frac{A}{\mathfrak{p}}\right] = \left[\frac{\mathfrak{P}}{\mathfrak{P}\mathfrak{P}_i} : \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}_i}\right]\left[\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}_i} : \frac{A}{\mathfrak{p}}\right] = f_i$. Como existem e_1 elementos entre $\mathcal{O}_{\mathbb{L}}$ e $\mathfrak{P}_1^{e_1}$, e_2 elementos entre $\mathfrak{P}_1^{e_1}$ e $\mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}$, e assim sucessivamente sempre deixando de considerar o último, segue que $\sum_{i=1}^{g} e_i f_i = \left[\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{O}_{\mathbb{L}}\mathfrak{p}} : \frac{A}{\mathfrak{p}}\right]$.

Agora, mostramos que $\left[\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{O}_{\mathbb{L}}\mathfrak{p}} : \frac{A}{\mathfrak{p}}\right] = n$. Para isto, lembramos que se A é principal, então $\mathcal{O}_{\mathbb{L}}$ é um A-módulo livre de posto n (Corolário 1.9). Assim, se $\{x_1, x_2, \ldots, x_n\}$ é uma base de $\mathcal{O}_{\mathbb{L}}$ sobre A, então teremos que $\{x_1 + \mathcal{O}_{\mathbb{L}}\mathfrak{p}, \ldots, x_n + \mathcal{O}_{\mathbb{L}}\mathfrak{p}\}$ é uma base de $\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{O}_{\mathbb{L}}\mathfrak{p}}$ sobre $\frac{A}{\mathfrak{p}}$. Pois, se $\bar{y} = y + \mathcal{O}_{\mathbb{L}}\mathfrak{p} \in \frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{O}_{\mathbb{L}}\mathfrak{p}}$, ou seja, $\bar{y} = (a_1x_1 + \ldots + a_nx_n) + \mathcal{O}_{\mathbb{L}}\mathfrak{p} = (a_1 + \mathfrak{p})(x_1 + \mathcal{O}_{\mathbb{L}}\mathfrak{p}) + \ldots + (a_n + \mathfrak{p})(x_n + \mathcal{O}_{\mathbb{L}}\mathfrak{p})$, com $a_i + \mathfrak{p} \in \frac{A}{\mathfrak{p}}$ e $x_i + \mathcal{O}_{\mathbb{L}}\mathfrak{p} \in \frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{O}_{\mathbb{L}}\mathfrak{p}}$, então $\{x_1 + \mathcal{O}_{\mathbb{L}}\mathfrak{p}, \ldots, x_n + \mathcal{O}_{\mathbb{L}}\}$ gera $\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{O}_{\mathbb{L}}\mathfrak{p}}$ sobre $\frac{A}{\mathfrak{p}}$. E se $\bar{a_1}\bar{x_1} + \ldots + \bar{a_n}\bar{x_n} = \bar{0}$, então $\sum_{i=1}^{n} \bar{a_i}\bar{x_i} \in \mathcal{O}_{\mathbb{L}}\mathfrak{p}$, ou seja, $\sum_{i=1}^{n} \bar{a_i}\bar{x_i} = \sum_{j=1}^{m} y_j p_j$, onde $y_j \in \mathcal{O}_{\mathbb{L}}$ e $p_j \in \mathfrak{p}$, e assim, $\sum_{i=1}^{n} \bar{a_i}\bar{x_i} = \sum_{j=1}^{m}(\sum_{i=1}^{n} c_{ij}x_i)p_j = \sum_{i=1}^{n}(\sum_{j=1}^{m} c_{ij}p_j)x_i$, com $a_i = \sum_{j=1}^{m} c_{ij}p_j \in \mathfrak{p}$, para $i = 1, 2, \ldots, n$, isto é, $\bar{a_i} = \bar{0}$, para $i = 1, 2, \ldots, n$ o que torna $\{\bar{x_1}, \bar{x_2}, \ldots, \bar{x_n}\}$ linearmente independente

sobre $\frac{A}{\mathfrak{p}}$. Agora, consideramos $S = A - \mathfrak{p}$, onde $\mathfrak{p}$ é um ideal primo não nulo de A, e assim, pela Proposição 2.10, segue que $S^{-1}A = A'$ é um anel principal. Assim, $S^{-1}\mathcal{O}_{\mathbb{L}} = \mathcal{O}'_{\mathbb{L}}$ é um A-módulo livre de posto n. Procedendo como na primeira parte tem-se que $\left[\frac{\mathcal{O}'_{\mathbb{L}}}{\mathcal{O}'_{\mathbb{L}}\mathfrak{p}} : \frac{A'}{A'\mathfrak{p}}\right] = n$. Consideramos a fatoração de $\mathcal{O}'_{\mathbb{L}}\mathfrak{p}$ em $\mathcal{O}'_{\mathbb{L}}$. Notemos, primeiramente, que se $\mathfrak{P}_i$ está acima de $\mathfrak{p}$ em $\mathcal{O}_{\mathbb{L}}$, então $\mathfrak{P}_i \cap S = \varnothing$, e assim $(\mathfrak{P}_i \cap \mathcal{O}_{\mathbb{L}})\mathcal{O}'_{\mathbb{L}}$ é um ideal primo de $\mathcal{O}'_{\mathbb{L}}$. Como $S^{-1}\mathfrak{P}_i \cap S^{-1}A = S^{-1}\mathfrak{p}$, segue que $\mathcal{O}'_{\mathbb{L}}\mathfrak{p} = \prod_{i=1}^{g} (S^{-1}\mathfrak{P}_i)^{e_i}$, com $e_i \in \mathbb{N}$. Além disso, o homomorfismo canônico φ de $\mathcal{O}_{\mathbb{L}}$ em $\mathcal{O}'_{\mathbb{L}}$ dado por $\varphi(x) = \frac{x}{1}$, induz um isomorfismo de $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}_i}$ em $\frac{\mathcal{O}'_{\mathbb{L}}}{S^{-1}\mathfrak{P}_i}$, o qual é um isomorfismo de um $\frac{A}{\mathfrak{p}}$-espaço em um $\frac{S^{-1}A}{S^{-1}\mathfrak{p}}$-espaço. Logo, podemos concluir que $e(S^{-1}\mathfrak{P}_i|S^{-1}\mathfrak{p}) = e(\mathfrak{P}_i|\mathfrak{p})$ e $f(S^{-1}\mathfrak{P}_i|S^{-1}\mathfrak{p}) = f(\mathfrak{P}_i|\mathfrak{p})$, para $1 \leq i \leq g$. Portanto, $n = \left[\frac{\mathcal{O}'_{\mathbb{L}}}{\mathcal{O}'_{\mathbb{L}}\mathfrak{P}} : \frac{A'}{A'\mathfrak{p}}\right] = \sum_{i=1}^{g} e(S^{-1}\mathfrak{P}_i|S^{-1}\mathfrak{p}) f(S^{-1}\mathfrak{P}_i|S^{-1}\mathfrak{p}) = \sum_{i=1}^{g} e(\mathfrak{P}_i|\mathfrak{p}) f(\mathfrak{P}_i|\mathfrak{p}) = \left[\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{O}_{\mathbb{L}}\mathfrak{p}} : \frac{A}{\mathfrak{p}}\right]$. ■

Definição 2.9 *Dizemos que o ideal primo $\mathfrak{p}$ de A é*

a) totalmente decomposto em $\mathcal{O}_{\mathbb{L}}$ ou $\mathbb{L}$, se $g = n$;

b) totalmente inerte em $\mathcal{O}_{\mathbb{L}}$ ou $\mathbb{L}$, se $f(\mathfrak{P}|\mathfrak{p}) = n$, para algum $\mathfrak{P}$ ideal acima de $\mathfrak{p}$;

c) totalmente ramificado em $\mathcal{O}_{\mathbb{L}}$ ou $\mathbb{L}$, se $e(\mathfrak{P}|\mathfrak{p}) = n$, para algum $\mathfrak{P}$ ideal acima de $\mathfrak{p}$;

d) ramificado em $\mathcal{O}_{\mathbb{L}}$ ou $\mathbb{L}$, se $e(\mathfrak{P}|\mathfrak{p}) > 1$ para algum $\mathfrak{P}$ ideal acima de $\mathfrak{p}$.

O próximo teorema permite indicar explicitamente a fatoração de um ideal primo $\mathfrak{p}$ em $\mathcal{O}_{\mathbb{L}}$, quando $\mathcal{O}_{\mathbb{L}}$ é da forma $A[\beta]$, onde $\beta \in \mathcal{O}_{\mathbb{L}}$.

Teorema 2.6 *(Kummer) Se $\mathcal{O}_{\mathbb{L}} = A[\beta]$, $p(x) = min_{\mathbb{K}}\beta$ e $p_1, \ldots, p_r$ são polinômios mônicos em $A[x]$ tais que $\overline{p} = \bar{p_1}^{e_1} \ldots \bar{p_r}^{e_r}$ (fatoração de $\bar{p}$ em polinômios irredutíveis em $\frac{A}{\mathfrak{p}}[x]$), então*

a) $\mathcal{O}_{\mathbb{L}}\mathfrak{p} = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r}$, onde $\mathfrak{P}_j = \mathcal{O}_{\mathbb{L}}\mathfrak{p} + \mathcal{O}_{\mathbb{L}}p_j(\beta)$, com $\mathfrak{P}_j$ os ideais primos distintos de $\mathcal{O}_{\mathbb{L}}$ acima de $\mathfrak{p}$. Logo, $e(\mathfrak{P}_j|\mathfrak{p}) = e_j$, para $1 \leq j \leq r$;

b) $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}_j} = \frac{A}{\mathfrak{p}}(\beta_j)$, onde β_j é raiz de p_j. Logo, $f(\mathfrak{P}_j|\mathfrak{p}) = gr(p_j)$, para $1 \leq j \leq r$.

Demonstração. Provamos inicialmente a existência de ideais primos $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ de $\mathcal{O}_{\mathbb{L}}$, distintos acima de $\mathfrak{p}$, que satisfazem (b).

b) Se $\widetilde{\beta}_j$ é uma raiz de $\bar{p_j}$, então $\bar{p_j} = min_{\frac{A}{\mathfrak{p}}}\widetilde{\beta}_j$, pois $\bar{p_j}$ é mônico e irredutível sobre $\frac{A}{\mathfrak{p}}$. Consideramos o homomorfismo $\varphi_j : A[x] \longrightarrow \left(\frac{A}{\mathfrak{p}}\right)[\widetilde{\beta}_j]$ dado por $\varphi_j(f(x)) = \bar{f}(\widetilde{\beta}_j)$. Tem-se que $f(x) \in Ker(\varphi_j)$ se, e somente se, $\bar{p_j}|\bar{f}$. Logo, $p(x) \in Ker(\varphi_j)$. Deste modo, podemos considerar o homomorfismo $\bar{\varphi_j} : \frac{A[x]}{\langle p(x)\rangle} \longrightarrow \left(\frac{A}{\mathfrak{p}}\right)[\widetilde{\beta}_j]$ induzido do homomorfismo φ_j. Agora, notemos que o homomorfismo sobrejetivo $\phi : A[x] \longrightarrow A[\beta]$ dado por $\phi(f(x)) = f(\beta)$ tem núcleo $\langle p(x)\rangle$, e assim, $\bar{\phi} : \frac{A[x]}{\langle p(x)\rangle} \longrightarrow A[\beta]$ é um isomorfismo. Deste modo, $\phi_j = \bar{\varphi_j} \circ \bar{\phi}^{-1}$ é um homomorfismo de $\mathcal{O}_{\mathbb{L}} = A[\beta]$ em $\left(\frac{A}{\mathfrak{p}}\right)[\widetilde{\beta}_j]$ tal que $\phi_j(f(\beta)) = \bar{f}(\widetilde{\beta}_j)$, para todo $f(x) \in A[x]$. Como $\left(\frac{A}{\mathfrak{p}}\right)[\widetilde{\beta}_j]$ é um corpo, segue que $Ker(\phi_j) = \mathfrak{P}_j$ é um ideal primo (maximal) de $\mathcal{O}_{\mathbb{L}}$. Assim, ϕ_j induz um isomorfismo $\bar{\phi_j} : \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}_j} \longrightarrow \left(\frac{A}{\mathfrak{p}}\right)[\widetilde{\beta}_j]$. Como $\mathfrak{p} \subseteq \mathfrak{P}_j \cap A$, segue, pela maximalidade de $\mathfrak{p}$, que $\mathfrak{p} = \mathfrak{P}_j \cap A$, ou seja, $\mathfrak{P}_j$ está acima de $\mathfrak{p}$. Além disso, se restringirmos ϕ_j a A, tem-se que $\phi_j|_A$ é o homomorfismo canônico de A em $\frac{A}{\mathfrak{p}}$, e assim, $\bar{\phi_j}$ é um $\frac{A}{\mathfrak{p}}$-isomorfismo de $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}_j}$ em $\left(\frac{A}{\mathfrak{p}}\right)[\widetilde{\beta}_j]$. Logo, $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}_j} = \left(\frac{A}{\mathfrak{p}}\right)[\bar{\beta}_j]$, para alguma raiz $\bar{\beta}_j \in \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}_j}$ de $\bar{p_j}$. Portanto, $f(\mathfrak{P}_j|\mathfrak{p}) = f_j$ e como $\phi_j(p_j(\beta)) = 0 \neq \phi_j(p_i(\beta))$, para $i \neq j$, segue que $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ são distintos dois a dois.

a) Tem-se que $\mathfrak{p}\mathcal{O}_{\mathbb{L}} + p_j(\beta)\mathcal{O}_{\mathbb{L}} \subseteq \mathfrak{P}_j$, para $j = 1, \ldots, r$. Seja $\alpha \in \mathfrak{P}_j$ tal que $\alpha = g(\beta)$, com $g(x) \in A[x]$. Como $\bar{g}(\widetilde{\beta}_j) = \phi_j(g(\beta)) = 0$ e $\bar{p_j}$ é o polinômio minimal de $\widetilde{\beta}_j$ sobre $\frac{A}{\mathfrak{p}}$, segue que existe $h(x) \in A[x]$ tal que $\bar{g} = \bar{p_j}\bar{h}$. Logo, $g - p_j h$ tem seus coeficientes em $\mathfrak{p}$ e $\alpha = (g - p_j h)(\beta) + p_j(\beta)h(\beta) \in \mathfrak{p}\mathcal{O}_{\mathbb{L}} + p_j(\beta)\mathcal{O}_{\mathbb{L}}$. Mostramos que $\mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r} \subseteq \mathfrak{p}\mathcal{O}_{\mathbb{L}}$. De fato, como $(\mathfrak{M} + \mathfrak{B})(\mathfrak{M} + \mathfrak{B}') \subseteq \mathfrak{M} + \mathfrak{B}\mathfrak{B}'$, para quaisquer ideais $\mathfrak{M}$, $\mathfrak{B}$, $\mathfrak{B}'$ de $\mathcal{O}_{\mathbb{L}}$, segue que $\mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r} \subseteq \mathfrak{p}\mathcal{O}_{\mathbb{L}} + \gamma\mathcal{O}_{\mathbb{L}}$, onde $\gamma = p_1(\beta)^{e_1} \ldots p_r(\beta)^{e_r}$. Como o polinômio $p_1^{e_1} \ldots p_r^{e_r} - p$ tem seus coeficientes em $\mathfrak{p}$ e $p(\beta) = 0$, segue que $\gamma = (p_1(\beta)^{e_1} \ldots p_r(\beta)^{e_r} - p)(\beta) \in \mathfrak{p}\mathcal{O}_{\mathbb{L}}$. Logo, $\mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r} \in \mathfrak{p}\mathcal{O}_{\mathbb{L}}$, ou seja, $\mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r}$ é um múltiplo de $\mathfrak{p}\mathcal{O}_{\mathbb{L}}$. Deste modo, $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ são os únicos ideais primos de $\mathcal{O}_{\mathbb{L}}$ acima de $\mathfrak{p}$ e $e(\mathfrak{P}_j|\mathfrak{p}) \leq e_j$, para $j = 1, \ldots, r$. Portanto, $\sum_{j=1}^{r} e(\mathfrak{P}_j|\mathfrak{p}) f(\mathfrak{P}_j|\mathfrak{p}) \leq \sum_{j=1}^{r} e_j gr(p_j) = gr(p_j) = n$. Da igualdade fundamental, vale a igualdade, o que prova o item (a). ■

Exemplo 2.3 *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{6})$, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{6}]$ *e* $p(x) = x^2 - 6 = min_{\mathbb{Q}}\sqrt{6}$. *Pelo*

Teorema de Kummer, tem-se:

a) 2 *é totalmente ramificado, pois* $2\mathcal{O}_{\mathbb{K}} = \mathfrak{P}_1^2$, *onde* $\mathfrak{P}_1 = 2\mathcal{O}_{\mathbb{K}} + p_1(\sqrt{6})\mathcal{O}_{\mathbb{K}}$ *e* $p_1(x) = x$;

b) 7 *é inerte, pois* $7\mathcal{O}_{\mathbb{K}} = \mathfrak{P}_1$, *onde* $\mathfrak{P}_1 = 7\mathcal{O}_{\mathbb{K}} + p_1(\sqrt{6})\mathcal{O}_{\mathbb{K}}$ *e* $p_1(x) = x^2 + 1$;

c) 5 *é totalmente decomposto, pois* $5\mathcal{O}_{\mathbb{K}} = \mathfrak{P}_1\mathfrak{P}_2$, *onde* $\mathfrak{P}_1 = 5\mathcal{O}_{\mathbb{K}} + p_1(\sqrt{6})\mathcal{O}_{\mathbb{K}}$, $\mathfrak{P}_2 = 5\mathcal{O}_{\mathbb{K}} + p_2(\sqrt{6})\mathcal{O}_{\mathbb{K}}$, $p_1(x) = x + 4$ *e* $p_2(x) = x + 1$.

Proposição 2.16 *(Multiplicidade de índice de ramificação e grau de inércia) Se* $\mathfrak{p}$ *é um ideal primo de* A, $\mathfrak{P}$ *um ideal primo de* $\mathcal{O}_{\mathbb{L}}$ *acima de* $\mathfrak{p}$, $\mathbb{K} \subseteq \mathbb{K}' \subseteq \mathbb{L}$, $\mathcal{O}_{\mathbb{K}'} = \mathcal{O}_{\mathbb{L}} \cap \mathbb{K}'$ *e* $\mathfrak{P}' = \mathfrak{P} \cap \mathcal{O}_{\mathbb{K}'}$, *então* $e(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{P}')e(\mathfrak{P}'|\mathfrak{p})$ *e* $f(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{P}')f(\mathfrak{P}'|\mathfrak{p})$.

Demonstração. Denotamos $e = e(\mathfrak{P}|\mathfrak{p})$, $e' = e(\mathfrak{P}|\mathfrak{P}')$ e $e'' = e(\mathfrak{P}'|\mathfrak{p})$. Como $(\mathfrak{P}')^{e''}$ divide $\mathfrak{p}\mathcal{O}_{\mathbb{K}'}$ e $(\mathfrak{P}')^{e''+1}$ não divide $\mathfrak{p}\mathcal{O}_{\mathbb{K}'}$, segue que podemos escrever $\mathfrak{p}\mathcal{O}_{\mathbb{K}'} = (\mathfrak{P}')^{e''}\mathfrak{M}'$, com $\mathfrak{M}'$ não divisível por $\mathfrak{P}'$. De modo análogo, podemos escrever $\mathfrak{P}'\mathcal{O}_{\mathbb{L}} = \mathfrak{P}^{e'}\mathfrak{M}$, com $\mathfrak{M}$ não divisível por $\mathfrak{P}$. Assim, $\mathfrak{p}\mathcal{O}_{\mathbb{L}} = (\mathfrak{p}\mathcal{O}_{\mathbb{K}'})\mathcal{O}_{\mathbb{L}} = ((\mathfrak{P}')^{e''}\mathfrak{M}')\mathcal{O}_{\mathbb{L}} = (\mathfrak{P}^{e'}\mathfrak{M})^{e''}\mathfrak{M}'\mathcal{O}_{\mathbb{L}} = (\mathfrak{P}^{e'e''})\mathfrak{M}^{e''}\mathfrak{M}'\mathcal{O}_{\mathbb{L}}$, com $\mathfrak{M}'\mathcal{O}_{\mathbb{L}}$ não divisível por $\mathfrak{P}$, pois caso contrário, $\mathfrak{M}'\mathcal{O}_{\mathbb{L}} \subseteq \mathfrak{P}$ o que implica que $\mathfrak{M} \subseteq \mathfrak{M}'\mathcal{O}_{\mathbb{L}} \cap \mathcal{O}_{\mathbb{K}'} \subseteq \mathfrak{P}'$, o que contraria o fato de $\mathfrak{M}$ não ser divisível por $\mathfrak{P}$. Portanto, $e = e'e''$. Agora, por definição tem-se que $f(\mathfrak{P}|\mathfrak{P}') = \left[\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}} : \dfrac{\mathcal{O}_{\mathbb{K}'}}{\mathfrak{P}'}\right]$ e $f(\mathfrak{P}'|\mathfrak{p}) = \left[\dfrac{\mathcal{O}_{\mathbb{K}'}}{\mathfrak{P}'} : \dfrac{A}{\mathfrak{p}}\right]$. Portanto, $f(\mathfrak{P}|\mathfrak{p}) = \left[\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}} : \dfrac{A}{\mathfrak{p}}\right] = f(\mathfrak{P}|\mathfrak{P}')f(\mathfrak{P}'|\mathfrak{p})$. ■

2.4.1 Ramificação e discriminante

A relação feita nesta seção entre ramificação e discriminante é de extrema importância, pois o último teorema desta seção nos mostra quais são os ideais primos que se ramificam em uma extensão, e garante que o número de ideais primos que se ramificam é finito. Pela referência [5], conhecemos o discriminante de todo corpo de número abeliano, o que facilita o estudo dos primos que se ramificam neste corpo. As principais referências desta seção são [7], [9] e [18].

