Uma prova elementar do teorema de Kronecker-Weber

Héctor Edonis Pinedo Tapia

Dissertação apresentada
ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para
obtenção do título
de
Mestre em Ciências

Área de Concentração : Matemática
Orientador: Prof. Dr. Paulo Agozzini Martin

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro do CNPq

São Paulo, 3 de Abril de 2009

Uma prova elementar do teorema de Kronecker-Weber

Este exemplar corresponde à redação
final da dissertação devidamente corrigida
e defendida por Héctor Edonis Pinedo Tapia
e aprovada pela Comissão Julgadora.

Banca Examinadora:

- Prof. Dr. Paulo Agozzini Martin (orientador) - IME-USP.
- Prof. Dr. Ricardo Bianconi - IME-USP.
- Prof. Dr. Daniel Levcovitz - ICMC-USP.

Agradecimentos

Agradeço primeiramente a Deus.

Aos meus pais Alfonso e Ana pelo incentivo, apoio e segurança, sempre.

Ao meu paciente orientador, o professor Paulo A. Martin, que com muita paciência resolveu todas as minhas dúvidas.

À Nubia e ao Oscar que me ajudaram muito quando cheguei nesta imensa cidade.

À Alejandra por muitas coisas boas que ela fez para mim.

Ao Rodrigo por ter me ajudado a corrigir meus erros de português.

Ao CNPq pelo apoio financiero.

A minha noiva Natali porque sem ela...

Resumo

Um dos resultados mais importantes da teoria dos números algébricos é o *Teorema de Kronecker-Weber*.
Ele afirma que, se K / $\mathbb{Q}$ é uma extensão finita e galoisiana com grupo de Galois abeliano, então existe uma raiz n-ésima da unidade, ζ, tal que $K \subset \mathbb{Q}(\zeta)$. Em outras palavras, K é um corpo ciclotômico. Esse teorema é como um teorema de uniformização em geometria.
Para prová-lo, precisamos estudar a teoria dos números algébricos, anéis de Dedekind, ramificação , grupos de ramificação , produto fibrado de grupos de Galois e alguns resultados sobre grupos abelianos finitos.

Palavras-chave: inteiro algébrico, domínio de Dedekind, corpo ciclotômico.

Abstract

One of the most important results in algebraic number theory is the *Kronecker-Weber Theorem*.
It stablishes that, if K / $\mathbb{Q}$ is a finite Galois extension whose galois group is abelian, there exists a primitive n-th root of unity ζ, such that $K \subset \mathbb{Q}(\zeta)$. In brief K is a ciclotomic field. This theorem is like an uniformization theorem in geometry.
In order to prove it, we study algebraic number theory, Dedekind rings, ramification, ramification groups, fibre products of Galois groups and some results about finite abelian groups.

Keywords: algebraic integer, dedekind domain, ciclotomic field.

Conteúdo

1 O Anel dos inteiros algébricos **2**
- 1.1 Traço e Norma 5
- 1.2 Domínios de Dedekind 9
- 1.3 Localização 17

2 Extensões de Galois **22**
- 2.1 Grupos de Decomposição e Inércia 23
- 2.2 Grupos de Ramificação 35
- 2.3 O Compositum 41

3 Corpos de Números Algébricos **44**
- 3.1 Discriminante 44
- 3.2 Método Geométrico 55
- 3.3 O espaço Ł^{s,t} 63
- 3.4 Automorfismo de Frobenius 70

4 Extensões Ciclotômicas **74**
- 4.1 Fatos e definições elementares 74
- 4.2 Teorema de Kronecker-Weber 79

Capítulo 1

O Anel dos inteiros algébricos

A teoria dos números *algébricos* surgiu, como uma ferramenta para resolver equações diofantinas, isto é, encontrar soluções inteiras para equações algébricas da forma $F(X_1, ..., X_n) = 0$, onde $F(X_1, ..., X_n) \in \mathbb{Z}[X_1, ..., X_n]$.
Como, por exemplo, a equação $X^p + Y^p = Z^p$ que, pelo famoso *Último Teorema de Fermat*, não possui soluções inteiras não triviais onde p é um primo ímpar. A prova desse resultado, feita por Andrew Wiles, é uma das mais importantes descobertas da Matemática atual.