Lema 2.2 *Sejam* A *um anel e* $B_1, \ldots, B_q$ *anéis contendo* A *e* A*-módulos livres finitamente gerados. Se* $B = \prod_{i=1}^{q} B_i$, *então* $\mathfrak{D}_{B|A} = \prod_{i=1}^{q} \mathfrak{D}_{B_i|A}$.

Demonstração. Provamos que para $q = 2$ a igualdade é válida e o caso geral segue por indução sobre q. Seja $B = B_1 \times B_2$, onde B_1 e B_2 são A-módulos livres finitamente gerados que contêm A. Sejam $\{x_1, \ldots, x_m\}$ e $\{y_1, \ldots, y_n\}$ bases de B_1 e B_2 respectivamente. Denotamos $z_i = (x_i, 0)$, para $i = 1, \ldots, m$ e $z_{m+j} = (0, y_j)$, para $j = 1, \ldots, n$. Logo, $\{z_1, \ldots, z_{m+n}\}$ é uma base de $B_1 \times B_2$ sobre A. Assim, $\mathfrak{D}_{B|A} = \langle D(z_1, \ldots, z_{m+n})\rangle = \langle det(Tr_{B|A}(z_i z_j))\rangle$. Notemos, que se $x \in B_1$, então $Tr_{B|A}(x, 0) = Tr_{B_1|A}(x)$ e se $y \in B_2$, então $Tr_{B|A}(0, y) = Tr_{B_2|A}(y)$. Assim, $det(Tr_{B|A}(z_i z_j)) = \begin{vmatrix} Tr_{B_1|A}(x_i x_j) & 0 \\ 0 & Tr_{B_2|A}(y_i y_j) \end{vmatrix} = det(Tr_{B_1|A}(x_i x_j))det(Tr_{B_2|A}(y_i y_j)) = D(x_1, \ldots, x_m)D(y_1, \ldots, y_n)$. Portanto, $\mathfrak{D}_{B|A} = \prod_{i=1}^{2} \mathfrak{D}_{B_i|A}$. ■

Lema 2.3 *Sejam B um anel, A um subanel de B e $\mathfrak{b}$ um ideal de A. Se B é um A-módulo livre com base $\{x_1, \ldots, x_n\}$, então escrevendo para cada $x \in B$, $\overline{x} = x + B\mathfrak{b} \in \frac{B}{B\mathfrak{b}}$, tem-se que $\{\overline{x_1}, \ldots, \overline{x_n}\}$ é uma base do $\frac{A}{\mathfrak{b}}$-módulo $\frac{B}{B\mathfrak{b}}$, e $D(\overline{x_1}, \ldots, \overline{x_n}) = \overline{D(x_1, \ldots, x_n)}$.*

Demonstração. Procedendo de forma análoga a demonstração do Teorema 2.5 podemos provar que $\{\overline{x_1}, \ldots, \overline{x_n}\}$ é uma base do $\frac{A}{\mathfrak{b}}$-módulo $\frac{B}{B\mathfrak{b}}$. Agora, consideramos $\varphi_{\overline{x}} : \frac{B}{B\mathfrak{b}} \longrightarrow \frac{B}{B\mathfrak{b}}$ dada por $\varphi_{\overline{x}}(\overline{y}) = \overline{xy}$ e a matriz $\varphi_{\overline{x}} = (\overline{a_{ij}})$, onde $(a_{ij}) = \varphi_x$. Assim, $Tr_{\frac{B}{B\mathfrak{b}}|\frac{A}{\mathfrak{b}}}(\overline{x}) = \overline{Tr_{B|A}(x)}$. Logo, $Tr_{\frac{B}{B\mathfrak{b}}|\frac{A}{\mathfrak{b}}}(\overline{x_i x_j}) = \overline{Tr_{B|A}(x_i x_j)}$. Pelo Lema 2.2, segue que $D(\overline{x_1}, \ldots, \overline{x_n}) = det(Tr_{\frac{B}{B\mathfrak{b}}|\frac{A}{\mathfrak{b}}}(\overline{x_i x_j})) = det(\overline{Tr_{B|A}(x_i x_j)}) = \overline{D(x_1, \ldots, x_n)}$. ■

Definição 2.10 *Seja A um anel. Dizemos que $a \in A$ é nilpotente se existe $n \in \mathbb{N}$ tal que $a^n = 0$. Dizemos que A é um anel reduzido se o único elemento nilpotente é o zero.*

Lema 2.4 *Se A é um anel Noetheriano e reduzido, então o ideal nulo é expresso como uma interseção finita de ideais primos.*

Demonstração. Como A é um anel Noetheriano, segue, pela Proposição 1.2, que $\langle 0\rangle = \prod_{i=1}^{q} \mathfrak{p}_i^{e_i}$, onde $\mathfrak{p}_i$'s são ideais primos, para $i = 1, 2, \ldots, q$. Tem-se que $\langle 0\rangle \subset \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_q$.

Agora, se $x \in \bigcap_{i=1}^{q} \mathfrak{p}_i$, então $x \in \mathfrak{p}_i$, para todo $1 \leq i \leq q$, e assim, $x^{e_1+\ldots+e_q} \in \prod_{i=1}^{q} \mathfrak{p}_i^{e_i} = \langle 0 \rangle$. Logo, $x^{e_1+\ldots+e_q} = 0$ e como A é reduzido, segue que $x = 0$. Portanto, $\langle 0 \rangle = \bigcap_{i=1}^{q} \mathfrak{p}_i$. ■

Definição 2.11 *Sejam A e B anéis e $\varphi : A \longrightarrow B$ um homomorfismo. Chamamos o par (B, φ) de uma A-álgebra. No caso, em que A é um corpo, tem-se que φ é injetiva.*

Lema 2.5 *Seja $\mathbb{K}$ um corpo finito ou de característica zero. Se $\mathbb{L}$ é uma $\mathbb{K}$-álgebra comutativa de dimensão finita, então $\mathbb{L}$ é reduzido se, e somente se, $\mathfrak{D}_{\mathbb{L}|\mathbb{K}} \neq \langle 0 \rangle$.*

Demonstração. Suponhamos que $\mathbb{L}$ não seja reduzido, ou seja, existe um $x \in \mathbb{L}$ não nulo tal que $x^m = 0$, para algum $m > 0$. Como $\mathbb{L}$ é uma $\mathbb{K}$-álgebra de dimensão finita, segue que existe uma base $\{x_1, \ldots, x_n\}$ de $\mathbb{L}$ sobre $\mathbb{K}$ e podemos supor $x = x_1$. Assim, $(x_1 x_j)^m = x_1^m x_j^m = 0$, para $j = 1, \ldots, n$. Consideramos $\varphi_{x_1 x_j} : \mathbb{L} \longrightarrow \mathbb{L}$ dada por $\varphi_{x_1 x_j}(y) = x_1 x_j y$. Tem-se que $\varphi_{x_1 x_j}(y)$ é nilpotente, para todo $y \in \mathbb{L}$. Logo, o polinômio minimal de $\varphi_{x_1 x_j}$ é t^m, e deste modo, zero é o único autovalor de $\varphi_{x_1 x_j}$. Assim, $Tr_{\mathbb{L}|\mathbb{K}}(x_1 x_j) = 0$. Portanto, $D(x_1, \ldots, x_n) = det(Tr_{\mathbb{L}|\mathbb{K}}(x_i x_j)) = 0$, pois a matriz $(Tr_{\mathbb{L}|\mathbb{K}}(x_i x_j))$ tem a primeira linha nula. Por outro lado, observamos que $\mathbb{L}$ é um $\mathbb{K}$-módulo finitamente gerado com $\mathbb{K}$ um anel Noetheriano ($\mathbb{K}$ é corpo), o que pelo Corolário 2.1, torna $\mathbb{L}$ um anel Noetheriano. Assim, supondo $\mathbb{L}$ reduzido tem-se que $\langle 0 \rangle = \bigcap_{i=1}^{q} \mathfrak{p}_i$. Como $\mathbb{L}$ é uma $\mathbb{K}$-álgebra de dimensão finita, segue que $\mathbb{L}$ contém um corpo isomorfo a $\mathbb{K}$ e $\mathbb{L}$ é inteiro sobre $\mathbb{K}$. Assim, o fato de $\frac{\mathbb{L}}{\mathfrak{p}_i}$ ser um domínio de integridade e $\mathbb{K} \subset \frac{\mathbb{L}}{\mathfrak{p}_i}$, implica pela Proposição 1.5, que $\frac{\mathbb{L}}{\mathfrak{p}_i}$ é um corpo. Portanto, $\mathfrak{p}_i$ é um ideal maximal de $\mathbb{L}$, para $1 \leq i \leq q$. Para $i \neq j$, tem-se que $\mathfrak{p}_i \neq \mathfrak{p}_j$, logo $\mathfrak{p}_i + \mathfrak{p}_j = \mathbb{L}$. Assim, $\frac{\mathbb{L}}{\bigcap_{i=1}^{q} \mathfrak{p}_i} \simeq \prod_{i=1}^{q} \frac{\mathbb{L}}{\mathfrak{p}_i}$, ou seja, $\mathbb{L} \simeq \prod_{i=1}^{q} \frac{\mathbb{L}}{\mathfrak{p}_i}$. Segue, pelo Lema 2.2, que $\mathfrak{D}_{\mathbb{L}|\mathbb{K}} = \prod_{i=1}^{q} \mathfrak{D}_{\frac{\mathbb{L}}{\mathfrak{p}_i}|\mathbb{K}}$. Pelo fato de $\mathbb{K}$ ser finito ou de característica zero e $\mathbb{K} \subset \frac{\mathbb{L}}{\mathfrak{p}_i}$ ser uma extensão de dimensão finita, segue que $\mathfrak{D}_{\frac{\mathbb{L}}{\mathfrak{p}_i}|\mathbb{K}} \neq \langle 0 \rangle$. Portanto, $\mathfrak{D}_{\mathbb{L}|\mathbb{K}} \neq \langle 0 \rangle$. ■

Consideramos até o fim desta seção $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{L}$ extensões de corpos, $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros algébricos de $\mathbb{K}$ e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros algébricos de $\mathbb{L}$.

Definição 2.12 *Chamamos de discriminante de $\mathcal{O}_{\mathbb{L}}$ sobre $\mathcal{O}_{\mathbb{K}}$ o ideal gerado pelo discriminante de uma base de $\mathbb{L}$ sobre $\mathbb{K}$ contida em $\mathcal{O}_{\mathbb{L}}$ e denotamos por $\mathfrak{D}_{\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}}}$.*

Teorema 2.7 *Se $\mathfrak{p}$ é um ideal primo de $\mathcal{O}_{\mathbb{K}}$, então $\mathfrak{p}$ se ramifica em $\mathcal{O}_{\mathbb{L}}$ se, e somente se, $\mathfrak{p}$ contém $\mathfrak{D}_{\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}}}$. Além disso, o conjunto dos ideais primos de A que se ramificam em $\mathcal{O}_{\mathbb{L}}$ é finito.*

Demonstração. Suponhamos que $\mathfrak{p}$ se ramifica em $\mathcal{O}_{\mathbb{L}}$ e consideramos $S = \mathcal{O}_{\mathbb{K}} - \mathfrak{p}$. Denotamos $\mathcal{O}'_{\mathbb{K}} = S^{-1}\mathcal{O}_{\mathbb{K}}$, $\mathcal{O}'_{\mathbb{L}} = S^{-1}\mathcal{O}_{\mathbb{L}}$ e $\mathfrak{p}' = \mathfrak{p}\mathcal{O}_{\mathbb{K}}{}'$. Pela Proposição 2.10, segue que $\mathcal{O}'_{\mathbb{K}}$ é um anel principal, e assim, $\mathcal{O}'_{\mathbb{L}}$ é um $\mathcal{O}'_{\mathbb{K}}$-módulo livre e $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}} \simeq \dfrac{\mathcal{O}'_{\mathbb{K}}}{\mathfrak{p}'}$ e $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}\mathcal{O}_{\mathbb{L}}} \simeq \dfrac{\mathcal{O}'_{\mathbb{L}}}{\mathfrak{p}'\mathcal{O}'_{\mathbb{L}}}$. Seja $\{e_1, \ldots, e_n\}$ uma base de $\mathcal{O}'_{\mathbb{L}}$ sobre $\mathcal{O}'_{\mathbb{K}}$. Como $\mathfrak{p}$ se ramifica em $\mathcal{O}_{\mathbb{L}}$, segue que $\mathfrak{D}_{\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}\mathcal{O}_{\mathbb{L}}}|\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}}} = \langle 0\rangle$ (Lema 2.5). Assim, $\bar{0} = \overline{D(e_1, \ldots, e_n)} \in \dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}} \simeq \dfrac{\mathcal{O}'_{\mathbb{K}}}{\mathfrak{p}'}$, o que implica que $D(e_1, \ldots, e_n) \in \mathfrak{p}'$. Agora, consideramos $\{x_1, \ldots, x_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$ contida em $\mathcal{O}_{\mathbb{L}}$. Assim, $x_i = \displaystyle\sum_{j=1}^{n} a_{ij}e_j$, com $a_{ij} \in \mathcal{O}'_{\mathbb{K}}$ e $i = 1, \ldots, n$. Logo, $D(x_1, \ldots, x_n) \in \mathcal{O}_{\mathbb{K}}$ e $D(x_1, \ldots, x_n) = det(a_{ij})^2 D(e_1, \ldots, e_n) \in \mathcal{O}'_{\mathbb{K}}\mathfrak{p}' \subset \mathfrak{p}'$. Assim, $D(x_1, \ldots, x_n) \in \mathcal{O}_{\mathbb{K}} \cap \mathfrak{p}' = \mathfrak{p}$. Portanto, $\mathfrak{D}_{\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}}} \subset \mathfrak{p}$. Por outro lado, se $\mathfrak{D}_{\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{K}}} \subset \mathfrak{p}$ e $\{e_1, \ldots, e_n\}$ é uma base de $\mathcal{O}'_{\mathbb{L}}$ sobre $\mathcal{O}'_{\mathbb{K}}$, então $e_i = \dfrac{y_i}{s}$, com $y_i \in \mathcal{O}_{\mathbb{L}}$, $s \in S$ e $i = 1, \ldots, n$. Assim,

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

Logo, $\overline{D(e_1, \ldots, e_n)} = \bar{0}$ em $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}'}$, e portanto, $\mathfrak{D}_{\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{p}\mathcal{O}_{\mathbb{L}}}|\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}}} = \langle 0\rangle$, o que implica, que $\mathfrak{p}$ se ramifica. ■

Exemplo 2.4 *Se $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com $d \in \mathbb{Z}$ livre de quadrados, então, pelo Teorema 1.16, segue que o discriminante*

$$D_{\mathbb{K}} = \begin{cases} 4d, & \text{se } d \equiv 2 \text{ ou } 3 (mod\ 4) \\ d, & \text{se } d \equiv 1 (mod\ 4) \end{cases}.$$

Assim, um ideal primo $\mathfrak{p} = p\mathbb{Z}$ de $\mathbb{Z}$ se ramifica em $\mathcal{O}_{\mathbb{K}}$ se, e somente se, $p|2$ ou $p|d$ no caso em que $D_{\mathbb{K}} = 4d$ e $p|d$ no caso em que $D_{\mathbb{K}} = d$.

Exemplo 2.5 *Se $\mathbb{K} = \mathbb{Q}(\zeta_p)$, onde ζ_p é uma raiz p-ésima primitiva da unidade, com p é um primo ímpar, então, pelo Teorema 1.18, tem-se que o discriminante $D_{\mathbb{K}} = (-1)^{\frac{p-1}{2}} p^{p-2}$. Assim, um ideal primo $\mathfrak{q} = q\mathbb{Z}$ de $\mathbb{Z}$ se ramifica em $\mathcal{O}_{\mathbb{K}}$ se, e somente se, $q|p$. Mas isso acontece apenas quando $q = p$. No caso de $\mathbb{K} = \mathbb{Q}(\zeta_n)$, tem-se que p se ramifica se, e somente se, $p|n$.*

Proposição 2.17 *Se $\mathbb{K}$ é uma extensão de $\mathbb{Q}$ tal que $\mathbb{K} \neq \mathbb{Q}$ e $\mathfrak{b}$ um ideal não nulo de $\mathcal{O}_{\mathbb{L}}$, então existe $b \in \mathfrak{b}$ não nulo tal que*

$$|N_{\mathbb{K}|\mathbb{Q}}(b)| < N(\mathfrak{b})\sqrt{|D_{\mathbb{K}}|},$$

onde $D_{\mathbb{K}}$ é o discrimante de uma base de $\mathbb{K}$ sobre $\mathbb{Q}$ contida em $\mathcal{O}_{\mathbb{L}}$.

Demonstração. [9], pág. 158.

Lema 2.6 *(Minkowski) Se $\mathbb{K}$ é uma extensão de $\mathbb{Q}$ tal que $\mathbb{K} \neq \mathbb{Q}$, então $|D_{\mathbb{K}}| \geq 2$.*

Demonstração. Se $\mathfrak{b} = \langle 1 \rangle$ é um ideal de $\mathcal{O}_{\mathbb{K}}$, então pela Proposição 2.17 tem-se que

$$1 \leq |N_{\mathbb{K}|\mathbb{Q}}(b) < N(\mathfrak{b})\sqrt{|D_{\mathbb{K}}|} = \sqrt{|D_{\mathbb{K}}|}.$$

Portanto, $|D_{\mathbb{K}}| \geq 2$. ■

2.4.2 Grupos de decomposição, inércia e ramificação

Os grupos de decomposição, inércia e ramificação são de fundamental importância na teoria da ramificação. Estes grupos tem características especiais que veremos neste seção. A demonstração do Teorema de Kronecker-Weber é feita observando tais características. A principal referência desta seção é [12].

Consideramos, nesta seção, A um domínio de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão de Galois de $\mathbb{K}$, com grupo de Galois G e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de $\mathbb{L}$ sobre A.

Proposição 2.18 *Sejam $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ ideais primos e $\mathfrak{b}$ um ideal arbitrário de A. Se $\mathfrak{b} \subseteq \mathfrak{p}_1 \cup \mathfrak{p}_2 \cup \ldots \cup \mathfrak{p}_r$, então $\mathfrak{b} \subseteq \mathfrak{p}_j$, para algum $j = 1, \ldots, r$.*

Demonstração. Como $\mathcal{O}_{\mathbb{L}}$ é um domínio de Dedekind, segue que $\mathfrak{p}_i \nsubseteq \mathfrak{p}_j$, para todo $i \neq j$, com $i, j = 1, \ldots, r$, pois $\mathfrak{p}_i$ é maximal. Seja $c_{j,i} \in \mathfrak{p}_i - \mathfrak{p}_j$. Suponhamos que $\mathfrak{b} \nsubseteq \mathfrak{p}_j$, para todo $j = 1, \ldots, r$. Assim, existe $b_j \in \mathfrak{b} - \mathfrak{p}_j$, para $j = 1, \ldots, r$. Consideramos $a_j = c_{j,1} \cdot \ldots \cdot c_{j,j-1} \cdot b_j \cdot c_{j,j+1} \cdot c_{j,r} \in (\mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_{j-1} \cap \mathfrak{b} \cap \mathfrak{p}_{j+1} \cap \mathfrak{p}_r) - \mathfrak{p}_j$. Logo, $\sum_{j=1}^{r} a_j \in \mathfrak{b} - (\mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_r)$, ou seja, $\mathfrak{b} \nsubseteq \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_r$. Portanto, $\mathfrak{b} \subseteq \mathfrak{p}_j$, para algum $j = 1, \ldots, r$. ■

Teorema 2.8 *Sejam $\mathfrak{p}$ um ideal primo não nulo de A e $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ os ideais primos de $\mathcal{O}_{\mathbb{L}}$ que estão acima de $\mathfrak{p}$.*

a) $\sigma(\mathcal{O}_{\mathbb{L}}) = \mathcal{O}_{\mathbb{L}}$, para qualquer $\sigma \in G$;

b) Todo $\sigma \in G$ induz um $\frac{A}{\mathfrak{p}}$-isomorfismo de $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}_j}$ sobre $\frac{\mathcal{O}_{\mathbb{L}}}{\sigma(\mathfrak{P}_j)}$, para $j = 1, \ldots, g$;

c) $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ são dois a dois conjugados;

d) $e = e(\mathfrak{P}_1|\mathfrak{p}) = \ldots = e(\mathfrak{P}_g|\mathfrak{p})$ e $f = f(\mathfrak{P}_1|\mathfrak{p}) = \ldots = f(\mathfrak{P}_g|\mathfrak{p})$.

Demonstração. a) Se $\alpha \in \mathcal{O}_{\mathbb{L}}$, então existe um polinômio mônico $f(x) \in A[x]$ tal que $f(\alpha) = 0$. Assim, para qualquer $\sigma \in G$, segue que $f(\sigma(\alpha)) = 0$. Portanto, $\sigma(\mathcal{O}_{\mathbb{L}}) \subseteq \mathcal{O}_{\mathbb{L}}$. Analogamente, tem-se que $\sigma^{-1}(\mathcal{O}_{\mathbb{L}}) \subseteq \mathcal{O}_{\mathbb{L}}$. Como $\mathcal{O}_{\mathbb{L}} = \sigma\sigma^{-1}(\mathcal{O}_{\mathbb{L}})$, segue que $\mathcal{O}_{\mathbb{L}} \subseteq \sigma(\mathcal{O}_{\mathbb{L}})$. Portanto, $\sigma(\mathcal{O}_{\mathbb{L}}) = \mathcal{O}_{\mathbb{L}}$.

b) Consideramos $\sigma|_{\mathcal{O}_{\mathbb{L}}}$, a restrição de $\sigma \in G$ a $\mathcal{O}_{\mathbb{L}}$, e $\varphi_j : \mathcal{O}_{\mathbb{L}} \longrightarrow \frac{\mathcal{O}_{\mathbb{L}}}{\sigma(\mathfrak{P}_j)}$ dada por $\varphi_j(\alpha) = \alpha + \sigma(\mathfrak{P}_j)$, para $j = 1, \ldots, g$. O homomorfismo composição

$$\begin{aligned} \varphi_j \circ \sigma|_{\mathcal{O}_{\mathbb{L}}} : \mathcal{O}_{\mathbb{L}} &\longrightarrow \frac{\mathcal{O}_{\mathbb{L}}}{\sigma(\mathfrak{P}_j)} \\ \alpha &\longmapsto \sigma(\alpha + \mathfrak{P}_j), \end{aligned}$$

é sobrejetor e tem núcleo $\mathfrak{P}_j$. Portanto, $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}_j} \simeq \frac{\mathcal{O}_{\mathbb{L}}}{\sigma(\mathfrak{P}_j)}$ como $\frac{A}{\mathfrak{p}}$-espaços vetoriais.

c) Mostramos que $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_g\} = \{\sigma(\mathfrak{P}_1); \sigma \in G\}$. De fato, para todo $\sigma \in G$, tem-se que $\sigma(\mathfrak{P}_1) \cap A = \sigma(\mathfrak{P}_1 \cap A) = \mathfrak{p}$. Portanto, $\sigma(\mathfrak{P}_1) \in \{\mathfrak{P}_1, \ldots, \mathfrak{P}_g\}$. Agora, suponhamos que $\mathfrak{P}_j \notin \{\sigma(\mathfrak{P}_1); \sigma \in G\}$, para algum $j = 1, \ldots, g$. Como $\mathfrak{P}_j$ é um ideal maximal de $\mathcal{O}_{\mathbb{L}}$, segue que $\mathfrak{P}_j \nsubseteq \sigma(\mathfrak{P}_1)$, para todo $\sigma \in G$. Pela Proposição 2.18, segue que $\mathfrak{P}_j \nsubseteq \bigcup_{\sigma \in G} \sigma(\mathfrak{P}_1)$.

Seja $\alpha \in \mathfrak{P}_j - \bigcup_{\sigma\in G} \sigma(\mathfrak{P}_1)$. De (a), tem-se que $\sigma(\alpha) \in \mathcal{O}_{\mathbb{L}}$, para todo $\sigma \in G$. Assim, $\prod_{\sigma\in G} \sigma(\alpha) = N_{\mathbb{L}|\mathbb{K}}(\alpha) \in \mathfrak{P}_j$, e consequentemente, $\prod_{\sigma\in G} \sigma(\alpha) \in \mathfrak{P}_j \cap A = \mathfrak{p} \subseteq \mathfrak{P}_1$. Pelo fato de $\mathfrak{P}_1$ ser primo, segue que $\sigma(\alpha) \in \mathfrak{P}_1$, para algum $\sigma \in G$. Assim, $\alpha \in \sigma^{-1}(\mathfrak{P}_1)$ o que contradiz o fato de $\alpha \in \mathfrak{P}_j - \bigcup_{\sigma\in G} \sigma(\mathfrak{P}_1)$.

d) Tem-se que $(\sigma(\mathfrak{P}_1))^k$ divide $\mathfrak{p}\mathcal{O}_{\mathbb{L}}$ se, e somente se, $\mathfrak{P}_1^k$ divide $\mathfrak{p}\mathcal{O}_{\mathbb{L}}$, para $\sigma \in G$ e $k \in \mathbb{N}$. Assim, $e(\sigma\mathfrak{P}_1|\mathfrak{p}) = e(\mathfrak{P}_1|\mathfrak{p})$. De (b) tem-se que $f(\sigma(\mathfrak{P}_1)|\mathfrak{p}) = f(\mathfrak{P}_1|\mathfrak{p})$. Portanto, por (c), segue que $e(\mathfrak{P}_1|\mathfrak{p}) = \ldots = e(\mathfrak{P}_g|\mathfrak{p}) = e$ e $f(\mathfrak{P}_1|\mathfrak{p}) = \ldots = f(\mathfrak{P}_g|\mathfrak{p}) = f$. ■

Corolário 2.1 *Com hipóteses do Teorema 2.8, tem-se que $efg = n$, onde n é o grau da extensão $\mathbb{L}$ de $\mathbb{K}$.* ■

Observação 2.2 *Como em uma extensão de Galois todos os índices de ramificação e graus de inércia são iguais para todos os ideais $\mathfrak{P}_j$'s acima de $\mathfrak{p}$, segue que basta estudarmos o índice de ramificação e grau de inércia de um único ideal $\mathfrak{P}$ acima de $\mathfrak{p}$.*

Teorema 2.9 *Se ζ_{p^r} é uma raíz p^r-ésima primitiva da unidade, com p primo e $r \in \mathbb{N}$, e $\mathfrak{P}$ é um ideal primo de $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$ acima de $p\mathbb{Z} = \mathfrak{p}$, então*

a) $(1-\zeta_{p^r})^{\varphi(p^r)}\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = p\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$;

b) $e(\mathfrak{P}|\mathfrak{p}) = \varphi(p^r)$, *ou seja,* $\mathfrak{p}$ *se ramifica totalmente em* $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$.

Demonstração. a) Para $r = 1$, tem-se, pelo Lema 1.7 item f, que $(1-\zeta_p)$ é um ideal de $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ acima de $p\mathbb{Z}$. Assim, pelo Teorema 1.8 item c, os conjugados de $(1-\zeta_p)$ também estão acima de $p\mathbb{Z}$. Como os conjugados de $(1-\zeta_p)$ são todos da forma $(1-\zeta_p^i) = (1-\zeta_p)(1+\zeta_p+\ldots+\zeta_p^{i-1})$, segue que $p\mathcal{O}_{\mathbb{Q}(\zeta_p)} = (1-\zeta_p)^{\varphi(p)}\mathcal{O}_{\mathbb{Q}(\zeta_p)}$. Assim, pela Observação 1.5, tem-se que $(1-\zeta_{p^r})^{\varphi(p^r)}\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = p\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$.

b) Segue do item (a). ■

Proposição 2.19 *Se $\mathfrak{p}$ é ideal primo não nulo de A e $\mathfrak{P}$ um ideal primo de $\mathcal{O}_{\mathbb{L}}$ acima de $\mathfrak{p}$, então $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}|\frac{A}{\mathfrak{p}}$ é uma extensão normal.*

Demonstração. Consideramos $\psi : A \longrightarrow \frac{A}{\mathfrak{p}}$ dada por $\psi(a) = a + \mathfrak{p}$ e $\varphi : \mathcal{O}_{\mathbb{L}} \longrightarrow \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}$ dada por $\varphi(\alpha) = \alpha + \mathfrak{P}$. Sejam $\alpha \in \mathcal{O}_{\mathbb{L}}$ e $p(x) = min_{\mathbb{K}}\alpha = \prod_{\sigma \in G}(x - \sigma(\alpha)) \in A[x]$. Tem-se que $\varphi(\alpha)$ é uma raiz de $\psi(p(x)) \in \frac{A}{\mathfrak{p}}[x]$, o qual se fatora em $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}$, pois $\psi(p(x))$ é um múltiplo de polinômio mininal de $\varphi(\alpha)$ sobre $\frac{A}{\mathfrak{p}}$. Portanto, $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}|\frac{A}{\mathfrak{p}}$ é uma extensão normal. ■

A extensão $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}|\frac{A}{\mathfrak{p}}$ será separável se $\frac{A}{\mathfrak{p}}$ for um corpo perfeito, ou seja, se $\frac{A}{\mathfrak{p}}$ tiver característica zero ou p primo e todo elemento de $\frac{A}{\mathfrak{p}}$ for uma potência p-ésima em $\frac{A}{\mathfrak{p}}$.

Definição 2.13 *Sejam $\mathfrak{p}$ um ideal primo não nulo de A e $\mathfrak{P}$ um ideal primo de $\mathcal{O}_{\mathbb{L}}$ acima de $\mathfrak{p}$.*

a) $Z(\mathfrak{P}|\mathfrak{p}) = Z = \{\sigma \in G; \sigma(\mathfrak{P}) = \mathfrak{P}\}$ é chamado de grupo de decomposição de $\mathfrak{P}$;

b) $T(\mathfrak{P}|\mathfrak{p}) = T = \{\sigma \in Z; \sigma(\alpha) \equiv \alpha (mod\ \mathfrak{P}),$ para todo $\alpha \in \mathcal{O}_{\mathbb{L}}\}$ é chamado de grupo de inércia de $\mathfrak{P}$;

c) $V_j(\mathfrak{P}|\mathfrak{p}) = V_j = \{\sigma \in Z; \sigma(\alpha) \equiv \alpha (mod\ \mathfrak{P}^{j+1}),$ para todo $\alpha \in \mathcal{O}_{\mathbb{L}}$, $j \in \mathbb{N}\}$ é chamado de j-ésimo grupo de ramificação de $\mathfrak{P}$.

Observação 2.3 *O grupo Z é um subgrupo G e os V_j's são subgrupos de Z e consequentemente de G.*

Proposição 2.20 *Com as notações da Definição 2.13, tem-se que*

a) Os grupos de decomposições de ideais primos de $\mathcal{O}_{\mathbb{L}}$ acima de $\mathfrak{p}$ são dois a dois conjugados e os grupos de inércia de ideais primos de $\mathcal{O}_{\mathbb{L}}$ acima de $\mathfrak{p}$ são também dois a dois conjugados;

b) $|Z| = ef$;

c) V_j's são subgrupos normais de Z.

Demonstração. a) Primeiramente provamos que $Z(\sigma(\mathfrak{P})|\mathfrak{p}) = \sigma \circ Z \circ \sigma^{-1}$, para todo $\sigma \in G$. Assim, se $\sigma \in G$ e $\theta \in Z$, então $\sigma \circ \theta \circ \sigma^{-1}(\sigma(\mathfrak{P})) = \sigma \circ \theta(\mathfrak{P}) = \sigma(\mathfrak{P})$. Logo,

$\sigma \circ Z \circ \sigma^{-1} \in Z(\sigma(\mathfrak{P})|\mathfrak{p})$. Por outro lado, se $\rho \in Z(\sigma(\mathfrak{P})|\mathfrak{p})$, então $\sigma^{-1} \circ \rho \circ \sigma(\mathfrak{P}) = \sigma^{-1}(\sigma(\mathfrak{P})) = \mathfrak{P}$. Logo, $\sigma^{-1} \circ Z(\sigma(\mathfrak{P})|\mathfrak{p}) \circ \sigma \in Z$. Portanto, $Z(\sigma(\mathfrak{P})|\mathfrak{p}) = \sigma \circ Z \circ \sigma^{-1}$, para qualquer $\sigma \in G$. Agora, provamos que $T(\sigma(\mathfrak{P})|\mathfrak{p}) = \sigma \circ T \circ \sigma^{-1}$, para qualquer $\sigma \in G$. De fato, se $\sigma \in G$, $\theta \in T$ e $\alpha \in \mathcal{O}_{\mathbb{L}}$, então $(\sigma \circ \theta \circ \sigma^{-1})(\sigma(\alpha)) - \sigma(\alpha) = \sigma(\theta(\alpha) - \alpha) \in \sigma(\mathfrak{P})$. Portanto, $\sigma \circ \theta \circ \sigma^{-1}(\sigma(\alpha)) \equiv \sigma(\alpha)$ $(mod\ \sigma(\mathfrak{P}))$, ou seja, $\sigma \circ T \circ \sigma^{-1} \in T(\sigma(\mathfrak{P})|\mathfrak{p})$. Por outro lado, se $\rho \in T(\sigma(\mathfrak{P})|\mathfrak{p})$, então $\sigma^{-1} \circ \rho \circ \sigma(\alpha) - \alpha = \sigma^{-1} \circ \rho \circ \sigma(\alpha) - \sigma^{-1} \circ \sigma(\alpha) = \sigma^{-1}(\rho(\sigma(\alpha)) - \sigma(\alpha)) \in \sigma^{-1}\sigma(\mathfrak{P}) = \mathfrak{P}$. Portanto, $\sigma^{-1} \circ \rho \circ \sigma(\alpha) \equiv \alpha$ $(mod\ \mathfrak{P})$, ou seja, $\sigma^{-1} \circ T(\sigma(\mathfrak{P})|\mathfrak{p}) \circ \sigma \in T$.

b) Consideramos a aplicação sobrejetiva $\phi : G \longrightarrow \{\sigma(\mathfrak{P}); \sigma \in G\}$ dada por $\phi(\sigma) = \sigma(\mathfrak{P})$. Notemos que $Ker(\phi) = Z$, e assim, $(G : Z) = g$ e pelo Corolário 2.1, segue que $|Z| = ef$.

c) Observamos que para qualquer $\sigma \in Z$, tem-se que $\sigma(\mathfrak{P}^{i+1}) = \mathfrak{P}^{i+1}$. Agora, consideramos o homomorfismo

$$\begin{aligned} \overline{\sigma_i} : \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}^{i+1}} &\longrightarrow \mathcal{O}_{\mathbb{L}} \longrightarrow \mathcal{O}_{\mathbb{L}} \longrightarrow \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}^{i+1}} \\ \alpha + \mathfrak{P}^{i+1} &\longmapsto \alpha \longmapsto \sigma(\alpha) \longmapsto \sigma(\alpha) + \mathfrak{P}^{i+1} \end{aligned}$$

o qual tem núcleo V_j, para $j \in \mathbb{N}$. Portanto, os V_j's são subgrupos normais de Z. ■

Proposição 2.21 *Sejam $\mathbb{K} \subseteq \mathbb{K}' \subseteq \mathbb{L}$, $\mathcal{O}_{\mathbb{K}'} = \mathcal{O}_{\mathbb{L}} \cap \mathbb{K}'$ e $\mathfrak{P}' = \mathfrak{P} \cap \mathcal{O}_{\mathbb{K}'}$.*

a) $Z(\mathfrak{P}|\mathfrak{P}') = Z \cap Gal(\mathbb{L}|\mathbb{K}')$. *Além disso, se $\mathbb{K}'|\mathbb{K}$ é uma extensão de Galois, então* $Z(\mathfrak{P}'|\mathfrak{p}) \simeq \dfrac{Z}{Z(\mathfrak{P}|\mathfrak{P}')}$;

b) $T(\mathfrak{P}|\mathfrak{P}') = T \cap Gal(\mathbb{L}|\mathbb{K}')$. *Além disso, se $\mathbb{K}'|\mathbb{K}$ é uma extensão de Galois, então* $T(\mathfrak{P}'|\mathfrak{p}) \simeq \dfrac{T}{T(\mathfrak{P}|\mathfrak{P}')}$;

c) $V_j(\mathfrak{P}|\mathfrak{P}') = V_j \cap Gal(\mathbb{L}|\mathbb{K}')$.

Demonstração. a) Se $\sigma \in Z(\mathfrak{P}|\mathfrak{P}')$, então $\sigma \in Gal(\mathbb{L}|\mathbb{K}')$ e $\sigma(\mathfrak{P}) = \mathfrak{P}$. Logo, se σ fixa $\mathbb{K}'$, então σ fixa $\mathbb{K}$, ou seja, $\sigma \in Gal(\mathbb{L}|\mathbb{K})$, e assim, $Z(\mathfrak{P}|\mathfrak{P}') \subseteq Z \cap Gal(\mathbb{L}|\mathbb{K}')$. Por outro lado, se $\sigma \in Z \cap Gal(\mathbb{L}|\mathbb{K}')$, então $\sigma \in Gal(\mathbb{L}|\mathbb{K}')$ e $\sigma(\mathfrak{P}) = \mathfrak{P}$, e assim, $Z \cap Gal(\mathbb{L}|\mathbb{K}') \subseteq Z(\mathfrak{P}|\mathfrak{P}')$. Portanto, $Z(\mathfrak{P}|\mathfrak{P}') = Z \cap Gal(\mathbb{L}|\mathbb{K}')$. Além disso, se $\mathbb{K}'|\mathbb{K}$ é

um extensão de Galois, então, considerando o homomorfismo canônico $\varphi : Gal(\mathbb{L}|\mathbb{K}) \longrightarrow Gal(\mathbb{K}'|\mathbb{K})$, dado por $\varphi(\sigma) = \sigma|_{\mathbb{K}'}$, o qual tem núcleo $Gal(\mathbb{L}|\mathbb{K}')$, tem-se que $\sigma|_Z : Z \longrightarrow Z(\mathfrak{P}'|\mathfrak{p})$ é um homomorfismo sobrejetivo, com núcleo $Z(\mathfrak{P}|\mathfrak{P}')$. Pois, se $\sigma \in Z$, então $\sigma|_{\mathbb{K}'}(\mathfrak{P}') = \sigma|_{\mathbb{K}'}(\mathfrak{P} \cap \mathcal{O}_{\mathbb{K}'}) = \sigma(\mathfrak{P}') \cap \mathcal{O}_{\mathbb{K}'} = \mathfrak{P}'$, ou seja, $\varphi|_Z(\sigma) \in Z(\mathfrak{P}'|\mathfrak{p})$. Por outro lado, se $\sigma \in Z(\mathfrak{p}'|\mathfrak{p})$, então estendendo σ a $\mathbb{L}$, tem-se que $\sigma(\mathfrak{P}) = \sigma(\mathfrak{P}' \cap \mathcal{O}_{\mathbb{K}'}) = \sigma(\mathfrak{P}') = \sigma(\mathfrak{P})$, ou seja, $\sigma \in Z$. Por fim, $\sigma \in Ker(\varphi|_Z) = \{\sigma \in Gal(\mathbb{L}|\mathbb{K}); \sigma|_{\mathbb{K}'} = id \text{ e } \sigma(\mathfrak{P}) = \mathfrak{P}\}$ se, e somente se, $\sigma \in Z(\mathfrak{P}|\mathfrak{P}')$. Portanto, $Z(\mathfrak{P}'|\mathfrak{p}) \simeq \dfrac{Z}{Z(\mathfrak{P}|\mathfrak{P}')}$.

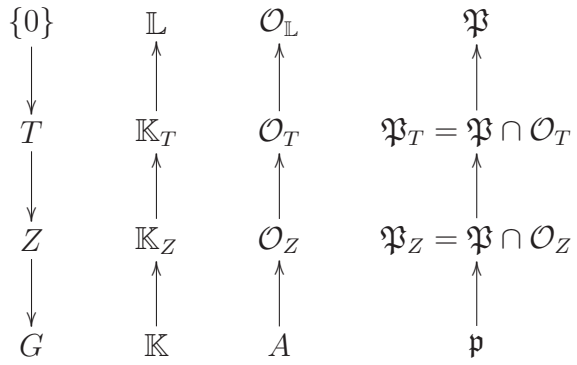
b) Se $\sigma \in T(\mathfrak{P}|\mathfrak{P}')$, então $\sigma \in Gal(\mathbb{L}|\mathbb{K}')$ e $\sigma(\alpha) \equiv \alpha (mod\ \mathfrak{P})$, para todo $\alpha \in \mathcal{O}_{\mathbb{L}}$. Como σ fixa $\mathbb{K}'$, segue que σ fixa $\mathbb{K}$, e assim, $T(\mathfrak{P}|\mathfrak{P}') \subseteq T \cap Gal(\mathbb{L}|\mathbb{K}')$. Por outro lado, se $\sigma \in T \cap Gal(\mathbb{L}|\mathbb{K}')$, então $\sigma \in Gal(\mathbb{L}|\mathbb{K}')$ e $\sigma(\alpha) \equiv \alpha (mod\ \mathfrak{P})$, para todo $\alpha \in \mathcal{O}_{\mathbb{L}}$, e assim, $T \cap Gal(\mathbb{L}|\mathbb{K}') \subseteq T(\mathfrak{P}|\mathfrak{P}')$. Portanto, $T(\mathfrak{P}|\mathfrak{P}') = T \cap Gal(\mathbb{L}|\mathbb{K}')$. Além disso, se $\mathbb{K}'|\mathbb{K}$ é uma extensão de Galois, então, de modo análogo ao item (a), tem-se que $\sigma|_T : T \longrightarrow T(\mathfrak{P}'|\mathfrak{p})$ é um homomorfismo sobrejetivo, com núcleo $T(\mathfrak{P}|\mathfrak{P}')$.

c) Se $\sigma \in V_j(\mathfrak{P}|\mathfrak{P}')$, então $\sigma \in Gal(\mathbb{L}|\mathbb{K}')$ e $\sigma(\alpha) \equiv \alpha (mod\ \mathfrak{P}^{j+1})$, para todo $\alpha \in \mathcal{O}_{\mathbb{L}}$. Como σ fixa $\mathbb{K}'$, segue que σ fixa $\mathbb{K}$, e assim, $V_j(\mathfrak{P}|\mathfrak{P}') \subseteq V_j \cap Gal(\mathbb{L}|\mathbb{K}')$. Se $\sigma \in V_j \cap Gal(\mathbb{L}|\mathbb{K}')$, então $\sigma \in Gal(\mathbb{L}|\mathbb{K}')$ e $\sigma(\alpha) \equiv \alpha (mod\ \mathfrak{P}^{j+1})$, para todo $\alpha \in \mathcal{O}_{\mathbb{L}}$, e assim, $V_j \cap Gal(\mathbb{L}|\mathbb{K}') \subseteq V_j(\mathfrak{P}|\mathfrak{P}')$. ■

Notemos que para $j = 0$, tem-se que $V_j = T$ e os V_j's são subgrupos de T, os quais formam uma cadeia decrescente de subgrupos de G. Pelo Teorema de Correspondência de Galois, Teorema 1.6, segue que existem corpos fixos $\mathbb{K}_Z$ e $\mathbb{K}_T$ dos subgrupos Z e T de G, respectivamente. Assim, $\mathbb{K} \subset \mathbb{K}_Z \subset \mathbb{K}_T \subset \mathbb{L}$.