Neste capítulo daremos as definições básicas e provaremos alguns resultados da teoria dos inteiros algébricos. Também definiremos os aneis de Dedekind e obteremos alguns resultados importantes sobre esses aneis.

Definição 1.1 *$\alpha \in \mathbb{C}$ é um número algébrico sobre $\mathbb{Q}$ se existe $f(X) \in \mathbb{Q}[X]$, mônico, tal que $f(\alpha) = 0$.*

Definição 1.2 *Seja L um corpo. Se L é uma extensão finita de $\mathbb{Q}$, então L é chamado um corpo de números algébricos.*

Vamos generalizar as definições anteriores.

Definição 1.3 *Seja L um corpo, B um subanel de L e A um subanel de B. Diremos que $\alpha \in B$ é inteiro sobre A se existir $f(X) \in A[X]$ mônico tal que $f(\alpha) = 0$.*

• Quando $B = \mathbb{C}$ e $A = \mathbb{Z}$ os inteiros sobre $\mathbb{Z}$ são chamados *inteiros algébricos*.
Vamos provar que o conjunto $I_B(A)$ formado pelos elementos de B que são inteiros sobre A é um subanel de B.

Teorema 1.1 *Sejam A e B como na definição anterior. As seguintes condições são equivalentes:*

1. *$\alpha \in B$ é inteiro sobre A.*
2. *$A[\alpha] = \{f(\alpha) \mid f(X) \in A[X]\}$ é um A-módulo finitamente gerado.*
3. *Existe um A-módulo finitamente gerado M talque $M \subset B$ e $\alpha M \subset M$.*

Demonstração:
$1 \Rightarrow 2$
Se α é inteiro sobre A, existe $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in A[X]$ tal que $f(\alpha) = 0$. Se $M = A + A\alpha + \cdots + A\alpha^{n-1}$, é claro que $M \subset A[\alpha]$. Vamos mostrar que, para todo inteiro k não negativo, temos que $1, \alpha, ..., \alpha^{n+k} \in M$.
De fato, como $f(\alpha) = 0$, tem-se que:

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0 \in M.$$

Logo $\alpha^n \in M$, e $1, \alpha, ..., \alpha^n \in M$.
Agora se $1, \alpha, ...\alpha^{n+k-1} \in M$, como $\alpha^{n+k} = -a_{n-1}\alpha^{n+k-1} - \cdots - a_1\alpha^{n+1} - a_0\alpha^n \in M$, temos $\alpha^{n+k} \in M$, então $M \supset A + A\alpha + \cdots + A\alpha^{n+k}$ para todo $k \in \mathbb{N}$, assim $M \supset A[\alpha]$, logo $M = A[\alpha]$ e $A[\alpha]$ é finitamente gerado.
$2 \Rightarrow 3$
Seja $M = A[\alpha]$, então M é um A-módulo finitamente gerado, $M \subset B$ e $\alpha M \subset M$.
$3 \Rightarrow 1$
Seja $m_1, \cdots, m_n$ um conjunto de geradores de M. Como $\alpha M \subset M$ temos que $\alpha m_j \in M$ para todo $j \in \{1, \cdots, n\}$, assim temos o sistema de equações :

$$\begin{aligned}
\alpha m_1 &= a_{11}m_1 + a_{12}m_2 + \cdots + a_{1n}m_n \\
\alpha m_2 &= a_{21}m_1 + a_{22}m_2 + \cdots + a_{2n}m_n \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\alpha m_n &= a_{n1}m_1 + a_{n2}m_2 + \cdots + a_{nn}m_n
\end{aligned}$$

que é equivalente a:

$$\begin{aligned}
0 &= (\alpha - a_{11})m_1 + a_{12}m_2 + \cdots + a_{1n}m_n \\
0 &= a_{21}m_1 + (\alpha - a_{22})m_2 + \cdots + a_{2n}m_n \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
0 &= a_{n1}m_1 + a_{n2}m_2 + \cdots + (\alpha - a_{nn})m_n
\end{aligned}$$

onde $a_{ij} \in A$ para $1 \leq i, j \leq n$. Portanto $m = (m_1, \cdots, m_n)$ é uma solução do sistema de equações lineares acima. Assim, se S é a matriz:

$$S = \begin{pmatrix} a_{11} - \alpha & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} - \alpha & \cdots & a_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} - \alpha \end{pmatrix},$$

tem-se que $\det S = 0$. Logo α é raiz do polinômio caracteristico de S, e, portanto, α é inteiro sobre A. ■

Corolário 1.2 *Se $\alpha_1, \cdots, \alpha_m$ são inteiros sobre A, então $A[\alpha_1, \cdots \alpha_m]$ é um A-módulo finitamente gerado.*

Demonstração: Vamos fazer indução sobre m.
Se $m = 1$, pelo item 2 do teorema 1.1 temos que $A[\alpha_1]$ é um A-módulo finitamente gerado. Seja $m > 1$ e suponhamos que $A_{m-1} = A[\alpha_1, \cdots, \alpha_{m-1}]$ seja um A-módulo finitamente gerado. Como α_m é inteiro sobre A_{m-1}, $A_m = A_{m-1}[\alpha_m]$ é um A_{m-1}-módulo finitamente gerado. Assim, se $\beta_1, \cdots, \beta_n$ um sistema de geradores de A_{m-1} sobre A e $\delta_1, \cdots, \delta_t$ um sistema de geradores de A_m sobre A_{m-1}, temos que $\{\delta_i\beta_j \mid 1 \leq i \leq t, 1 \leq j \leq n\}$ é um sistema de geradores de $A_m = A[\alpha_1, \cdots \alpha_m]$ sobre A. ■

Corolário 1.3 *$I_B(A)$ é um subanel de B que contém A.*

Demonstração: Sejam $\alpha, \beta \in I_B(A)$. Então $A[\alpha, \beta]$ é um A-módulo finitamente gerado e temos que $\alpha - \beta$, $\alpha\beta \in A[\alpha, \beta]$.
Logo $(\alpha - \beta)A[\alpha, \beta] \subset A[\alpha, \beta]$ e $(\alpha\beta)A[\alpha, \beta] \subset A[\alpha, \beta]$, assim pela parte 3 do Teorema 1.1, $\alpha - \beta$ e $\alpha\beta$ são inteiros sobre A. ■

- $I_B(A)$ é chamado o *fecho inteiro de A em B*.
- Se $I_B(A) = A$, dizemos que A é *integralmente fechado em B*.
- Se A é integralmente fechado no seu corpo de frações dizemos que A é *integralmente fechado*.
- Se $I_B(A) = B$, dizemos que B é *inteiro sobre A*.
- No caso $B = L$ e $A = \mathbb{Z}$, o anel dos inteiros algébricos de L sera denotado por I_L.

Exemplo 1.1 *Sejam E e K corpos. Se E é uma extensão algébrica de K, então* $I_E(K) = E$.

Teorema 1.4 *Se A é um domínio fatorial, A é integralmente fechado. Em particular* $I_{\mathbb{Q}} = \mathbb{Z}$.