Definição 2.14 *O grupo $\mathbb{K}_Z$ é chamado de corpo de decomposição de $\mathfrak{P}$ e $\mathbb{K}_T$ o corpo de inércia de $\mathfrak{P}$.*

Observação 2.4 *Tem-se os seguintes diagramas*



Proposição 2.22 *Seja* $\mathbb{K} \subseteq \mathbb{K}' \subseteq \mathbb{L}$.

a) $\mathbb{K}_Z(\mathfrak{P}|\mathfrak{P}') = \mathbb{K}_Z\mathbb{K}'$. *Além disso, se* $\mathbb{K}'|\mathbb{K}$ *é uma extensão de Galois, então* $\mathbb{K}_Z(\mathfrak{P}'|\mathfrak{p}) = \mathbb{K}_Z \cap \mathbb{K}'$;

b) $\mathbb{K}_T(\mathfrak{P}|\mathfrak{P}') = \mathbb{K}_T\mathbb{K}'$. *Além disso, se* $\mathbb{K}'|\mathbb{K}$ *é uma extensão de Galois, então* $\mathbb{K}_T(\mathfrak{P}'|\mathfrak{p}) = \mathbb{K}_T \cap \mathbb{K}'$.

Demonstração. As demonstrações dos itens (a) e (b) seguem da Proposição 2.21. ■

Proposição 2.23 *Com as notações da Proposição 2.21 tem-se que* $\mathbb{K}_Z \subseteq \mathbb{K}'$ *se, e somente se,* $g(\mathfrak{P}|\mathfrak{P}') = 1$.

Demonstração. Sejam $G' = Gal(\mathbb{L}|\mathbb{K}')$ e $Z(\mathfrak{P}|\mathfrak{P}')$ o grupo de inércia de $\mathfrak{P}$ sobre $\mathfrak{P}'$. Pela igualdade fundamental tem-se que $e(\mathfrak{P}|\mathfrak{P}')f(\mathfrak{P}|\mathfrak{P}')g(\mathfrak{P}|\mathfrak{P}') = [\mathbb{L} : \mathbb{K}']$. Como $|Z(\mathfrak{P}|\mathfrak{P}')| = e(\mathfrak{P}|\mathfrak{P}')f(\mathfrak{P}|\mathfrak{P}')$, segue que $g(\mathfrak{P}|\mathfrak{P}') = (G' : Z(\mathfrak{P}|\mathfrak{P}'))$. Logo, $g(\mathfrak{P}|\mathfrak{P}') = 1$ se, e somente se, $Z(\mathfrak{P}|\mathfrak{P}') = Gal(\mathbb{L}|\mathbb{K}')$. Portanto, pela Proposição 2.21 item (a), $Z(\mathfrak{P}|\mathfrak{P}') = Gal(\mathbb{L}|\mathbb{K}')$ se, e somente se, $Gal(\mathbb{L}|\mathbb{K}') \subseteq Z$ se, e somente se, $\mathbb{K}_Z \subseteq \mathbb{K}'$. ■

Teorema 2.10 *Com as mesmas notações da Observação 2.4 tem-se que:*

a) $[\mathbb{L} : \mathbb{K}_Z] = ef$;

b) $e(\mathfrak{P}_Z|\mathfrak{p}) = 1,\ f(\mathfrak{P}_Z|\mathfrak{p}) = 1\ e\ \dfrac{\mathcal{O}_Z}{\mathfrak{P}_Z} = \dfrac{A}{\mathfrak{p}}$;

c) $g(\mathfrak{P}|\mathfrak{P}_Z) = 1,\ e(\mathfrak{P}|\mathfrak{P}_Z) = e,\ f(\mathfrak{P}|\mathfrak{P}_Z) = f$;

Demonstração. a) Segue da Proposição 2.20 item (b).

b) e c) Da Proposição 2.23 resulta que $g(\mathfrak{P}|\mathfrak{P}_Z) = 1$. Logo, $[\mathbb{L} : \mathbb{K}_Z] = e(\mathfrak{P}|\mathfrak{P}_Z)f(\mathfrak{P}|\mathfrak{P}_Z)$. Como $[\mathbb{L} : \mathbb{K}_Z] = ef$ e pela multiplicidade de índices de ramificação e graus de inércia $e = e(\mathfrak{P}|\mathfrak{P}_Z)e(\mathfrak{P}_Z|\mathfrak{p})$ e $f = f(\mathfrak{P}|\mathfrak{P}_Z)f(\mathfrak{P}_Z|\mathfrak{p})$, segue que $e(\mathfrak{P}_Z|\mathfrak{p}) = f(\mathfrak{P}_Z|\mathfrak{p}) = 1$, $e(\mathfrak{P}|\mathfrak{P}_Z) = e$ e $f(\mathfrak{P}|\mathfrak{P}_Z) = f$. ■

Teorema 2.11 *Existe um homomorfismo sobrejetor de Z no grupo de Galois de $\dfrac{\mathcal{O}_\mathbb{L}}{\mathfrak{P}}$ sobre $\dfrac{A}{\mathfrak{p}}$, com núcleo T. Este homomorfismo induz um isomorfismo de $Gal(\mathbb{K}_T|\mathbb{K}_Z)$ sobre $Gal\left(\dfrac{\mathcal{O}_\mathbb{L}}{\mathfrak{P}}|\dfrac{A}{\mathfrak{p}}\right) = \widehat{G}$.*

Demonstração. Pelo item (b) do Teorema 2.8, segue que cada $\sigma \in G$ induz um $\dfrac{A}{\mathfrak{p}}$-isomorfismo de $\dfrac{\mathcal{O}_\mathbb{L}}{\mathfrak{P}}$ em $\dfrac{\mathcal{O}_\mathbb{L}}{\sigma(\mathfrak{P})}$. Assim, se $\sigma \in Z$, então σ induz um $\dfrac{A}{\mathfrak{p}}$-automorfismo de $\dfrac{\mathcal{O}_\mathbb{L}}{\mathfrak{P}}$. Consideramos a aplicação $\Phi : Z \longrightarrow Gal\left(\dfrac{\mathcal{O}_\mathbb{L}}{\mathfrak{P}}|\dfrac{A}{\mathfrak{p}}\right)$ dada por $\Phi(\sigma) = \overline{\sigma} = \varphi \circ \sigma|_{\mathcal{O}_\mathbb{L}} \circ \varphi^{-1}$, onde φ é o homomorfismo canônico de $\mathcal{O}_\mathbb{L}$ em $\dfrac{\mathcal{O}_\mathbb{L}}{\mathfrak{P}}$. Tem-se que Φ é um homomorfismo, pois para $\sigma,\ \rho \in Z$, $\Phi(\sigma\rho) = \varphi \circ \sigma|_{\mathcal{O}_\mathbb{L}} \circ \rho|_{\mathcal{O}_\mathbb{L}} \circ \varphi^{-1} = \varphi \circ \sigma|_{\mathcal{O}_\mathbb{L}} \circ \varphi^{-1} \circ \varphi \circ \rho|_{\mathcal{O}_\mathbb{L}} \circ \varphi^{-1} = \overline{\sigma\rho}$. Agora, $\sigma \in Z$ está no núcleo de Φ se, e somente se, $\sigma(\alpha) + \mathfrak{P} = \alpha + \mathfrak{P}$ se, e somente se, $\sigma(\alpha) \equiv \alpha\ (mod\ \mathfrak{P})$, para todo $\alpha \in \mathcal{O}_\mathbb{L}$ se, e somente se, $\sigma \in T$. Por fim mostramos que Φ é sobrejetiva. Seja $\widehat{\sigma} \in \widehat{G}$. Se $\overline{\alpha} \in \dfrac{O_\mathbb{L}}{\mathfrak{P}}$, podemos considerar $\overline{\alpha} = \varphi(\alpha)$. Assim, $\widehat{\sigma}(\varphi(\alpha))$ é uma raiz do $min_{\frac{A}{\mathfrak{p}}}\varphi(\alpha)$. Como a extensão $\mathbb{L}|\mathbb{K}_Z$ é normal, segue que para $\alpha \in \mathcal{O}_\mathbb{L}$, todas as raízes do $min_{\mathbb{K}_Z}\varphi(\alpha)$ pertencem ao conjunto $\{\varphi(\sigma(\alpha)); \sigma \in G\}$. Pelo item (b) do Teorema 2.10, segue que $\mathbb{K}_Z = \dfrac{A}{\mathfrak{p}}$, e assim, $min_{\mathbb{K}_Z}\varphi(\alpha) = min_{\frac{A}{\mathfrak{p}}}\varphi(\alpha)$. Logo, $\widehat{\sigma}(\varphi(\alpha)) = \varphi(\sigma(\alpha))$, para algum $\sigma \in Z$. Portanto, $\widehat{\sigma} = \Phi(\sigma)$, ou seja, Φ é sobrejetiva. Assim, $\overline{\Phi} : Gal(\mathbb{K}_T|\mathbb{K}_Z) \longrightarrow \widehat{G}$ é um isomorfismo, pois $Gal(\mathbb{K}_T|\mathbb{K}_Z) = \dfrac{Z}{T}$. ■

Corolário 2.2 *O homomorfismo Φ dado no Teorema 2.11 restrito a $Z(\mathfrak{P}|\mathfrak{P}')$, induz um isomorfismo de $\dfrac{Z(\mathfrak{P}|\mathfrak{P}')}{T(\mathfrak{P}|\mathfrak{P}')}$ no grupo de Galois de $\dfrac{\mathcal{O}_\mathbb{L}}{\mathfrak{P}}$ sobre $\dfrac{\mathcal{O}_{\mathbb{K}'}}{\mathfrak{P}'}$.* ■

Proposição 2.24 *Com as notações da Proposição 2.22 e se $\mathbb{K}_Z \subseteq \mathbb{K}' \subseteq \mathbb{L}$, então $\mathbb{K}_T \subseteq \mathbb{K}'$ se, e somente se, $f(\mathfrak{P}|\mathfrak{P}') = 1$.*

Demonstração. Como $\mathbb{K}_Z \subseteq \mathbb{K}'$, segue, pela Proposição 2.23, que $g(\mathfrak{P}|\mathfrak{P}') = 1$. Assim, $Z(\mathfrak{P}|\mathfrak{P}') = Gal(\mathbb{L}|\mathbb{K}')$. Agora, $f(\mathfrak{P}|\mathfrak{P}') = 1$ se, e somente se, $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}} = \dfrac{\mathcal{O}_{\mathbb{K}'}}{\mathfrak{P}}$ se, e somente se, $Gal\left(\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}|\dfrac{\mathcal{O}_{\mathbb{K}'}}{\mathfrak{P}'}\right) = \{id\}$ se, e somente se, $T(\mathfrak{P}|\mathfrak{P}') = Z(\mathfrak{P}|\mathfrak{P}')$ se, e somente se, $Gal(\mathbb{L}|\mathbb{K}') \subseteq Gal(\mathbb{L}|\mathbb{K}_T)$ se, e somente se, $\mathbb{K}_T \subseteq \mathbb{K}'$. ■

Teorema 2.12 *Com as mesmas notações da Observação 2.4 tem-se que:*

a) $[\mathbb{L} : \mathbb{K}_T] = e,\ [\mathbb{K}_T : \mathbb{K}_Z] = f$;

b) $g(\mathfrak{P}|\mathfrak{P}_T) = 1,\ e(\mathfrak{P}|\mathfrak{P}_T) = e,\ f(\mathfrak{P}|\mathfrak{P}_T) = 1$ *e* $\dfrac{\mathcal{O}_T}{\mathfrak{P}_T} = \dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}$;

c) $g(\mathfrak{P}_T|\mathfrak{P}_Z) = 1,\ e(\mathfrak{P}_T|\mathfrak{P}_Z) = 1,\ f(\mathfrak{P}_T|\mathfrak{P}_Z) = f$;

Demonstração. a) Pela Proposição 2.20, tem-se que $[\mathbb{L} : \mathbb{K}_Z] = ef$ e pelo Teorema 2.11, tem-se que $[\mathbb{K}_T : \mathbb{K}_Z] = f = \left|Gal\left(\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}|\dfrac{A}{\mathfrak{p}}\right)\right|$. Portanto, $[\mathbb{L} : \mathbb{K}_T] = e$, $[\mathbb{K}_T : \mathbb{K}_Z] = f$.

b) Como $g(\mathfrak{P}|\mathfrak{P}_Z) = 1$, segue que $g(\mathfrak{P}|\mathfrak{P}_T) = g(\mathfrak{P}_T|\mathfrak{P}_Z) = 1$. Tomando $\mathbb{K}_T = \mathbb{K}'$ na Proposição 2.24, segue que $f(\mathfrak{P}|\mathfrak{P}_T) = 1$. Assim, $e(\mathfrak{P}|\mathfrak{P}_T) = [\mathbb{L} : \mathbb{K}_T] = e$.

c) Segue do item (b) e da multiplicidade de índice de ramificação e grau de inércia.■

Proposição 2.25 *Existe $t \in \mathbb{N}$ tal que V_t é trivial.*

Demonstração. Como G é finito, segue que a cadeia $G \supseteq Z \supseteq T \supseteq V_1 \supseteq \ldots$ é estacionária, ou seja, existe $t \in \mathbb{N}$ tal que $V_t = V_{t+1} = \ldots$. Assim, $V_t = \bigcap_{i\in\mathbb{N}} V_i$. Se $\sigma \in V_i$, para todo $i \in \mathbb{N}$, então $\sigma(\alpha) \equiv \alpha(mod \bigcap_{i\in\mathbb{N}} \mathfrak{P}^{i+1})$, para todo $\alpha \in \mathcal{O}_{\mathbb{L}}$. Como $\bigcap_{i\in\mathbb{N}} \mathfrak{P}^{i+1} = \{0\}$, segue que $\sigma(\alpha) = \alpha$, para todo $\alpha \in \mathcal{O}_{\mathbb{L}}$, ou seja, $\sigma = id$. ■

Proposição 2.26 *Os grupos de decomposição, inércia e ramificação não se alteram no processo de localização, ou seja, se $S = A - \mathfrak{p}$, então $Z = \{\sigma \in G; \sigma(S^{-1}\mathfrak{P}) = S^{-1}\mathfrak{P}\}$ e $V_j = \{\sigma \in Z; \sigma(\alpha) \equiv \alpha(mod\ (S^{-1}\mathfrak{P})^{j+1}),$ para todo $\alpha \in S^{-1}\mathcal{O}_{\mathbb{L}}\}$, para $j \in \mathbb{N}$.*

Demonstração. Se $\sigma \in Z$ e $\dfrac{b}{s} \in S^{-1}\mathfrak{P}$, então $\sigma(\dfrac{b}{s}) = \dfrac{\sigma(b)}{s} \subseteq S^{-1}\mathfrak{P}$. Tomando $\sigma = id$, tem-se que $S^{-1}\mathfrak{P} \subseteq \sigma(S^{-1}\mathfrak{P})$. Por outro lado, observamos que $S^{-1}\mathfrak{P} \cap \mathcal{O}_{\mathbb{L}} = \mathfrak{P}$ (Proposição 2.5). Assim, $\sigma(\mathfrak{P}) = \sigma(S^{-1}\mathfrak{P} \cap \mathcal{O}_{\mathbb{L}}) = \sigma(S^{-1}\mathfrak{P} \cap \mathcal{O}_{\mathbb{L}} = S^{-1}\mathfrak{P} \cap \mathcal{O}_{\mathbb{L}} = \mathfrak{P}$.

Portanto, $Z = \{\sigma \in G; \sigma(S^{-1}\mathfrak{P}) = S^{-1}\mathfrak{P}\}$. Agora, se $\sigma \in V_j$ e $\frac{\alpha}{s} \in S^{-1}\mathcal{O}_{\mathbb{L}}$, então $\frac{\sigma(\alpha)}{s} - \frac{\alpha}{s} = \frac{\sigma(\alpha)-\alpha}{s} \in (S^{-1}\mathfrak{P})^{j+1}$. Por outro lado, como $\mathfrak{P}^{j+1} = (S^{-1}\mathfrak{P})^{j+1} \cap \mathcal{O}_{\mathbb{L}}$, $\sigma(\alpha) - \alpha \in (S^{-1}\mathfrak{P})^{j+1}$, para $\frac{\alpha}{1} \in S^{-1}\mathcal{O}_{\mathbb{L}}$, segue que $\sigma(\alpha) - \alpha \in (S^{-1}\mathfrak{P})^{j+1} \cap \mathcal{O}_{\mathbb{L}}$, pois $\sigma(\alpha) \in \mathcal{O}_{\mathbb{L}}$. Pelo fato de que $\mathfrak{P}^{j+1} = (S^{-1}\mathfrak{P})^{j+1} \cap \mathcal{O}_{\mathbb{L}}$, tem-se que $\sigma(\alpha) - \alpha \in \mathfrak{P}^{j+1}$. Portanto, $V_j = \{\sigma \in Z; \sigma(\alpha) \equiv \alpha (mod\ (S^{-1}\mathfrak{P})^{j+1})$, para todo $\alpha \in S^{-1}\mathcal{O}_{\mathbb{L}}$. ■

Observação 2.5 *Se $\mathfrak{P}$ é um ideal primo de $\mathcal{O}_{\mathbb{L}}$, então $\mathfrak{P} \cap A$ é um ideal primo de A. No processo de localização, tem-se que $S^{-1}\mathfrak{p}$ é o único ideal primo de $S^{-1}A$, e assim, $S^{-1}\mathfrak{P} \cap S^{-1}A = S^{-1}\mathfrak{p}$, para todo $\mathfrak{P}$ ideal primo de $\mathcal{O}_{\mathbb{L}}$, ou seja, $S^{-1}\mathfrak{P}$ está acima de $S^{-1}\mathfrak{p}$. Como existe um número finito de ideais de $S^{-1}\mathcal{O}_{\mathbb{L}}$ acima de $S^{-1}\mathfrak{p}$, segue que $S^{-1}\mathcal{O}_{\mathbb{L}}$ é um anel principal, ou seja, $S^{-1}\mathfrak{P}$ é um ideal principal. Portanto, pela Proposição 2.26, podemos considerar $\mathcal{O}_{\mathbb{L}}$ um anel principal, pois os grupos de decomposição, inércia e ramificação não se alteram.*

Lema 2.7 *Se $\mathbb{K}$ é um corpo e G um subgrupo finito de ordem m do grupo $\mathbb{K}^*$, o grupo multiplicativo de $\mathbb{K}$, então G é ciclíco.*

Demonstração. Como $\mathbb{K}^*$ é um grupo abeliano, segue que G é um grupo abeliano finito de ordem m. Assim, pelo Corolário 1.7, existe um elemento $\beta \in G$ tal que $o(\beta) = mmc\{o(\alpha); \alpha \in G\} = r$. Logo, r é um múltiplo da $o(\alpha)$, para todo $\alpha \in G$ e m é um múltiplo de r, e assim, tem-se que $G \subseteq U_r \subseteq U_m$, onde U_i é o conjunto das raízes i-ésimas da unidade, para $i = r, m$. Pelo fato de $|U_m| = m$, segue que $G = U_m$. Portanto, G é ciclíco. ■

Pelo Lema 2.7, segue que se $q = card(\mathbb{K})$, então $\mathbb{K}^*$ é ciclíco de ordem $q - 1$.