Demonstração: Seja $K = Q(A)$ o corpo de frações de A e $\alpha \in I_K(A)$. Então podemos escrever $\alpha = \dfrac{a}{b}$ com $a, b \in A, b \neq 0$ e $mdc(a, b) = 1$.
Sabemos que existe $f(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0 \in A[X]$ tal que $f(\alpha) = 0$, e, portanto,

$$\frac{a^n}{b^n} = -\left(c_{n-1}\frac{a^{n-1}}{b^{n-1}} + \cdots + c_1\frac{a}{b} + c_0\right).$$

Desse modo $a^n = -b(c_{n-1}a^{n-1} + \cdots + b^{n-1}c_1a + b^nc_0)$ e, portanto, $b \mid a^n$. Mas como $mdc(a, b) = 1$, temos que $b \mid 1$ e $b \in U(A)$ (o grupo das unidades de A), logo $\alpha \in A$. ■

1.1 Traço e Norma

Sejam K um corpo, L uma K-álgebra de dimensão n, $\{\beta_1, \cdots, \beta_n\}$ uma base de L sobre K e $\alpha \in L$. Consideremos a transformação linear $T_\alpha \colon L \longrightarrow L$ tal que $T_\alpha(y) = \alpha y$ para todo $y \in L$ e seja $A = (a_{ij})$ a representacão matricial de T.

Definição 1.4 *O polinômio* $\chi_\alpha(X) = det(XI - A)$ *é chamado polinômio característico de* α *em K.*

Definição 1.5 *Se* $\chi_\alpha(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, *definimos o Traço e norma de* α *em relação a* $L \mid K$, *como:*

$$T_{L|K}\,\alpha = -a_{n-1} = \sum_{i=1}^{n} a_{ii} \quad e \quad N_{L|K}\,\alpha = (-1)^n a_0 = \det A$$

Propriedades: Sejam $\alpha, \beta \in L$, $P_\alpha(X)$ o polinômio minimal de α sobre K e $a, b \in K$ então :

- $\chi_\alpha(X) = P_\alpha(X)^m$ onde $m = [L : K(\alpha)]$.
- $T_{L|K}(a\alpha + b\beta) = aT_{L|K}(\alpha) + bT_{L|K}(\beta)$ e $T_{L|K}(a) = na$.
- $N_{L|K}(\alpha\beta) = (N_{L|K}\alpha)(N_{L|K}\beta)$ e $N_{L|K}(a)=a^n$.
- Se L é uma extensão finita e separável de K e $\sigma_1, \cdots, \sigma_n$ são os K isomorfismos de L em subcorpos de $\overline{K}$ (fecho algébrico de K), então :

$$\chi_\alpha(X) = \prod_{i=1}^{n}(X - \sigma_i(\alpha))$$
$$N_{L|K}(\alpha) = \prod_{i=1}^{n}\sigma_i(\alpha)$$
$$T_{L|K}(\alpha) = \sum_{i=1}^{n}\sigma_i(\alpha).$$

  Veja [5] p.87 e p.93.

Teorema 1.5 *Sejam A um domínio integralmente fechado, L uma extensão finita e separável de $K = Q(A)$ e $\alpha \in I_L(A)$, com $\alpha \neq 0$ então :*

1. $P_\alpha(X)$ e $\chi_\alpha(X) \in A[X]$, *e, portanto,* $N_{L|K}(\alpha)$ e $T_{L|K}(\alpha) \in A$.
2. $\alpha \mid N_{L|K}(\alpha)$ *em* $I_L(A)$.
3. $\alpha \in U(I_L(A)) \Longleftrightarrow N_{L|K}(\alpha) \in U(A)$.
4. *Se* $N_{L|K}(\alpha)$ *é irredutível em* A *então* α *é irredutível em* $I_L(A)$.

Demonstração:

1. Como α é inteiro sobre A, existem $h(X) \in A[X]$ mônico tal que $h(\alpha) = 0$ e $g(X) \in K[X]$ tal que $P_\alpha(X)g(X) = h(X)$. Assim $g(X)$ é mônico.
   Escrevendo $g(X) = \prod_{i=1}^{m}(X - \beta_i)$ e $P_\alpha(X) = \prod_{i=1}^{n}(X - \alpha_i)$ em $\bar{K}[X]$, como $P_\alpha(X)g(X) \in A[X]$, temos que $\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_m \in I_{\bar{K}}(A)$.
   Portanto os coeficientes de $g(X)$ e $P_\alpha(X)$ estão em $I_{\bar{K}}(A) \cap K = I_K(A) = A$, onde a ultima igualdade se verifica por ser A é integralmente fechado.
   Assim $P_\alpha(X) \in A[X]$ e, como $\chi_\alpha(X) = P_\alpha(X)^m$, temos que $\chi_\alpha(X) \in A[X]$.

2. Sejam $\sigma_1, \cdots, \sigma_n$ os K monomorfismos de L em $\bar{K}$. Então

   $N_{L|K}(\alpha) = \prod_{i=1}^{n}\sigma_i(\alpha) = \alpha\prod_{i=2}^{n}\sigma_i(\alpha)$, assim $\prod_{i=2}^{n}\sigma_i(\alpha) = N_{L|K}(\alpha)\alpha^{-1}$, então $\prod_{i=2}^{n}\sigma_i(\alpha) \in L$, e desse modo $\prod_{i=2}^{n}\sigma_i(\alpha) \in L \cap I_{\bar{K}}(A) = I_L(A)$ como queríamos demonstrar. ■

3. ($\Rightarrow$) Se $\beta \in I_L(A)$ é tal que $\alpha\beta = 1$, então $N_{L|K}(\alpha)N_{L|K}(\beta) = 1$. Desse modo $N_{L|K}(\alpha)$ é inversível em $I_L(A)$.
   ($\Leftarrow$) Pelo item anterior, existe $\lambda \in I_L(A)$ tal que $\lambda\alpha = N_{L|K}(\alpha)$. Assim se δ é o inverso de $N_{L|K}(\alpha)$ em A, então $\lambda\delta$ é o inverso de α em $I_L(A)$.

4. Se $\alpha = \beta\theta$ com β e θ em $I_L(A)$. Temos que, $N_{L|K}(\alpha) = N_{L|K}(\beta)N_{L|K}(\theta)$, desse modo $N_{L|K}(\beta) \in U(A)$ ou $N_{L|K}(\theta) \in U(A)$, logo pelo item anterior $\beta \in U(I_L(A))$ ou $\theta \in U(I_L(A))$, assim α é irredutível. ■

Definição 1.6 Corpos quadráticos*:*
São, por definição , subcorpos L de $\mathbb{C}$ *tais que* $[L : \mathbb{Q}] = 2$.

Consideremos o conjunto $\mathcal{D}$ formado pelos $d \in \mathbb{Z} - \{0, 1\}$ tais que d é livre de quadrados. A aplicação definida por $d \longrightarrow \mathbb{Q}(\sqrt{d})$ é uma bijeção de $\mathcal{D}$ sobre o conjunto dos corpos quadráticos. Veja [2] p.19.

Teorema 1.6 *Seja* $L = \mathbb{Q}(\sqrt{d})$ *um corpo quádratico. Então o anel* I_L *dos inteiros algébricos de L é dado por:*

$$I_L = \left\{ \frac{m}{2} + \frac{n}{2}\sqrt{d} \;\middle|\; m, n \in \mathbb{Z}, m^2 \equiv n^2 d \,(mod\, 4) \right\}$$

Demonstração: Provaremos primeiramente que I_L é um subconjunto do conjunto da direita.
Para $\alpha \in I_L \subset L$, temos que $\alpha = r + s\sqrt{d}$, onde $r, s \in \mathbb{Q}$. Pela parte 1 do teorema anterior, temos que $P_\alpha(X) \in \mathbb{Z}[X]$, e como $P_\alpha(X) = X^2 - 2rX + (r^2 - s^2 d)$, podemos concluir que $2r, r^2 - s^2 d \in \mathbb{Z}$, e, portanto $\triangle = (2r)^2 - 4(r^2 - s^2 d) = (2s)^2 d \in \mathbb{Z}$.
Sejam $k_p \in \mathbb{Z}$ e $e_p \in \{0, 1\}$, os expoentes do primo p nas fatorações de $2s$ e d respectivamente. Como $(2s)^2 d \in \mathbb{Z}$, temos que $2k_p + e_p \geq 0$. Desse modo, $k_p \geq -\frac{e_p}{2} \geq -\frac{1}{2}$, o que implica que $k_p \geq 0$. Portanto, $2s \in \mathbb{Z}$, logo $2r = m$ e $2s = n$, com $m, n \in \mathbb{Z}$.