Lema 2.8 *Se $\mathbb{K}$ é um corpo de característica p e G um subgrupo de ordem n do grupo $\mathbb{K}^*$, então $p \nmid n$.*

Demonstração. Seja ζ_n raíz n-ésima primitiva da unidade. Se $p|n$, então $p \neq 0$ e $(\zeta_n^{\frac{n}{p}})^p = \zeta_n^n = 1$. Assim, $\zeta_n^{\frac{n}{p}} = 1$, o que é um absurdo. ■

Definição 2.15 *Sejam G um grupo finito e p um número primo. Se p^n divide a ordem de G e p^{n+1} não divide a ordem G, dizemos que os subgrupos de G de ordem p^n são p-subgrupos de Sylow de G.*

Observação 2.6 *Os p-subgrupos de Sylow de um grupo G são dois a dois conjugados. O grupo aditivo de um corpo $\mathbb{K}$ possui apenas o subgrupo trivial se $\mathbb{K}$ tiver característica zero ou os p-subgrupos elementares (grupos isomorfos a produtos de grupos de ordem p) se $\mathbb{K}$ tiver característica p primo.*

Teorema 2.13 *O grupo quociente $\frac{T}{V_1}$ é canonicamente isomorfo a um subgrupo do grupo multiplicativo de $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}$ e para todo $i \geq 1$, o grupo quociente $\frac{V_j}{V_{j+1}}$ é isomorfo a um subgrupo do grupo aditivo de $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}$.*

Demonstração. Localizando, tem-se que $\mathfrak{P} = \langle b \rangle$, com $b \in \mathcal{O}_{\mathbb{L}}$. Se $\sigma \in T$, então $\sigma(b) \equiv b(mod\ \mathfrak{P})$, e assim, $\sigma(b) \in \mathfrak{P}$. Mas, $\sigma(b) \notin \mathfrak{P}^2$, pois se $\sigma(b) \in \mathfrak{P}^2$, então $\mathfrak{P} \subset \mathfrak{P}^2$, o que contraria a Proposição 2.3. Como $\sigma(b) \in \mathfrak{P}$, segue que podemos escrever $\sigma(b) = x_\sigma b$, com $x_\sigma \in \mathcal{O}_{\mathbb{L}}$ e $b \nmid x_\sigma$. Seja $\tau \in T$. Tem-se que $\sigma\tau(b) = \sigma(x_\tau b) = \sigma(x_\tau)\sigma(b) = \sigma(x_\tau)x_\sigma b$. Logo, $x_{\sigma\tau} = \sigma(x_\tau)x_\sigma$. Como $\sigma \in T$ e $x_\tau \in \mathcal{O}_{\mathbb{L}}$, segue que $\sigma(x_\tau) \equiv x_\tau(mod\ \mathfrak{P})$. Portanto, $x_{\sigma\tau} \equiv x_\tau x_\sigma(mod\ \mathfrak{P})$, ou seja, $\overline{x}_{\sigma\tau} = \overline{x_\sigma x_\tau}$. Assim, a aplicação $\Phi : T \longrightarrow J$, dada por $\Phi(\sigma) = \overline{x}_\sigma$, onde $J = \left\{ \overline{x}_\sigma \in \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}^* ;\ x_\sigma b = \sigma(b) \right\}$ é um homomorfismo sobrejetor. O $Ker(\Phi) = \{\sigma \in T;\ \overline{x}_\sigma = \overline{1}\} = \{\sigma \in T; x_\sigma b \equiv b(mod\ \mathfrak{P}^2)\} = \{\sigma \in T;\ \sigma(b) \equiv b(mod\ \mathfrak{P}^2)\} \supseteq V_1$. Agora, consideramos $\sigma \in V_j$ $(j \geq 1)$. Assim, $\sigma(b) \equiv b(mod\ \mathfrak{P}^{j+1})$, ou seja, $\sigma(b) - b \in \mathfrak{P}^{j+1}$. Logo, podemos escrever $\sigma(b) - b = y_\sigma b^{j+1}$, com $y_\sigma \in \mathcal{O}_{\mathbb{L}}$ e $b^{j+1} \nmid y_\sigma$. Seja $\tau \in V_j$. Tem-se que $y_{\sigma\tau}b^{j+1} = \sigma\tau(b) - b = \sigma(y_\tau b^{j+1} + b) - b = \sigma(y_\tau)\sigma(b)^{j+1} + \sigma(b) - b = \sigma(y_\tau)(y_\sigma b^{j+1} + b)^{j+1} + y_\sigma b^{j+1}$. Assim, $y_{\sigma\tau} = \sigma(y_\tau)\left(\frac{b + y_\sigma b^{j+1}}{b}\right)^{j+1} + \frac{y_\sigma b^{j+1}}{b^{j+1}} = \sigma(y_\tau)(1 + y_\sigma b^j)^{j+1} + y_\sigma$. Como $\sigma \in V_j$ e $y_\tau \in \mathcal{O}_{\mathbb{L}}$, segue que $\sigma(y_\tau) \equiv y_\tau(mod\ \mathfrak{P}^{j+1})$ o que implica que $\sigma(y_\tau) \equiv y_\tau(mod\ \mathfrak{P})$, pois $V_j \subseteq T$. Expandindo a equação $(1 + y_\sigma b^j)^{j+1}$, tem-se que todos os termos exceto o primeiro estão em $\mathfrak{P}^j \subset \mathfrak{P}$. Assim, $y_{\sigma\tau} \equiv y_\tau + y_\sigma(mod\ \mathfrak{P})$, ou seja, $\overline{y}_{\sigma\tau} = \overline{y}_\tau + \overline{y}_\sigma$. Portanto, a aplicação $\Omega : V_j \longrightarrow H$, dada por $\Omega(\sigma) = \overline{y}_\sigma$, onde $H = \left\{ \overline{y}_\sigma \in \frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}};\ \sigma(b) - b = y_\sigma b^{j+1} \right\}$, é um homomorfismo sobrejetor. O $Ker(\Omega) = \{\sigma \in V_j;\ y_\sigma \equiv 0(mod\ \mathfrak{P})\} = \{\sigma \in V_j;\ y_\sigma b^{j+1} \equiv 0(mod\ \mathfrak{P}^{j+2})\} = \{\sigma \in V_j;\ \sigma(b) \equiv b(mod\ \mathfrak{P}^{j+2})\} \supseteq V_{j+1}$. Agora, mostramos que $Ker(\Phi) = V_1$ e $Ker(\Omega) = V_{j+1}$. Seja $\sigma \in T$ tal que $\sigma \in Ker(\Phi)$. Se $z \in \mathfrak{P}$, então podemos escrever $z = ab$, com $a \in \mathcal{O}_{\mathbb{L}}$ e $b \nmid a$. Assim, $\sigma(z) - z = \sigma(ab) - ab = \sigma(a)\sigma(b) - ab + \sigma(a)b - \sigma(a)b = b(\sigma(a) - a) + \sigma(a)(\sigma(b) - b)$.

Notemos que $\sigma(a) - a \in \mathfrak{P}$, $b \in \mathfrak{P}$, $\sigma(b) - b \in \mathfrak{P}^2$ e $\sigma(a) \in \mathcal{O}_{\mathbb{L}}$. Assim, $\sigma(z) - z \in \mathfrak{P}^2$. Portanto, para qualquer $z \in \mathfrak{P}$, tem-se que $\sigma(z) - z \in \mathfrak{P}^2$. Consideramos $x \in \mathcal{O}_{\mathbb{L}}$ e escrevemos $\sigma^p(x) - x = \sigma^{p-1}(\sigma(x) - x) + \sigma^{p-2}(\sigma(x) - x) + \ldots + \sigma(\sigma(x) - x) + \sigma(x) - x$. Tem-se que $\sigma(x) - x \in \mathfrak{P}$, pois $x \in \mathcal{O}_{\mathbb{L}}$ e $\sigma \in T$. Assim, $\sigma(x) - x = z \in \mathfrak{P}$. Pela primeira parte tem-se que $\sigma(z) - z \in \mathfrak{P}^2$, e assim, $\sigma(z) \equiv z (mod\ \mathfrak{P}^2)$ o que implica que $\sigma^k(z) \equiv z(mod\ \mathfrak{P}^2)$, para $1 \leq k \leq p$. Logo, $\sigma^p(x) - x \equiv pz(mod\ \mathfrak{P}^2)$. Se $p = car\left(\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}\right)$, então $p1 \in \mathfrak{P}$. Como $z \in \mathfrak{P}$, segue que $pz \in \mathfrak{P}^2$, ou seja, $\sigma^p(x) \equiv x(mod\ \mathfrak{P}^2)$. Portanto, $\sigma^p \in V_1$. De modo análogo, mostramos que $Ker(\Omega) = V_{j+1}$. De fato, se $\sigma \in V_j$ e $\sigma(b) \equiv b(mod\ \mathfrak{P}^{j+2})$, então $\sigma(z) - z \in \mathfrak{P}^{j+2}$, para todo $z \in \mathfrak{P}$. Logo, $\sigma(z) - z \in \mathfrak{P}^{j+2}$. Agora, se $x \in \mathcal{O}_{\mathbb{L}}$, então $\sigma(x) - x \in \mathfrak{P}^{j+1} \subset \mathfrak{P}$. Assim, $\sigma(x) - x = z \in \mathfrak{P}$, o que implica que $\sigma(z) - z \in \mathfrak{P}^{j+2}$. Assim, $\sigma^p(x) - x \equiv pz(mod\ \mathfrak{P}^{j+2})$. Portanto, $\sigma^p(x) - x(mod\ \mathfrak{P}^{j+2})$, ou seja, $\sigma^p \in V_{j+1}$. ■

Corolário 2.3 *Se* $car\left(\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}\right) = 0$, *então* T *é ciclíco e* V_1 *é trivial. Se* $car\left(\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}\right) = p$, *com* p *primo, então* $\dfrac{T}{V_1}$ *é ciclíco, cuja a ordem não é divisível por* p *e* $\dfrac{V_j}{V_{j+1}}$ *é um produto direto de grupos ciclícos de ordem* p, *para* $j \geq 1$. *Além disso,* V_1 *é o único subgrupo de Sylow de* T. ■

Demonstração. Pelo Teorema 2.13, tem-se que $\dfrac{T}{V_1}$ é isomorfo a um subgrupo do grupo multiplicativo de $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}$, e assim, pelo Lema 2.7, $\dfrac{T}{V_1}$ é ciclíco. Se $car(\dfrac{\mathcal{O}_L}{\mathfrak{P}}) = 0$ e $\dfrac{V_j}{V_{j+1}}$ é isomorfo a um subgrupo do grupo aditivo de $\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}$ (Teorema 2.13), segue, pela Observação 2.6, que $\dfrac{V_j}{V_{j+1}}$ é trivial. Logo, $V_j = V_{j+1}$, para todo $j \geq 1$. Portanto, pela Proposição 2.25, tem-se que V_j é trivial, para todo $j \geq 1$, e consequentemente, $T = \dfrac{T}{V_1}$ é ciclíco. Agora, se $car(\dfrac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}) = p \neq 0$, então, pelo Teorema 2.13 e pelo Lema 2.8, tem-se que $\dfrac{V_j}{V_{j+1}}$ é p-grupo elementar, para todo $j \geq 1$. Logo, $\left|\dfrac{T}{V_1}\right| = \dfrac{|T|}{p^k} = m$, ou seja, $|T| = mp^k$, com $p \nmid m$. Assim, V_1 é um p-subgrupo de Sylow de T e é o único, pois V_1 é um subgrupo normal de T. ■

A seguir definimos o automorfismo de Frobenius que será útil quando um ideal primo $\mathfrak{p}$ de A não ramifica em $\mathcal{O}_{\mathbb{L}}$.

Sejam A um domínio de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n, $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de $\mathbb{L}$ sobre A, $\mathfrak{p}$ um ideal primo A e $\mathfrak{P}$ um ideal primo de $\mathcal{O}_{\mathbb{L}}$ acima de $\mathfrak{p}$.

Suponhamos que $\mathfrak{p}$ não se ramifica em $\mathcal{O}_{\mathbb{L}}$. Tem-se que $\frac{A}{\mathfrak{p}}$ é um corpo finito com q elementos e de característica p primo. Assim, T é trivial e Z é isomorfo ao grupo de Galois de $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}$ sobre $\frac{A}{\mathfrak{p}}$. Portanto, Z é ciclíco de ordem q, gerado pelo automorfismo σ tal que

$$\sigma(\alpha) \equiv \alpha^q \ (mod\ \mathfrak{P}).$$

Definição 2.16 *O automorfismo σ que gera Z é chamado de automorfismo de Frobenius associado a $\mathfrak{P}$ e denotado por $(\mathfrak{P}, \mathcal{O}_{\mathbb{L}}|A)$.*

Proposição 2.27 *Se $\frac{Z}{V_1}$ é abeliano, então $\frac{T}{V_1}$ é ciclíco de ordem dividindo $q-1$.*

Demonstração. Se $\mathcal{O}_{\mathbb{L}}$ é um anel principal, então $\mathfrak{P} = \langle b \rangle$, com $b \in \mathcal{O}_{\mathbb{L}}$. Para cada $\sigma \in Z$, tem-se que $\sigma(b) = kb$, com $k \in \mathcal{O}_{\mathbb{L}}$ e $b \nmid k$, pois $\sigma(b) \equiv b\ (mod \mathfrak{P})$, isto é, pertence a $\mathfrak{P}$. Como $\frac{T}{V_1}$ é isomorfo a um subgrupo do grupo multiplicativo de $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}$, segue, pelo Lema 2.7, que $\frac{T}{V_1}$ é ciclíco gerado por um $\tau \in T$ tal que $\overline{\tau} = \tau \circ V_1$. Para cada $\sigma \in Z$, pelo Teorema 2.11, σ induz um $\overline{\sigma} \in Gal\left(\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}|\frac{A}{\mathfrak{p}}\right) = \widehat{G}$. Tem-se que $\hat{G}$ é ciclíco gerado por um automorfismo de Frobenius. Sejam $\sigma(b) = kb$, $\tau(b) = mb$ e $\sigma\tau\sigma^{-1}(b) = lb$. Notemos que $\sigma(b) = kb$ implica que $\sigma^{-1}(b) = b(\sigma^{-1}(k))^{-1}$. Como $\frac{Z}{V_1}$ é abeliano, segue que $\sigma\tau\sigma^{-1} = \tau$ o que implica que $\overline{l} = \overline{m}$. Calculemos o valor de l.

$$\sigma\tau\sigma^{-1}(b) = \sigma\tau(b(\sigma^{-1}(k))^{-1}) = \sigma(mb\tau\sigma^{-1}(k^{-1})) = \sigma(m)kb\sigma\tau\sigma^{-1}(k^{-1}).$$

Logo, $l = \sigma(m)k\sigma\tau\sigma^{-1}(k^{-1})$. Reduzindo $mod\ \mathfrak{P}$, tem-se $\tau(\sigma^{-1}(k^{-1})) \equiv \sigma^{-1}(k^{-1})(mod\mathfrak{P})$, pois $\sigma^{-1}(k^{-1}) \in \mathcal{O}_{\mathbb{L}}$. Assim, $\sigma\tau\sigma^{-1}(k^{-1}) = k^{-1}$. Logo, $\overline{l} = \overline{\sigma(m)} = \overline{\sigma}(\overline{m})$, onde $\overline{\sigma} = \varphi \circ \sigma|_{\mathcal{O}_{\mathbb{L}}} \circ \varphi^{-1}$, com φ o homomorfismo canônico de $\mathcal{O}_{\mathbb{L}}$ em $\frac{\mathcal{O}_{\mathbb{L}}}{\mathfrak{P}}$. Como $\overline{\sigma} \in \hat{G}$, segue que podemos considerar $\overline{\sigma}$ como gerador de $\hat{G}$. Logo, $\overline{\sigma}(\overline{m}) = \overline{m}^q$, e daí, $\overline{l} = \overline{m}^q$. Portanto, $\overline{m}^q = \overline{m}$ o que implica que $\overline{m}^{q-1} = \overline{1}$. Portanto, $\frac{T}{V_1}$ é ciclíco de ordem $q-1$. ■

2.5 Diferente

O objetivo desta seção é definir diferente de uma extensão. O principal resultado é a transitividade do diferente, a qual é usada na demonstração do Teorema de Kronecker-Weber. Os resultados desta seção podem ser encontrados com mais detalhes em [9] e [16].

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

Definição 2.17 *Seja M um subconjunto de $\mathbb{L}$. Chamamos o conjunto $M^* = \{x \in \mathbb{L};\ Tr_{\mathbb{L}|\mathbb{K}}(xy) \in A,\ \text{para todo } y \in M\}$ de codiferente de M sobre $\mathbb{K}$, ou ainda, de espaço dual ou complementar de M.*

Proposição 2.28 *Sejam M um subconjunto de $\mathbb{L}$ e M^* o complementar de M.*

a) M^* é um A-módulo e se $\mathcal{O}_{\mathbb{L}}M \subseteq M$, então M^* é um $\mathcal{O}_{\mathbb{L}}$-módulo.

b) Se $M_1 \subseteq M_2 \subseteq \mathbb{L}$, então $M_2^* \subseteq M_1^* \subseteq \mathbb{L}$.

c) $\mathcal{O}_{\mathbb{L}} \subseteq \mathcal{O}_{\mathbb{L}}^*$ e $Tr_{\mathbb{L}|\mathbb{K}}\mathcal{O}_{\mathbb{L}}^* \subseteq A$.

d) Se M é um A-módulo livre cojm base $\{x_1, \ldots, x_n\}$, então M^* é um A-módulo livre com base $\{x_1^*, \ldots, x_n^*\}$ e $M^{**} = M$.

Demonstração. [9], pág. 240.

Proposição 2.29 *$\mathcal{O}_{\mathbb{L}}^*$ é um ideal fracionário de $\mathcal{O}_{\mathbb{L}}$.*

Demonstração. Basta mostrarmos que $\mathcal{O}_{\mathbb{L}}^*$ é um $\mathcal{O}_{\mathbb{L}}$-módulo finitamente gerado, pois assim existe um denominador comum $d \in \mathcal{O}_{\mathbb{L}} - \{0\}$ dos elementos de $\mathcal{O}_{\mathbb{L}}^*$ tal que $d\mathcal{O}_{\mathbb{L}}^* \subseteq \mathcal{O}_{\mathbb{L}}$. Se $t \in \mathcal{O}_{\mathbb{L}}$, então $A[t]$ é um A-módulo finitamente gerado, pois t é inteiro sobre A. Logo, pela Proposição 2.28 $A[t]^*$ é um A-módulo finitamente gerado. Como $A[t] \subseteq \mathcal{O}_{\mathbb{L}}$, segue que $\mathcal{O}_{\mathbb{L}}^* \subseteq A[t]^*$, com $A[t]^*$ um anel Noetheriano, pois A é um domínio de Dedekind e $A[t]^*$ um A-módulo finitamente gerado. Assim, $\mathcal{O}_{\mathbb{L}}^*$ é um $A[t]^*$-módulo finitamente gerado, e consequentemente, um $\mathcal{O}_{\mathbb{L}}$-módulo finitamente gerado. ■

Definição 2.18 *O inverso do ideal fracionário $\mathcal{O}_{\mathbb{L}}^*$ de $\mathcal{O}_{\mathbb{L}}$ é chamado de diferente de $\mathcal{O}_{\mathbb{L}}$ sobre A e denotado por $\Delta(\mathcal{O}_{\mathbb{L}}|A)$ ou $\Delta(\mathbb{L}|\mathbb{K})$.*

Como $\mathcal{O}_{\mathbb{L}} \subseteq \mathcal{O}_{\mathbb{L}}^*$, segue que $\Delta(\mathcal{O}_{\mathbb{L}}|A)$ é um ideal inteiro de $\mathcal{O}_{\mathbb{L}}$. Assim, $\Delta(\mathcal{O}_{\mathbb{L}}|A)$ é decomposto como produto de potências de ideais primo e $\mathcal{O}_{\mathbb{L}}$, ou seja, $\Delta(\mathcal{O}_{\mathbb{L}}|A) = \prod(\mathfrak{P}_1 \dots \mathfrak{P}_q)^e$, onde $\mathfrak{P}_i$'s são ideais primos de $\mathcal{O}_{\mathbb{L}}$ e e um inteiro positivo.

Proposição 2.30 *Se $\mathfrak{B}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{L}}$, então $Tr_{\mathbb{L}|\mathbb{K}}(\mathfrak{B}) \subseteq A$ se, e somente se, $\mathfrak{B} \subseteq \mathcal{O}_{\mathbb{L}}^* = \Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1}$.*

Demonstração. Se $\mathfrak{B} \subseteq \mathcal{O}_{\mathbb{L}}^*$, então $Tr_{\mathbb{L}|\mathbb{K}}(\mathfrak{B}) \subseteq Tr_{\mathbb{L}|\mathbb{K}}(\mathcal{O}_{\mathbb{L}}^*) \subseteq A$. Por outro lado, se $Tr_{\mathbb{L}|\mathbb{K}}(\mathfrak{B}) \subseteq A$, então $\mathfrak{B} \subseteq \mathcal{O}_{\mathbb{L}}^* = \{x \in \mathbb{L};\ Tr_{\mathbb{L}|\mathbb{K}}(xy) \in A,\ \text{para todo } y \in \mathcal{O}_{\mathbb{L}}\}$, pois $\mathfrak{B} = \mathfrak{B}\mathcal{O}_{\mathbb{L}}$. ■

Lema 2.9 *Sejam $\mathfrak{P}$ e $\mathfrak{B}$ ideais fracionários de $\mathcal{O}_{\mathbb{L}}$. Se para todo $\mathfrak{M}$ ideal fracionário de $\mathcal{O}_{\mathbb{L}}$ tem-se que $\mathfrak{M} \subseteq \mathfrak{P}$ se, e somente se, $\mathfrak{M} \subseteq \mathfrak{B}$, então $\mathfrak{P} = \mathfrak{B}$.*

Demonstração. Se $x \in \mathfrak{P}$, então $\langle x \rangle \subseteq \mathfrak{P}$. Se $\mathfrak{M} = \langle x \rangle$, então $\mathfrak{M} \subseteq \mathfrak{B}$, ou seja, $x \in \mathfrak{B}$. Portanto, $\mathfrak{P} \subseteq \mathfrak{B}$. Por outro lado, se $x \in \mathfrak{B}$, então $\mathfrak{M} = \langle x \rangle \subseteq \mathfrak{B}$ o que implica que $\mathfrak{M} = \langle x \rangle \subseteq \mathfrak{P}$. Portanto, $\mathfrak{B} \subseteq \mathfrak{P}$. ■

Proposição 2.31 *(Transitividade do diferente) Se $\mathbb{M}$ é um corpo tal que $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ e $\mathcal{O}_{\mathbb{M}}$ o anel de inteiros de $\mathbb{M}$ sobre A, então $\Delta(\mathcal{O}_{\mathbb{L}}|A) = \mathcal{O}_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{M}}|A)\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{M}})$.*

Demonstração. Seja $\mathfrak{B}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{L}}$ tal que $\mathfrak{B} \subseteq \Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{M}})^{-1}$. Pela Proposição 2.30 $Tr_{\mathbb{L}|\mathbb{M}}(\mathfrak{B}) \subseteq \mathcal{O}_{\mathbb{M}}$. Logo, $\Delta(\mathcal{O}_M|A)^{-1}Tr_{\mathbb{L}|\mathbb{M}}(\mathfrak{B}) \subseteq \Delta(\mathcal{O}_{\mathbb{M}}|A)^{-1}$. Como $\mathfrak{B} = \mathfrak{B}\mathcal{O}_{\mathbb{L}}$, segue que $Tr_{\mathbb{L}|\mathbb{M}}(\mathcal{O}_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{M}}|A)^{-1}\mathfrak{B}) \subseteq \Delta(\mathcal{O}_{\mathbb{M}}|A)^{-1}$. Tem-se que $A \supseteq Tr_{\mathbb{M}|\mathbb{K}}(\Delta(\mathcal{O}_{\mathbb{M}}|A)^{-1}) \supseteq Tr_{\mathbb{L}|\mathbb{K}}(\mathcal{O}_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{M}}|A)^{-1}\mathfrak{B})$. Novamente pela Proposição 2.30, tem-se que $\mathcal{O}_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{M}}|A)^{-1}\mathfrak{B} \subseteq \Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1}$, ou seja, $\mathfrak{B} \subseteq \mathcal{O}_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{M}}|A)\Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1}$. Portanto, pelo Lema 2.9, tem-se que $\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{M}})^{-1} = \mathcal{O}_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{M}}|A)\Delta(\mathcal{O}_{\mathbb{L}}|A)^{-1}$, ou seja, $\Delta(\mathcal{O}_{\mathbb{L}}|A) = \mathcal{O}_{\mathbb{L}}\Delta(\mathcal{O}_{\mathbb{M}}|A)\Delta(\mathcal{O}_{\mathbb{L}}|\mathcal{O}_{\mathbb{M}})$. ■

Definição 2.19 *Seja $\mathbb{K}$ é um corpo de número algébrico. O ideal $\Delta(\mathcal{O}_{\mathbb{L}}|A)$ é chamado de diferente da extensão $\mathbb{L}|\mathbb{K}$ e denotado por $\Delta_{\mathbb{L}|\mathbb{K}}$. Quando $\mathbb{K} = \mathbb{Q}$ o ideal $\Delta_{\mathbb{L}|\mathbb{K}}$ é chamado de*

diferente absoluto de $\mathbb{L}$ *e denotado por* $\Delta_{\mathbb{L}}$. *No processo de localização, ou seja, quando consideramos* $S = A - \mathfrak{p}$, *o diferente* $\Delta(S^{-1}\mathcal{O}_{\mathbb{L}}|S^{-1}A)$ *é chamado de diferente de* $\mathbb{L}|\mathbb{K}$ *acima de* $\mathfrak{p}$ *e denotado por* $\Delta_{\mathfrak{p}}(\mathbb{L}|\mathbb{K})$.

Lema 2.10 $\Delta_{\mathbb{L}|\mathbb{K}}S^{-1}\mathcal{O}_{\mathbb{L}} = \Delta_{\mathfrak{p}}(\mathbb{L}|\mathbb{K})$.

Demonstração. [9], pág. 245.

Lema 2.11 *Se* $\mathfrak{p}$ *é um ideal primo de* A *não nulo que se ramifa totalmente em* $\mathcal{O}_{\mathbb{L}}$, *então* $\Delta_{\mathfrak{p}}(\mathbb{L}|\mathbb{K}) = S^{-1}f'(\alpha)^{(\sum_{i\geq 0}\#V_i - 1)}$, *onde* α *é um elemento primitvo,* $f(x) = min_{\mathbb{K}}\alpha$ *e os* V_i*'s são os* i*-ésimos grupos de ramificação de* $\mathfrak{P}$ *sobre* $\mathfrak{p}$, *com* $\mathfrak{P} \cap A = \mathfrak{p}$.

Demonstração. [9], pág. 270.

Observação 2.7 *No processo de localização podemos tomar* α *(do Lema 2.11) como um gerador do ideal primo* $\mathfrak{P}$ *acima de* p.

2.6 Valorização

Esta seção traz alguns resultados sobre anéis de valorização e valorização associada a um ideal, os quais são usados como artifício para facilitar as demonstrações de alguns resultados envolvendo o Teorema de Kronecker-Weber. Os resultados desta seção não serão demonstrados, pois não é o objetivo deste trabalho. A principal referência desta seção é [6].

Definição 2.20 *Sejam* A *um domínio de integridade e* $\mathbb{K}$ *seu corpo de frações. O anel* A *é chamado anel de Valorização de* $\mathbb{K}$ *se para cada* $x \in \mathbb{K}$ *não nulo, tem-se que* $x \in A$ *ou* $x^{-1} \in A$.

Proposição 2.32 *Seja* A *um anel de valorização.*

i) A *é um anel local, ou seja, tem um único ideal maximal;*

ii) Se A' *é um anel tal que* $A \subseteq A' \subseteq \mathbb{K}$, *então* A' *é um anel de valorização de* $\mathbb{K}$;

iii) A é integralmente fechado.

Definição 2.21 *Uma valorização discreta de um corpo $\mathbb{K}$ é uma aplicação $v : \mathbb{K}^* \longrightarrow \mathbb{Z}$ tal que*

a) $v(xy) = v(x) + v(y)$;

b) $v(x + y) \geq min\{v(x), v(y)\}$ e a igualdade ocorre se $v(x) \neq v(y)$.

Definição 2.22 *O anel formado pelo zero e por todos $x \in \mathbb{K}^*$ tal que $v(x) \geq 0$ é chamado anel da valorização v.*

Observação 2.8 *Um domínio de integridade A é um anel de valorização discreta se existir uma valorização discreta v de $\mathbb{K}$ (corpo de frações de A) tal que A é o anel de valorização de v.*

Proposição 2.33 *Se A é um domínio de integridade, local e Noetheriano, então são equivalentes*

i) A é um anel de valorização discreta;

ii) Todo ideal não nulo de A é um potência de $\mathfrak{m}$, onde $\mathfrak{m}$ é o único ideal maximal de A.

Exemplo 2.6 *Pela Proposição 2.10, segue que $S^{-1}A$ é um anel de valorização discreta, para $S = A - \mathfrak{p}$.*

Sejam A um anel de Dedekind, $\mathbb{K}$ seu corpo de frações e $\mathbb{L}$ uma extensão finita de grau n de $\mathbb{K}$.

Definição 2.23 *Uma valorização discreta v de um corpo $\mathbb{K}$ é uma valorização associada a um ideal $\mathfrak{P}$ de $\mathcal{O}_\mathbb{L}$ se $v : \mathbb{K}^* \longrightarrow \mathbb{Z}$ é dada por $v(x) = k$, onde k é a potência de $\mathfrak{P}$ na fatoração de $x\mathcal{O}_\mathbb{L}$ em $\mathcal{O}_\mathbb{L}$.*

Observação 2.9 *Pela Proposição 2.3 tem-se que se $x\mathcal{O}_\mathbb{L} \subseteq y\mathcal{O}_\mathbb{L}$, então $v(x) \geq v(y)$.*

2.7 Considerações finais

Neste capítulo foi desenvolvido a teoria da ramificação, a principal teoria para a demonstração do Teorema de Kronecker-Weber. Os resultados da Seção 2.4.2 são pré-requisitos essenciais, apresentados pela principal referência deste trabalho [1], para a compreensão das argumentações usadas na demonstração do Teorema dde Kronecker-Weber.

Capítulo 3

Teorema de Kronecker-Weber

O Teorema Kronecker-Weber é importante na teoria algébrica dos números, pois equivale o estudo de corpos de números abelianos ao estudo de subcorpos de corpos ciclotômicos. Deste modo, o principal resultado deste capítulo é o teorema de Kronecker-Weber juntamente com sua demonstração que faz uso de resultados sobre ramificação de ideais. As principais referências desta seção são [1], [4], [9] e [10].

3.1 Preliminares

Esta seção traz alguns resultados preliminares a demonstração do Teorema de Kronecker-Weber.

Observação 3.1 *Lembramos que os ideais primos* $\mathfrak{p}$ *de* $\mathbb{Z}$ *são ideais gerados por números primos* p *de* $\mathbb{Z}$*. Assim, para simplificar a notação quando nos referirmos a um ideal primo de* $\mathbb{Z}$ *nos referiremos a um número* p *primo de* $\mathbb{Z}$*.*

Lema 3.1 *Se* $\mathbb{K}$ *e* $\mathbb{L}$ *são extensões de Galois de* $\mathbb{Q}$ *e* q *é um primo que não se ramifica em* $\mathbb{K}|\mathbb{Q}$ *e* $\mathbb{L}|\mathbb{Q}$*, então* q *não se ramifica em* $\mathbb{KL}|\mathbb{Q}$*.*

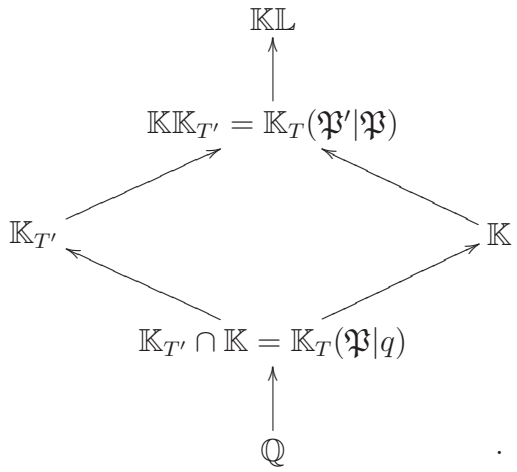
Demonstração. Sejam $\mathfrak{P}$ um ideal primo de $\mathcal{O}_{\mathbb{KL}}$ acima de q, $T = T(\mathfrak{P}|q)$, $T' = T(\mathfrak{P} \cap \mathcal{O}_{\mathbb{K}}|q)$ e $T'' = T(\mathfrak{P} \cap \mathcal{O}_{\mathbb{L}}|q)$. Se $\sigma \in T \cap Gal(\mathbb{KL}|\mathbb{K} \cap \mathbb{L})$, então $\sigma|_{\mathbb{K}} \in T'$ e $\sigma|_{\mathbb{L}} \in T''$. Como q não se ramifica em $\mathbb{K}$ e em $\mathbb{L}$, segue que $[\mathbb{K} : \mathbb{K}_{T'}] = [\mathbb{L} : \mathbb{K}_{T''}] = 1$, ou seja, T' e

T'' são triviais. Assim, σ é igual a identidade. Deste modo, q não ramifica em $\mathbb{KL}|\mathbb{K}\cap\mathbb{L}$ e por hipótese q não se ramifica em $\mathbb{K}\cap\mathbb{L}|\mathbb{Q}$. Portanto, q não ramifica em $\mathbb{KL}|\mathbb{Q}$. ■

Lema 3.2 *Se o Teorema de Kronecker-Weber é válido para extensões abelianas de $\mathbb{Q}$ de grau p^m, com p primo, $m \in \mathbb{N}$ e p o único primo que se ramifica, então o Teorema de Kronecker-Weber é válido para extensões abelianas de $\mathbb{Q}$ de grau p^m, com p primo e $m \in \mathbb{N}$.*

Demonstração. De fato, seja $\mathbb{K}$ é uma extensão abeliana de $\mathbb{Q}$ de grau p^m, com p primo e $m \in \mathbb{N}$. Suponhamos que existe q primo tal que $q \neq p$ e q se ramifica em $\mathcal{O}_{\mathbb{K}}$. Assim, existe um ideal primo $\mathfrak{P}$ de $\mathcal{O}_{\mathbb{K}}$ que está acima de q. Seja T o grupo de inércia de $\mathfrak{P}$ e V_j os j-ésimos grupos de ramificação de $\mathfrak{P}$, para $j \geq 1$. Como $G = Gal(\mathbb{K}|\mathbb{Q})$ tem ordem p^m e q não divide p^m, segue que não existe subgrupo de G de ordem q. Como $\dfrac{V_j}{V_{j+1}}$ é isomorfo a um subgrupo do grupo aditivo $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{P}}$, o qual tem ordem q^f (Proposição 2.14), segue que os grupos de ramificação de $\mathfrak{P}$ são triviais, para $j \geq 1$. Além disso, o grupo de inércia T de $\mathfrak{P}$ tem ordem p^u, para $1 \leq u \leq m$, pois é um subgrupo de G. Assim, pela Proposição 2.27, segue que $p^u|(q-1)$. Agora, notemos que $\mathbb{Q}(\zeta_q)$ é ciclíco e tem grau $q-1$ sobre $\mathbb{Q}$, e como $p^u|(q-1)$, segue que existe um único corpo $\mathbb{L}$ tal que $\mathbb{Q} \subseteq \mathbb{L} \subseteq \mathbb{Q}(\zeta_q)$ e $\mathbb{L}$ tem grau p^u sobre $\mathbb{Q}$, ou seja, existe um único subgrupo de $Gal(\mathbb{Q}(\zeta_q)|\mathbb{Q})$ de índice p^u. Pelo Teorema 1.18, segue que $D_{\mathbb{Q}(\zeta_q)}$ é uma potência de q. Assim, q é o único primo que se ramifica em $\mathcal{O}_{\mathbb{Q}(\zeta_q)}$ e se ramifica totalmente (Teorema 2.9). Como $q-1 = e(\mathfrak{P}|q) = e(\mathfrak{P}|\mathfrak{P}\cap\mathcal{O}_{\mathbb{L}})e(\mathfrak{P}\cap\mathcal{O}_{\mathbb{L}}|q)$ e $e(\mathfrak{P}|\mathfrak{P}\cap\mathcal{O}_{\mathbb{L}}) = |Z(\mathfrak{P}|\mathfrak{P}\cap\mathcal{O}_{\mathbb{L}})| = |Z(\mathfrak{P}|\mathfrak{q})\cap Gal(\mathbb{Q}(\zeta_q)|\mathbb{L})| = |Gal(\mathbb{Q}(\zeta_q)|\mathbb{Q})\cap Gal(\mathbb{Q}(\zeta_q)|\mathbb{L})| = |Gal(\mathbb{Q}(\zeta_q)|\mathbb{L})| = \dfrac{q-1}{p^u}$, segue que $e(\mathfrak{P}\cap\mathcal{O}_{\mathbb{L}}|q) = p^u = [\mathbb{L}:\mathbb{Q}]$, ou seja, q se ramifica totalmente em $\mathcal{O}_{\mathbb{L}}$. Consideramos a extensão composição $\mathbb{KL}$ de $\mathbb{Q}$. Como $\mathbb{K}|\mathbb{Q}$ e $\mathbb{L}|\mathbb{Q}$ são extensões de Galois, segue pelo Teorema 1.11 que $\mathbb{KL}|\mathbb{Q}$ é de Galois e $[\mathbb{KL}:\mathbb{Q}] = p^{m+v}$, com $v \leq u$. Consideramos $\mathfrak{P}'$ o ideal primo de $\mathcal{O}_{\mathbb{KL}}$ acima de $\mathfrak{P}$, T' o grupo de inércia de $\mathfrak{P}'$ e $H = Gal(\mathbb{L}|\mathbb{Q})$. Notemos que se $\sigma \in T'$, então σ é um $\mathbb{Q}$-automorfismo de $\mathbb{KL}$ tal que $\sigma(\alpha) \equiv \alpha (mod\ \mathfrak{P}')$, para todo $\alpha \in \mathcal{O}_{\mathbb{KL}}$, e assim, restringindo σ a $\mathbb{K}$, tem-se que $\sigma \in T$, pois $\mathfrak{P}'\cap\mathcal{O}_{\mathbb{K}} = \mathfrak{P}$. Assim, pelo Teorema 1.11, segue que $T' \leq T \times H$. Seja $\mathbb{K}_{T'}$ o corpo fixo de T'. Logo, pelo Teorema 2.10, segue que q não ramifica em $\mathcal{O}_{\mathbb{K}_{T'}}$. Agora, pelo item (b) da Proposição 2.22, tem-se

o seguinte diagrama



Observamos que $\mathbb{K}_T(\mathfrak{P}|q)$ é o corpo fixo de T. Assim, pelo Teorema 1.9, segue que $|T| = [\mathbb{K} : \mathbb{K}_T(\mathfrak{P}|q)] = p^u = [\mathbb{K}\mathbb{K}_{T'} : \mathbb{K}_{T'}]$. Logo, $|T'| = [\mathbb{K}\mathbb{L} : \mathbb{K}_{T'}] \geq p^u$. Pelo mesmo argumento, segue que os grupos de ramificação de $\mathfrak{P}'$ são tiviais, e assim, pela Proposição 2.27, segue que T' é ciclíco e como qualquer elemento de $T \times H$ tem ordem no máximo p^u, segue que $|T'| = p^u$. Se substituirmos $\mathbb{K}$ por $\mathbb{L}$ no diagrama e observando que q se ramifica totalmente em $\mathcal{O}_{\mathbb{L}}$, segue que $\mathbb{K}_{T'} \cap \mathbb{L} = \mathbb{Q}$, pois o grupo de inércia de qualquer ideal primo de $\mathcal{O}_{\mathbb{L}}$ acima de q é igual a $Gal(\mathbb{L}|\mathbb{Q})$. Observamos que $[\mathbb{K}\mathbb{L} : \mathbb{K}_{T'}] = [\mathbb{K}\mathbb{L} : \mathbb{K}_{T'}\mathbb{L}][\mathbb{K}_{T'}\mathbb{L} : \mathbb{K}_{T'}] = [\mathbb{K}\mathbb{L} : \mathbb{K}_{T'}\mathbb{L}][\mathbb{L} : \mathbb{Q}] = [\mathbb{K}\mathbb{L} : \mathbb{K}_{T'}\mathbb{L}]p^u$. Logo, $\mathbb{K}\mathbb{L} = \mathbb{K}_{T'}\mathbb{L}$. Assim, $\mathbb{K}$ está contido em um corpo ciclotômico se, e somente se, $\mathbb{K}_{T'}$ está contido em um corpo ciclotômico. Como q não se ramifica em $\mathcal{O}_{\mathbb{K}_{T'}}$, segue que somente p se ramifica em $\mathcal{O}_{\mathbb{K}_{T'}}$, e assim, $\mathbb{K}_{T'}$ está contido em um corpo ciclotômico. ■

Corolário 3.1 *Seja $\mathbb{K}$ uma extensão abeliana de $\mathbb{Q}$ de grau p^m, com p primo e $m \in \mathbb{N}$. Se $q \neq p$ é o único primo que se ramifica em $\mathcal{O}_{\mathbb{K}}$, então q se ramifica totalmente, $q \equiv 1 \ (mod\ p^m)$ e $\mathbb{K}$ é o único subcorpo de $\mathbb{Q}(\zeta_q)$ de grau p^m sobre $\mathbb{Q}$. Além disso, $\mathbb{K}|\mathbb{Q}$ é ciclíca.*

Demonstração. Se $q \neq p$ é o único primo que se ramifica em $\mathcal{O}_{\mathbb{K}}$, então pelo Lema 3.2 o corpo $\mathbb{K}_{T'}$ (construído na demonstração do Lema 3.2) é igual a $\mathbb{Q}$ (teorema de Minkowski). Assim, $\mathbb{K} = \mathbb{L}$, onde $\mathbb{L}$ é o único subcorpo de $\mathbb{Q}(\zeta_q)$ de grau p^m sobre $\mathbb{Q}$ tal que $q \equiv 1 \ (mod\ p^m)$. ■

Corolário 3.2 *Se $\mathbb{K}$ é uma extensão abeliana de $\mathbb{Q}$ de grau um número primo ímpar, então 2 não se ramifica.*

Demonstração. Suponhamos que 2 se ramifica em $\mathcal{O}_{\mathbb{K}}$. Seja $\mathfrak{P}$ o ideal de $\mathcal{O}_{\mathbb{K}}$ acima de 2. Como $G = Gal(\mathbb{K}|\mathbb{Q})$ tem ordem p, primo ímpar, e 2 não divide p, segue que não existe subgrupo de G de ordem 2. Além disso, $\dfrac{V_j}{V_{j+1}}$ é isomorfo a um subgrupo do grupo aditivo $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{P}}$, o qual tem ordem 2^f. Assim, os grupos de ramificação de $\mathfrak{P}$ são triviais, para $j \geq 1$. Deste modo, T é trivial (Proposição 2.27). Portanto, 2 não se ramifica em $\mathbb{K}$. ■

Lema 3.3 *Se $\mathbb{K}$ é uma extensão abeliana de $\mathbb{Q}$ de grau p, com p primo ímpar e o único que se ramifica, então V_2 é trivial.*

Demonstração. Sejam $\mathfrak{P}$ um ideal primo de $\mathcal{O}_{\mathbb{K}}$ acima de p e T o grupo de inércia de $\mathfrak{P}$. Como p é o único primo que se ramifica em $\mathcal{O}_{\mathbb{K}}$ e p não se ramifica em $\mathcal{O}_{\mathbb{K}_T}$, onde $\mathbb{K}_T$ é o corpo fixo de T, segue pelo Teorema de Minkowski, que $\mathbb{K}_T = \mathbb{Q}$, ou seja, $T = Gal(\mathbb{K}|\mathbb{Q})$. Assim, p se ramifica totalmente em $\mathcal{O}_{\mathbb{K}}$. Logo, pela Proposição 2.14, segue que $\#\left(\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{P}}\right) = p$ e $f = 1$. Como, $p^n \nmid (p-1)$, para qualquer n inteiro positivo, e como a ordem de $\dfrac{T}{V_1}$ é uma potência de p que divide $p-1$, segue que $V_1 = T$, ou seja, $n = 0$. Usando o processo de localização, ou seja, tomando $S = \mathbb{Z} - p\mathbb{Z}$ e omitindo as notações de anéis de frações, podemos supor $\mathcal{O}_{\mathbb{K}}$ um domínio de Dedekind principal, e assim, $\mathfrak{P} = \langle b \rangle$, com $b \in \mathcal{O}_{\mathbb{K}}$. Suponhamos que j é o menor inteiro positivo tal que V_{j+1} é trivial. Assim, $V_j = Gal(\mathbb{K}|\mathbb{Q})$, pois $\dfrac{V_j}{V_{j+1}} = V_j$ é isomorfo a um subgrupo do grupo aditivo $\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{P}}$, o qual tem ordem p e pelo fato de p ser primo, segue que $V_j = Gal(\mathbb{K}|\mathbb{Q})$. Consideramos v a valorização de $\mathbb{K}$ associada a $\mathfrak{P}$ e $f(x) = min_{\mathbb{Q}} b = \prod_{\sigma \in G}(x - \sigma(b))$. Notemos que $f'(x) = \sum_{i=1}^{p} \prod_{j=1, j\neq 1}^{p} (x - \sigma_j(b))$ e $f'(b) = \prod_{\sigma \in G, \sigma \neq id} (b - \sigma(b)) = \prod_{\sigma \in V_j - V_{j+1}} (b - \sigma(b))$, pois $V_{j+1} = \{id\}$ e $V_j = G$. Como $\sigma \in V_j$, segue que $\sigma(b) \equiv b (mod\ \mathfrak{P}^{j+1})$, e assim, $v(b - \sigma(b)) = j + 1$. Assim,

$$v(f'(b)) = v\left(\prod_{\sigma \in G, \sigma \neq id} (b - \sigma(b))\right) = \sum_{\sigma \in G, \sigma \neq id} v(b - \sigma(b)) = (j+1)(p-1). \qquad (3.1)$$

Por outro lado, como $f(x) = x^p + a_{p-1}x^{p-1} + \ldots + a_1x + a_0$, com $a_i \in \mathbb{Z}$, segue que $f'(b) = pb^{p-1} + a_{p-1}(p-1)b^{p-2} + \ldots + a_1$, com $a_i \in \mathbb{Z}$. Pelo fato de que p se ramifica totalmente em $\mathcal{O}_{\mathbb{K}}$, segue que $v(p) = p$. Como $a_i \in \mathbb{Z}$, podemos considerar a fatoração de a_i em primos, e assim, $v(a_i) = v(\prod p_i^{m_i}) = \sum m_i v(p_i) = mp$, pois estamos no processo de localização, e assim $v(p_i) = 0$, para todo $p_i \neq p$. Logo, $v(a_i) \equiv 0(mod\ p)$. Assim, $v(f'(b)) \geq min\{v(pb^{p-1}), v(a_{p-1}(p-1)b^{p-2}), \ldots, v(a_1)\}$. Notemos que para $k \in \{0, 1, \ldots, p-1\}$, tem-se que $v(a_{p-k}(p-k)b^{p-(k+1)}) = v(a_{p-k}) + v(p-k) + v(b^{p-(k+1)})$. Reduzindo $mod\ p$, tem-se que $v(a_{p-k}(p-k)b^{p-(k+1)}) \equiv p - (k+1)(mod\ p)$, pois $v(a_{p-k}) \equiv 0(mod\ p)$, o mesmo ocorre com $v(k)$, o que torna $v(p-k) \equiv 0(mod\ p)$. Portanto, as valorizações dos termos envolvendo $b^{p-(k+1)}$ são diferentes, e assim, $v(f'(b)) = min\{v(pb^{p-1}), v(a_{p-1}(p-1)b^{p-2}), \ldots, v(a_1)\}$. Como $v(pb^{p-1}) = v(p) + (p-1)v(b) = 2p-1$, segue que

$$v(f'(b)) \leq 2p - 1. \tag{3.2}$$

Considerando as Equações (3.1) e (3.2), tem-se que $(j+1)(p-1) \leq 2p-1$. Como p é primo ímpar, segue que 1 é o único inteiro $j \geq 1$ tal que $(j+1)(p-1) \leq 2p-1$. Portanto, V_2 é trivial. ■

Lema 3.4 *Se $\mathbb{K}$ é uma extensão abeliana de $\mathbb{Q}$ de grau p^m, com p primo ímpar, $m \in \mathbb{N}$ e p o único primo que se ramifica em $\mathcal{O}_{\mathbb{K}}$, então $\mathbb{K}|\mathbb{Q}$ é ciclíca.*

Demonstração. Sejam $\mathfrak{P}$ ideal primo não nulo de $\mathcal{O}_{\mathbb{K}}$ acima de p, $T = T(\mathfrak{P}|p)$ o grupo de inércia de $\mathfrak{P}$ sobre p e $\mathbb{K}_T$ o corpo fixo de T. Como p é o único que se ramifica em $\mathcal{O}_{\mathbb{K}}$ e não se ramifica em $\mathbb{K}_T$, segue que $\mathbb{K}_T = \mathbb{Q}$. Assim, $[\mathbb{K} : \mathbb{Q}] = p^m = e(\mathfrak{P}|p) = [\mathbb{K} : \mathbb{K}_T]$, ou seja, p se ramifica totalmente. Logo, $T = Gal(\mathbb{K}|\mathbb{Q})$. Como $\dfrac{T}{V_1}$ é ciclíco de ordem dividindo $p-1$ e também tem ordem uma potência de p, segue que $\dfrac{T}{V_1}$ é trivial, ou seja, $T = V_1$. Além disso, $\dfrac{V_j}{V_{j+1}}$ são ou triviais ou ciclícos de ordem p, pois são isomorfos a um subgrupo do grupo aditivo $\left(\dfrac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{P}}, +\right)$ o qual é ciclíco de ordem p. Suponhamos que j seja o maior inteiro tal que $V_j = Gal(\mathbb{K}|\mathbb{Q})$ e $V_{j+1} \subsetneq V_j$. Neste caso, $\dfrac{V_j}{V_{j+1}}$ é ciclíco de ordem p, ou seja, $[\mathbb{K}_{V_{j+1}} : \mathbb{Q}] = p$. Para mostrar que $G = Gal(\mathbb{K}|\mathbb{Q})$ é ciclíco, mostramos que G tem um único subgrupo de índice p, que é V_{j+1}. De fato, suponhamos que existe um subgrupo

H de G de índice p e diferente de V_{j+1}. Consideramos $\mathfrak{P}_H = \mathfrak{P} \cap \mathcal{O}_H$, $\mathfrak{P}_{V_{j+1}} = \mathfrak{P} \cap \mathcal{O}_{V_{j+1}}$. Observamos que $Gal(\mathbb{K}|\mathbb{K}_H) = H$, $Gal(\mathbb{K}|\mathbb{K}_{V_{j+1}}) = V_{j+1}$ e $G = T = V_1 = \ldots = V_j \supsetneq V_{j+1} \supseteq \ldots$, e assim,

$$V_i' = V_i(\mathfrak{P}|\mathfrak{P}_{V_{j+1}}) = \begin{cases} V_i \cap V_{j+1} = V_{j+1}, & \text{se } 0 \leq i \leq j+1 \\ V_i \cap V_{j+1} = V_i, & \text{se } i > j+1 \end{cases}$$

$$V_i'' = V_i(\mathfrak{P}|\mathfrak{P}_H) = \begin{cases} V_i \cap H = H, & \text{se } 0 \leq i < j \\ V_i \cap H \subsetneq V_{j+1}, & \text{se } i \geq j+1 \end{cases},$$

pois $H \neq V_{j+1}$. Consideremos os diferentes $\Delta_{\mathbb{K}|\mathbb{K}_H}$ e $\Delta_{\mathbb{K}|\mathbb{K}_{V_{j+1}}}$, os quais são ideais de $\mathcal{O}_{\mathbb{K}}$. Aplicando o processo de localização, ou seja, tomando $S = \mathbb{Z} - p\mathbb{Z}$, tem-se que $\Delta_{\mathbb{K}|\mathbb{K}_H} S^{-1}\mathcal{O}_{\mathbb{K}} = \Delta_p(\mathbb{K}|\mathbb{K}_H) = S^{-1}\mathcal{O}_{\mathbb{K}} f'(\alpha)^{(\sum_{i\geq 0}(\#V_i'-1))}$ e $\Delta_{\mathbb{K}|\mathbb{K}_{V_{j+1}}} S^{-1}\mathcal{O}_{\mathbb{K}} = \Delta_p(\mathbb{K}|\mathbb{K}_{V_{j+1}}) = S^{-1}\mathcal{O}_{\mathbb{K}} f'(\alpha)^{(\sum_{i\geq 0}(\#V_i''-1))}$, onde $\mathfrak{P} = \langle \alpha \rangle$ e $f(x) = min_{\mathbb{Q}}\alpha$. Como $f'(\alpha) \in \mathfrak{P}$, segue que $e(\mathfrak{P}|\Delta_{\mathbb{K}|\mathbb{K}_H}) = \sum_{i\geq 0}(\#V_i' - 1)$ e $e(\mathfrak{P}|\Delta_{\mathbb{K}|\mathbb{K}_{V_{j+1}}}) = \sum_{i\geq 0}(\#V_i'' - 1)$. Notamos que

$$\sum_{i\geq 0}(\#V_i' - 1) < \sum_{i\geq 0}(\#V_i'' - 1), \tag{3.3}$$

pois para $i < j$ vale a igualdade, para $i = j+1$ vale $<$ e para $i > j+1$ vale $\leq$. Pelo Lema 3.3, tem-se que o segundo grupo de ramificação das extensões $\mathbb{K}_H|\mathbb{Q}$ e $\mathbb{K}_{V_{j+1}}|\mathbb{Q}$ saõ triviais. De modo análogo ao anterior, tem-se que $e(\mathfrak{P}_H|\Delta_{\mathbb{K}_H}) = \sum_{i\geq 0}(\#\overline{V_i} - 1)$ e $e(\mathfrak{P}_{V_{j+1}}|\Delta_{\mathbb{K}_{V_{j+1}}}) = \sum_{i\geq 0}(\#\overline{\overline{V_i}} - 1)$, onde $\overline{V_i}$ e $\overline{\overline{V_i}}$ são os i-ésimos grupos de ramificação de $\mathbb{K}_H|\mathbb{Q}$ e $\mathbb{K}_{V_{j+1}}|\mathbb{Q}$ respectivamente. Assim,

$$e(\mathfrak{P}_H|\Delta_{K_H}) = p - 1 + p - 1 = 2(p-1) = e(\mathfrak{P}_{V_{j+1}}|\Delta_{\mathbb{K}_{V_{j+1}}}) \tag{3.4}$$

Agora, pela transitividade do diferente, ou seja,

$$\Delta_{\mathbb{K}} = \mathcal{O}_{\mathbb{K}}\Delta_{\mathbb{K}_H}\Delta_{\mathbb{K}|\mathbb{K}_H} = \mathcal{O}_{\mathbb{K}}\Delta_{\mathbb{K}_{V_{j+1}}}\Delta_{\mathbb{K}|\mathbb{K}_{V_{j=1}}},$$

e por 3.3 e 3.4 tem-se uma contradição. Portanto, $V_{j+1} = H$, e consequêntemente, $Gal(\mathbb{K}|\mathbb{Q})$ é ciclíco. ■

3.2 Teorema de Kronecker-Weber

Esta seção tem como objetivo demonstrar o Teorema de Kronecker-Weber, onde a demonstração é feita para extensões ciclícas de grau potência de um primo, pois pelo Corolário 1.6 se $G = Gal(\mathbb{K}|\mathbb{Q})$ é abeliano finito, então $G = \prod_{i=1}^{r} G_i$, onde os G_i's são ciclícos e $|G_i| = p_i^{m_i}$, com p_i primo, para $1 \leq i \leq r$. Assim, se mostrarmos que cada extensão $\mathbb{K}_i$ de $\mathbb{Q}$, com grupo de Galois G_i, está contida em um corpo ciclotômico $\mathbb{Q}(\zeta_{n_i})$, então o Teorema de Kronecker-Weber segue facilmente.

Proposição 3.1 *Se $\mathbb{K}$ é uma extensão abeliana de $\mathbb{Q}$ de grau p^m, com p primo ímpar e $m \in \mathbb{N}$, então $\mathbb{K}$ está contido em um corpo ciclotômico.*

Demonstração. Tem-se que existe um número finito de primos que se ramificam na extensão $\mathbb{K}|\mathbb{Q}$ e pelo Lema 3.1, podemos supor que p é o único primo que se ramifica na extensão $\mathbb{K}|\mathbb{Q}$. Assim, pelo Lema 3.4, $\mathbb{K}|\mathbb{Q}$ é ciclíca. Consideramos $\zeta_{p^{m+1}}$ uma raiz p^{m+1}-ésima primitiva da unidade. Como a extensão $\mathbb{Q}(\zeta_{p^{m+1}})|\mathbb{Q}$ é ciclíca de grau $p^m(p-1)$, segue que existe um único subcorpo $\mathbb{K}'$ de $\mathbb{Q}(\zeta_{p^{m+1}})$ de grau p^m sobre $\mathbb{Q}$. Pelo Teorema 1.20, tem-se que p é o único primo que se ramifica em $\mathbb{Q}(\zeta_{p^{m+1}})$ e como $\mathbb{Q} \subsetneq \mathbb{K}'$, segue, pelo Teorema 2.7, que p é o único primo que se ramifica em $\mathbb{K}'$. Suponhamos que $\mathbb{K}$ é diferente de $\mathbb{K}'$. Assim, pelo Teorema 1.10, segue que a extensão composição $\mathbb{K}\mathbb{K}'$ de $\mathbb{Q}$ é uma extensão de Galois. Além disso, como $\mathbb{K}|\mathbb{Q}$ e $\mathbb{K}'|\mathbb{Q}$ são extensões abelianos, segue que $\mathbb{K}\mathbb{K}'|\mathbb{Q}$ é uma extensão abeliana, e que $Gal(\mathbb{K}\mathbb{K}'|\mathbb{Q}) \leq Gal(\mathbb{K}|\mathbb{Q}) \times Gal(\mathbb{K}'|\mathbb{Q})$ (Teorema 1.11). Logo, pelo Lema 3.1, p é o único primo que se ramifica em $\mathcal{O}_{\mathbb{K}\mathbb{K}'}$. Observamos que $[\mathbb{K}\mathbb{K}' : \mathbb{K}'] = [\mathbb{K} : \mathbb{K} \cap \mathbb{K}'] = p^k$ (Teorema 1.9), com $0 \leq k \leq m$. Se $k = 0$, então $\mathbb{K} \subseteq \mathbb{K}'$, e portanto, $\mathbb{K}$ está contido em um corpo ciclotômico. Se $1 \leq k \leq m$, então $[\mathbb{K}\mathbb{K}' : \mathbb{Q}] = p^{m+k} > p^m$. Assim, pelo Lema 3.4, segue que $\mathbb{K}\mathbb{K}'|\mathbb{Q}$ é ciclíca, ou seja, o grupo de Galois é gerado por um elemento de ordem p^{m+k}. Porém, como $Gal(\mathbb{K}\mathbb{K}'|\mathbb{Q}) \leq Gal(\mathbb{K}|\mathbb{Q}) \times Gal(\mathbb{K}'|\mathbb{Q})$ (Teorema 1.11), segue que não existe elemento no grupo $Gal(\mathbb{K}\mathbb{K}'|\mathbb{Q})$ com ordem maior que p^m. Portanto, $\mathbb{K} = \mathbb{K}'$. ■

Proposição 3.2 *Se $\mathbb{K}$ é uma extensão quadrática de $\mathbb{Q}$, então $\mathbb{K}$ está contido em um corpo ciclotômico.*

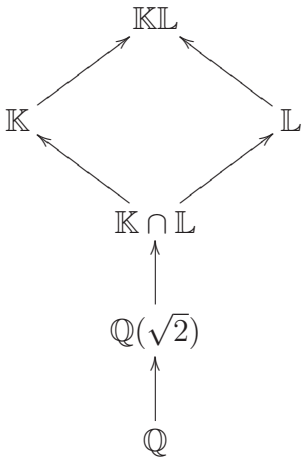
Demonstração. De fato, pela Observação 1.4, tem-se que $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com $d \in \mathbb{Z}$ livre de quadrados. Pelo Lema 3.2, podemos supor que 2 é o único primo que se ramificada em $\mathcal{O}_{\mathbb{K}}$. Assim, pelo Exemplo 2.4, segue que $d = \pm 2$ ou $d = -1$. Portanto, $\mathbb{K} = \mathbb{Q}(\sqrt{\pm 2}) \subseteq \mathbb{Q}(\zeta_8)$ ou $\mathbb{K} = \mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$. ■

Observação 3.2 *Notamos que* $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\zeta_8 + \zeta_8^{-1})$, $\mathbb{Q}(\sqrt{-2}) = \mathbb{Q}(\zeta_8 - \zeta_8^{-1})$ *e* $\mathbb{Q}(i) = \mathbb{Q}(\zeta_8^2) = \mathbb{Q}(\zeta_4)$.

Proposição 3.3 *Se* $\mathbb{K}$ *é uma extensão ciclíca de* $\mathbb{Q}$ *de grau* 2^m*, com* $m \geq 1$*, então* $\mathbb{K}$ *está contido em um corpo ciclotômico.*

Demonstração. Mostramos a proposição por indução sobre m. Se $m = 1$, então o resultado é válido pela Proposição 3.2. Suponhamos o resultado válido para todo $r < m$ e provamos para m. Podemos supor que 2 é o único primo que se ramifica em $\mathcal{O}_{\mathbb{K}}$. Como $\mathbb{K}|\mathbb{Q}$ é ciclíca, segue que existe um único subcorpo $\mathbb{K}'$ de grau 2 sobre $\mathbb{Q}$ em que 2 é o único primo que se ramifica. Se $\mathbb{K} \subseteq \mathbb{R}$, então $\mathbb{K}' = \mathbb{Q}(\sqrt{2})$. Caso contrário, consideramos σ a conjugação complexa. Tem-se que $\sigma|_{\mathbb{K}}$ gera um subgrupo J de $Gal(\mathbb{K}|\mathbb{Q})$ de ordem 2, ou seja, $[\mathbb{K} : \mathbb{K}_J] = 2^{m-1}$, onde $\mathbb{K}_J$ é o corpo fixo de J. Como $\mathbb{K}_J = \{x \in \mathbb{K}; \sigma(x) = x, \text{ para todo } \sigma \in J\}$, segue que $\mathbb{K}_J \subseteq \mathbb{R}$. Pelo fato de $\mathbb{K}|\mathbb{Q}$ ser ciclíca, tem-se que $\mathbb{K}_J|\mathbb{Q}$ também é ciclíca e de grau 2^{m-1}. Logo, existe um único subcorpo $\mathbb{K}' \subseteq \mathbb{K}_J$ tal que $[\mathbb{K}' : \mathbb{Q}] = 2$ e 2 é o único primo que se ramifica. Portanto, $\mathbb{K}' = \mathbb{Q}(\sqrt{2})$. Agora, consideramos ζ uma raiz 2^{m+2}-ésima primitiva da unidade e $\mathbb{L} = \mathbb{Q}(\zeta + \zeta^{-1})$ o corpo real maximal de $\mathbb{Q}(\zeta)$, o qual tem ordem 2^m sobre $\mathbb{Q}$. Provamos que $\mathbb{L}|\mathbb{Q}$ é ciclíca. De fato, o grupo $Gal(\mathbb{Q}(\zeta)|\mathbb{Q}) \simeq Gal(\mathbb{Q}(\zeta)|\mathbb{L}) \times G_2$, onde G_2 é um grupo ciclíco de ordem 2^m. Logo, $Gal(\mathbb{L}|\mathbb{Q}) \simeq \dfrac{Gal(\mathbb{Q}(\zeta)|\mathbb{Q})}{Gal(\mathbb{Q}(\zeta)|\mathbb{L})} \simeq G_2$. Portanto, $\mathbb{L}|\mathbb{Q}$ é ciclíca de grau 2^m, onde 2 é o único primo que se ramifica e pelo argumento anterior $\mathbb{Q}(\sqrt{2}) \subset \mathbb{L}$. Deste modo, $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{K} \cap \mathbb{L}$, ou seja, $[\mathbb{K} \cap \mathbb{L} : \mathbb{Q}] \geq 2$. Notemos que

$[\mathbb{KL} : \mathbb{Q}] = [\mathbb{KL} : \mathbb{L}][\mathbb{L} : \mathbb{Q}] = [\mathbb{K} : \mathbb{K} \cap \mathbb{L}][\mathbb{L} : \mathbb{Q}] = 2^r 2^m = 2^{r+m}$, onde $0 \leq r < m$.



Tem-se que $Gal(\mathbb{KL}|\mathbb{Q}) \lneq Gal(\mathbb{K}|\mathbb{Q}) \times Gal(\mathbb{L}|\mathbb{Q})$ e existem $(\sigma, \tau) \in Gal(\mathbb{K}|\mathbb{Q}) \times Gal(\mathbb{L}|\mathbb{Q})$ tal que $\sigma|_{\mathbb{K}\cap\mathbb{L}} = \tau|_{\mathbb{K}\cap\mathbb{L}}$. Agora, consideramos H o subgrupo de $Gal(\mathbb{KL}|\mathbb{Q})$ gerado por (σ, τ), o qual tem ordem 2^m, e assim, se $\mathbb{F}$ é o corpo fixo de H, tem-se que $[\mathbb{F} : \mathbb{Q}] = \dfrac{[\mathbb{KL} : \mathbb{Q}]}{[\mathbb{KL} : \mathbb{F}]} = \dfrac{2^{r+m}}{2^m} = 2^r$. Provamos agora que $\mathbb{F}|\mathbb{Q}$ é ciclíca. De fato, tem-se que $Gal(\mathbb{F}|\mathbb{Q}) \simeq \dfrac{Gal(\mathbb{KL}|\mathbb{Q})}{Gal(\mathbb{KL}|\mathbb{F})}$. Logo, existe um homomorfismo injetor entre $\dfrac{Gal(\mathbb{KL}|\mathbb{Q})}{H}$ e $\dfrac{Gal(\mathbb{K}|\mathbb{Q}) \times Gal(\mathbb{L}|\mathbb{Q})}{H}$. Tem-se que $\dfrac{Gal(\mathbb{K}|\mathbb{Q}) \times Gal(\mathbb{L}|\mathbb{Q})}{H}$ é ciclíco gerado por $(id, \tau)H$, pois dado qualquer elemento $(\sigma^k, \tau^l)H$ em $\dfrac{Gal(\mathbb{K}|\mathbb{Q}) \times Gal(\mathbb{L}|\mathbb{Q})}{H}$, tem-se que $(\sigma^k, \tau^l)H = (id, \tau^j)H \Leftrightarrow (\sigma^k, \tau^l)(id, \tau^j) \in H \Leftrightarrow k = l - j \Leftrightarrow j = l - k$. Portanto, existe $j = l - k$ tal que $(\sigma^k, \tau^l)H = (id, \tau^j)H$, ou seja $(id, \tau)H$ gera $\dfrac{Gal(\mathbb{K}|\mathbb{Q}) \times Gal(\mathbb{L}|\mathbb{Q})}{H}$. Assim, $Gal(\mathbb{F}|\mathbb{Q})$ é ciclíco. Deste modo, podemos aplicar a hipótese de indução sobre $\mathbb{F}$. Como $\mathbb{F} \subseteq \mathbb{KL}$, segue que $\mathbb{FL} \subseteq \mathbb{KL}$. Mostramos que $\mathbb{F} \cap \mathbb{L} = \mathbb{Q}$. Para isto consideramos o isomorfismo $\Phi : H \longrightarrow Gal(\mathbb{L}|\mathbb{Q})$ dado por $\Phi(\sigma^k, \tau^k) = \tau^k|_{\mathbb{L}}$. Seja $m \in \mathbb{F} \cap \mathbb{L}$. Se $\tau_1 \in Gal(\mathbb{L}|\mathbb{Q})$, então existe $(\sigma_2, \tau_2) \in H$ tal que $\tau_2|_{\mathbb{L}} = \tau_1$. Assim, $\tau_1(m) = \tau_2|_{\mathbb{L}}(m) = m$, pois $\mathbb{F}$ é o corpo fixo de H. Logo, $\tau_1|_{\mathbb{F}\cap\mathbb{L}} = id$, para qualquer $\tau_1 \in Gal(\mathbb{L}|\mathbb{Q})$, e assim, $\mathbb{F} \cap \mathbb{L} = \mathbb{Q}$. Portanto, $[\mathbb{FL} : \mathbb{F}] = [\mathbb{L} : \mathbb{F} \cap \mathbb{L}] = [\mathbb{L} : \mathbb{Q}] = 2^m = [\mathbb{KL} : \mathbb{F}]$ e $\mathbb{FL} \subseteq \mathbb{KL}$ o que implica que $\mathbb{FL} = \mathbb{KL}$. Portanto, $\mathbb{K}$ está contido em um corpo ciclotômico. ■

Lema 3.5 *Se $\mathbb{K}|\mathbb{Q}$ é abeliana de grau 2^m e $\mathbb{K} \subseteq \mathbb{R}$, então $\mathbb{K} = \mathbb{Q}(\zeta + \zeta^{-1})$, onde ζ é uma raiz 2^{m+2}-ésima primitiva da unidade.*

Demonstração. Denotamos por $\mathbb{L}$ a extensão $\mathbb{Q}(\zeta + \zeta^{-1})$ de $\mathbb{Q}$ e suponhamos que $\mathbb{K} \neq \mathbb{L}$. Consideramos a extensão composição $\mathbb{KL}|\mathbb{Q}$ a qual é abeliana, tem grau uma potência de 2 e com 2 é o único primo que se ramifica em $\mathcal{O}_{\mathbb{KL}}$. Como $Gal(\mathbb{KL}|\mathbb{K} \cap \mathbb{L}) \simeq Gal(\mathbb{K}|\mathbb{K}\cap\mathbb{L}) \times Gal(\mathbb{L}|\mathbb{K}\cap\mathbb{L})$, segue que $Gal(\mathbb{K}|\mathbb{K}\cap\mathbb{L}) = id$ ou $Gal(\mathbb{L}|\mathbb{K}\cap\mathbb{L}) = id$, pois se $G \simeq G_1 \times G_2$, com G_1 e G_2 ciclícos, então G é ciclíco se, e somente se, as ordens de G_1 e G_2 são primas entre si. Assim, $\mathbb{K} \subseteq \mathbb{L}$ ou $\mathbb{L} \subseteq \mathbb{K}$. Portanto, $\mathbb{K} = \mathbb{L}$, pois $[\mathbb{K} : \mathbb{Q}] = [\mathbb{L} : \mathbb{Q}]$.■

Observação 3.3 *Usando o Lema 3.5 podemos encontrar a extensão ciclotômica que contém $\mathbb{KL} = \mathbb{FL}$, na Proposição 3.3. Sabemos que $[\mathbb{F} : \mathbb{Q}] = 2^r$, com $0 \leq r < m$. Se $\mathbb{F} \subseteq \mathbb{R}$, então, pelo Lema 3.5, $\mathbb{F} = \mathbb{Q}(\zeta_{2^{r+2}} + \zeta_{2^{r+2}}^{-1})$. Logo, $\mathbb{FL} = \mathbb{KL} \subseteq \mathbb{Q}(\zeta_{2^{m+2}}, \zeta_{2^{r+2}}) \subseteq \mathbb{Q}(\zeta_{2^{m+2}})$, pois $r < m$. Agora, se $\mathbb{F}$ não é um corpo totalmente real, então consideramos a extensão composição $\mathbb{F}(i)$ de $\mathbb{F}$ e $\mathbb{Q}(i)$. Seja $\mathbb{F}' = \mathbb{F}(i) \cap \mathbb{R}$. Tem-se que $\mathbb{F}'$ é uma extensão abeliana de $\mathbb{Q}$ de grau 2^s , com $s \leq r + 1$. Assim, pelo Lema 3.5 $\mathbb{F}' \subseteq \mathbb{Q}(\zeta_{2^{s+2}})$, onde $s \leq m$. Como $\mathbb{F} \subseteq \mathbb{F}(i) = \mathbb{F}'(i) \subseteq \mathbb{Q}(\zeta_{2^{s+2}}, \zeta_4) \subseteq \mathbb{Q}(\zeta_{2^{s+2}})$, segue que $\mathbb{KL} = \mathbb{FL} \subseteq \mathbb{Q}(\zeta_{2^{s+2}}, \zeta_{2^{m+2}}) = \mathbb{Q}(\zeta_{2^{m+2}})$, pois $s \leq m$.*

Observação 3.4 *Como na Observação 3.2, tem-se que os corpos de $\mathbb{Q}(\zeta_{2^{m+2}})$ de grau 2^m sobre $\mathbb{Q}$ são $\mathbb{Q}(\zeta_{2^{m+2}} + \zeta_{2^{m+2}}^{-1})$, $\mathbb{Q}(\zeta_{2^{m+2}} - \zeta_{2^{m+2}}^{-1})$ e $\mathbb{Q}(\zeta_{2^{m+2}}^2)$.*

Por fim apresentamos o Teorema de Kronecker-Weber.

Teorema 3.1 *(Kronecker-Weber) Se $\mathbb{K}$ é uma extensão abeliana finita de $\mathbb{Q}$, então $\mathbb{K}$ está contido em um corpo ciclotômico.*

Demonstração. Pelo teorema fundamental dos grupos abelianos finitos tem-se que $G = Gal(\mathbb{K}|\mathbb{Q}) = \prod_{i=1}^{r} G_i$, onde cada G_i é ciclíco de ordem $p_i^{m_i}$. Consideramos $H_i = \prod_{j\neq i} G_i$, para todo $i = 1, \ldots, r$ e denotemos por $\mathbb{K}_i$ o corpo fixo de H_i. Assim, $Gal(\mathbb{K}_i|\mathbb{Q}) \simeq G_i$. Além disso, $\mathbb{K} = \mathbb{K}_1 \ldots \mathbb{K}_r$, pois $Gal(\mathbb{K}|\mathbb{K}_1 \ldots \mathbb{K}_r) \subseteq \bigcap_{i=1}^{r} H_i = \{e\}$. Como vimos nas Proposições 3.1, 3.2 e 3.3 o teorema é válido para cada $\mathbb{K}_i$, ou seja, $\mathbb{K}_i \subseteq \mathbb{Q}(\zeta_{n_i})$, e assim, $\mathbb{K} = \mathbb{K}_1 \ldots \mathbb{K}_r \subseteq \mathbb{Q}(\zeta_{n_1}, \zeta_{n_2}, \ldots, \zeta_{n_r}) \subseteq \mathbb{Q}(\zeta_m)$, onde $m = mmc(n_1, \ldots, n_r)$. ■

Para extensões quadráticas de $\mathbb{Q}$, podemos mostrar o teorema de Kronecker-Weber de forma direta, através do seguinte Corolário.

Corolário 3.3 *Se $\mathbb{K}$ é uma extensão quadrática $\mathbb{Q}$, então $\mathbb{K}$ está contido em um corpo ciclotômico.*

Demonstração. Pela Observação 1.4, tem-se que $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com $d \in \mathbb{Z}$ livre de quadrados. Consideramos $d = \pm p_1 \dots p_r$ a fatoração de d em números primos. Se mostrarmos que $\mathbb{Q}(\sqrt{\pm p_i}) \subseteq \mathbb{Q}(\zeta_{n_i})$, então o resultado segue para $\mathbb{K} = \mathbb{Q}(\sqrt{d})$. Se p é primo ímpar, então pelo Teorema 1.18, segue que $D_{\mathbb{Q}(\zeta_p)} = (-1)^{\frac{p-1}{2}} p^{p-2}$. Assim,

$$D_{\mathbb{Q}(\zeta_p)} = \begin{cases} p^{p-2}, & \text{se} \quad \frac{p-1}{2} \text{ é par} \\ -p^{p-2}, & \text{se} \quad \frac{p-1}{2} \text{ é ímpar} \end{cases}.$$

Notemos que se $\dfrac{p-1}{2}$ é par, então $p \equiv 1(mod\ 4)$ e se $\dfrac{p-1}{2}$ é ímpar, então $p \equiv 3(mod\ 4)$. Além disso, pela Proposição 1.13, tem-se que $D_{\mathbb{Q}(\zeta_p)} = det(\sigma_i(\zeta_p^j))^2$. Logo,

$$\sqrt{D_{\mathbb{Q}(\zeta_p)}} = \begin{cases} \sqrt{p} p^{\frac{p-3}{2}}, & \text{se} \quad p \equiv 1(mod\ 4) \\ i\sqrt{p} p^{\frac{p-3}{2}}, & \text{se} \quad p \equiv 3(mod\ 4) \end{cases}$$

e $\sqrt{D_{\mathbb{Q}(\zeta_p)}} \in \mathbb{Q}(\zeta_p)$. Assim,

$$\sqrt{p} = \begin{cases} \dfrac{\sqrt{D_{\mathbb{Q}(\zeta_p)}}}{p^{\frac{p-3}{2}}}, & \text{se} \quad p \equiv 1(mod\ 4) \\ \dfrac{\sqrt{D_{\mathbb{Q}(\zeta_p)}}}{ip^{\frac{p-3}{2}}}, & \text{se} \quad p \equiv 3(mod\ 4) \end{cases}.$$

Portanto, $\sqrt{p} \in \mathbb{Q}(\zeta_p)$ se $p \equiv 1(mod\ 4)$ e $\sqrt{p} \in \mathbb{Q}(\zeta_p, i)$ se $p \equiv 3(mod\ 4)$. Agora, se $p = 2$, então $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$, pois

$$\zeta_8 = e^{\frac{2\pi i}{8}} = cos\left(\frac{\pi}{4}\right) + i\ sen\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2}(1+i),$$

e assim $\sqrt{2} = \dfrac{2\zeta_8}{1+i} = \dfrac{2\zeta_8}{1+i}\dfrac{1-i}{1-i} = \zeta_8(1-i) \in \mathbb{Q}(\zeta_8)$. ■

Exemplo 3.1 *Consideramos $\mathbb{K} = \mathbb{Q}(\sqrt{6})$. Como $6 = 2.3$ basta encontrarmos os corpos ciclotômicos que contenham $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{3})$. Sabemos que $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8)$ e $\mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\zeta_{12})$. Como $mmc(8, 12) = 24$, segue que $\mathbb{Q}(\sqrt{6}) \subset \mathbb{Q}(\zeta_{24})$.*

3.3 Aplicações

O Teorema de Kronecker-Weber garante a existência de n tal que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$, onde $\mathbb{K}$ é um corpo de números abeliano. O objetivo desta seção é explicitar o valor de n.

Definição 3.1 *O condutor de uma extensão abeliana $\mathbb{K}$ de $\mathbb{Q}$ é o menor n tal que $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$.*

Notemos que $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$ se n é ímpar, pois $\mathbb{Q}(\zeta_n) \subset \mathbb{Q}(\zeta_{2n})$ e $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = \varphi(2)\varphi(n) = [\mathbb{Q}(\zeta_{2n}) : \mathbb{Q}]$. Assim, o condutor de uma extensão abeliana é um número $n \neq 4k+2$. Deste modo, o objetivo é mostrar o seguinte teorema:

Teorema 3.2 *Se $\mathbb{K}$ é uma extensão abeliana finita de $\mathbb{Q}$, onde $p_1, p_2, \ldots, p_r$ são os primos que se ramificam em $\mathbb{K}$ com índices de ramificação $e_i = p_i^{m_i} e_i'$ e $e_i' \nmid p_i$, $1 \leq i \leq r$, então o condutor de $\mathbb{K}$ é dado por*

$$n = \begin{cases} p_1^{m_1+1} p_2^{m_2+1} \ldots p_r^{m_r+1}, & \text{se } p_i \neq 2 \text{ para } 1 \leq i \leq r, \\ 2^{\epsilon} p_1^{m_1+1} p_2^{m_2+1} \ldots p_r^{m_r+1}, & \text{se } p_1 = 2 \end{cases}$$

onde $\epsilon = 0$ ou 1.

Demonstração. Como $\mathbb{K}|\mathbb{Q}$ é abeliana finita, segue que $Gal(\mathbb{K}|\mathbb{Q}) \simeq \prod_{i=1}^{r} G_i$, onde G_i é ciclíco de ordem $p_i^{m_i}$, com p_i primo e $m_i \in \mathbb{N}$. Assim, $\mathbb{K} = \mathbb{K}_1 \ldots \mathbb{K}_r$, com $G_i = Gal(\mathbb{K}_i|\mathbb{Q})$. Mostramos, na Seção 3.2, que $\mathbb{K}_i \subseteq \mathbb{Q}(\zeta_{n_i})$, onde $n_i = p_i^{m_i+1}$ se p_i é primo ímpar e $n_i = 2^{\epsilon} 2^{m_i+1}$ se $p_i = 2$, com $\epsilon \in \{0, 1\}$. Logo, $\mathbb{K} = \mathbb{K}_1 \ldots \mathbb{K}_r \subseteq \mathbb{Q}(\zeta_{n_1}, \ldots, \zeta_{n_r}) = \mathbb{Q}(\zeta_n)$, onde $n = mmc\{n_1, \ldots, n_r\}$. Portanto, n é um múltiplo do condutor de $\mathbb{K}$. Agora, se $m = p_1^{m_1} p_2^{m_2+1} \ldots p_r^{m_r+1}$ é o condutor de $\mathbb{K}$, então $\mathbb{K}_1 \subseteq \mathbb{Q}(\zeta_{p_1^{m_1}})$, mas $[\mathbb{Q}(\zeta_{p_1^{m_1}} : \mathbb{Q}] = p_i^{m_1-1}(p-1)$ que não é divisível por $p_1^{m_1}$. Portanto, n é o condutor de $\mathbb{K}$. ■

Exemplo 3.2 *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{6})$. Como $6 \equiv 2 (mod\ 4)$ segue que $D_{\mathbb{K}} = 24$. Tem-se que 2 e 3 dividem 24, e assim, 2 e 3 se ramificam em $\mathcal{O}_{\mathbb{K}}$. Pelo Teorema de Kummer tem-se que o índice de ramificação de 2 e 3 é 2. Logo, pelo Teorema 3.2, segue que $n = 2^{\epsilon} 2^2 3$. Neste caso, $\epsilon = 1$, pois $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\zeta_8 + \zeta_8^{-1})$. Portanto, $\mathbb{Q}(\sqrt{6}) \subset \mathbb{Q}(\zeta_{24})$ como já foi visto anteriormente.*

Exemplo 3.3 *Seja* $\mathbb{K}|\mathbb{Q}$ *é uma extensão abeliana de grau* $n = 3^1 5^2$*, com* $Gal(\mathbb{K}|\mathbb{Q}) = G \simeq \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$*. Tem-se que* $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{3^2 5^2})$*. Agora, se* $G \simeq \mathbb{Z}_3 \times \mathbb{Z}_{5^2}$*, então* $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{3^2 5^3})$*.*

Exemplo 3.4 *Se* $\mathbb{K}|\mathbb{Q}$ *é uma extensão de grau* $n = 2^3$*, com* $Gal(\mathbb{K}|\mathbb{Q}) = G \simeq \mathbb{Z}_{2^2} \times \mathbb{Z}_2$*. Consideramos* $H_1 \simeq \mathbb{Z}_2$ *e* $H_2 \simeq \mathbb{Z}_{2^2}$*. Os corpos fixos* $\mathbb{K}_1$ *e* $\mathbb{K}_2$ *iram determinar o valor de* ϵ*, ou seja, se* $\mathbb{K}_1 = \mathbb{Q}(\zeta_{2^4} + \zeta_{2^4}^{-1})$ *ou* $\mathbb{Q}(\zeta_{2^4} - \zeta_{2^4}^{-1})$*, então* $\epsilon = 1$ *e se* $\mathbb{K}_1 = \mathbb{Q}(\zeta_{2^4}^2)$*, então* $\epsilon = 0$*.*

3.4 Considerações finais

No presente capítulo apresentamos o Teorema de Kroncker-Weber juntamente com a sua demonstração. O presente teorema é o resultado principal do nosso trabalho. Finalmente, apresentamos uma seção de aplicações do teorema com o objetivo de fornecer condições de encontrar o condutor de um corpo de números abeliano.

Capítulo 4

Considerações finais e perspectivas

Neste trabalho vimos a demonstração do teorema de Kronecker-Weber usando teoria da ramificação. Embora este teorema possa ser demonstrado usando a teoria de classes de corpos e a teoria da localização, através da teoria da ramificação tem-se um demonstração mais elementar de teorema.

Na verdade, apenas garantir que um corpo de números abeliano está contido em um corpo ciclotômico não é útil se não soubermos o seu condutor. Outra forma de estudar o condutor de um corpo de números abelianos é fazer um estudo sobre caracteres de Dirichlet. Um caracter de Dirichlet definido módulo n é um homomorfismo $\chi : \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* \longrightarrow \mathbb{C}^*$. Se $m|n$, então um caracter de Dirichlet definido módulo n pode ser induzido de um caracter de Dirichlet definido módulo m. O menor m que induz um caracter módulo n é chamado condutor do caracter χ e coincide com o condutor do corpo $\mathbb{K}$ que é o corpo fixo de $Ker(\chi)$.

No caso de extensões abelianas infinitas é preciso fazer um estudo de extensões de Galois infinitas, consequentemente dos grupos de inércia, decomposição e ramificação. Este estudo pode ser encontrado em [4].

Como perspectiva de futuros trabalhos, fazendo o uso do presente trabalho, é encontrar subcorpos de um corpo ciclotômico com seus respectivos anéis de inteiros e discriminantes.

Referências Bibliográficas

[1] GREENBERG, M. J. An Elementary Proof of the Kronecker-Weber Theorem. **Amer. Math. Monthly**, v.81 (1974), p. 601-607; correction,v.82 (1975), p. 803.

[2] LANG, S. **Algebraic Number Theory**. Springer-Verlag, New York, 1994.

[3] WASHINGTON, L.C. **Introduction to cyclotomic fields**. Springer-Verlag, New York, 1982.

[4] TRAVESA, A. El teorema de Kronecker-Weber. **CSIC**, Madri, 2008.

[5] NOBREGA NETO, T. P.; INTERLANDO, J. C.; LOPES, J. O. D. The discriminant of abelian number fields. **Journal of Algebra and Its Applications**, vol. 5 N 1, 35-41, 2006.

[6] ATIYAH, M. F.; MACDONALD, I. J. **Introduction to commutative algebra**. Addison-Wesley, London, 1969.

[7] SAMUEL, P. **Algebraic theory of numbers**. Hermann, Paris, 1970.

[8] MORANDI, P. **Fields and Galois theory**. Springer-Verlag, New York, 1996.

[9] RIBENBOIM, P. **Classical Theory of Algebraic Numbers**. Springer-Verlag, New York, 2001.

[10] TAPIA, H. E. P. **Uma prova elementar do teorema de Kronecker-Weber**. 2009. 95f. Dissertação (Mestrado em Ciências), Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2009.

[11] ENDLER, O. **Teoria dos corpos**. IMPA, Rio de Janeiro, 1987.

[12] ENDLER, O. **Teoria dos números algébricos**. IMPA, Rio de Janeiro, 2006.

[13] LANG, S **Algebra**. Addison-Wesley, New York, 1972.

[14] STEWAR, I.; TALL, D. **Algebraic number theory**. A K Peters, London, 1987.

[15] STEWART, I. **Galois Theory**. Chapman and Hall, 2004.

[16] QUILLES, C. R. O. **Discriminante de Corpos de Números**. 2008. 140f. Dissertação (Mestrado em Matemática), Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2008.

[17] ZARISKI, O.; PIERRE, S. **Commutative algebra**. Springer-Verlag, New York, 1958.

[18] OLIVEIRA, C. M. **Discriminante, ramificação e diferente**. 2005. 124f. Dissertação (Mestrado em Matemática), Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São José do Rio Preto, 2005.

[19] DOMINGUES, H. H.; IEZZI, G. **Álgebra Moderna**. Atual Editora, São Paulo, 1982.

Autorizo a reprodução xerográfica para fins de pesquisa.

São José do Rio Preto, 24 / 02 / 2012

Ana Cláudia Machado Mendonça

Assinatura