Assim, $\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d}$ e $m^2 - n^2 d = 4(r^2 - s^2 d) = 4N_{L|\mathbb{Q}}(\alpha)$, desse modo $m^2 \equiv n^2 d \,(mod\, 4)$.
Provaremos agora a inclução recíproca. Seja $\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d}$ com $m, n \in \mathbb{Z}$ e $m^2 \equiv n^2 d \,(mod\, 4)$ e consideremos $\{1, \sqrt{d}\}$ como base de $L/\mathbb{Q}$.
Como,

$$\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d} \quad \text{e} \quad \alpha\sqrt{d} = \frac{nd}{2} + \frac{m}{2}\sqrt{d}$$

Temos que,

$$\chi_\alpha(X) = \det\begin{pmatrix} X - \frac{m}{2} & -\frac{n}{2} \\ -\frac{nd}{2} & X - \frac{m}{2} \end{pmatrix} = \left(X - \frac{m}{2}\right)^2 - \frac{n^2 d}{4} = X^2 - mX + \frac{(m^2 - n^2)d}{4} \in \mathbb{Z}[X]$$

e $\chi_\alpha(\alpha) = 0$, logo $\alpha \in I_L$. ■

Mostraremos a seguir que I_L é um $\mathbb{Z}$-módulo livre; mais especificamente mostraremos o seguinte resultado:

Teorema 1.7 *Se $L = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados e*

$$\delta = \begin{cases} \sqrt{d}, \ \textit{se } d \equiv 2, 3 \,(mod\, 4). \\ \dfrac{1 + \sqrt{d}}{2}, \ \textit{se } d \equiv 1 \,(mod\, 4). \end{cases}$$

Então , $\{1, \delta\}$ é uma base do $\mathbb{Z}$-módulo I_L.

Demonstração: $\{1, \sqrt{d}\}$ é um conjunto LI sobre $\mathbb{Z}$, pois é LI sobre $\mathbb{Q}$. Logo $\{1, \delta\}$ também é LI sobre $\mathbb{Q}$, sabemos que $I_L = \left\{ \frac{m}{2} + \frac{n}{2}\sqrt{d} \;\middle|\; m, n \in \mathbb{Z}, m^2 \equiv n^2 d \,(mod\, 4) \right\}$.

Se $\delta = \sqrt{d}$, temos que $\delta \in I_L$, e, se $\delta = \frac{1+\sqrt{d}}{2}$, temos que $\delta = \frac{1}{2} + \frac{1}{2}\sqrt{d}$ e $d \equiv 1 \,(mod\, 4)$ o que implica $\delta \in I_L$, assim $\mathbb{Z} + \mathbb{Z}\delta \subset I_L$.

Seja agora $\alpha \in I_L$, então $\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d}$, com $m, n \in \mathbb{Z}$ e $m^2 \equiv n^2 d (mod\, 4)$.
Se $d \equiv 1 \,(mod\, 4)$, temos $m^2 \equiv n^2 (mod\, 4)$, logo existe $k \in \mathbb{Z}$ tal que $m^2 - n^2 = 4k$.

Assim, $(m-n)^2 = 4k - 2mn + 2n^2$, portanto $m - n$ é par, desse modo $m = 2k' + n$, com $k' \in \mathbb{Z}$, logo $\alpha = \frac{2k'+n}{2} + \frac{n}{2}\sqrt{d} = k' + n\frac{1+\sqrt{d}}{2} = k' + n\delta \in \mathbb{Z} + \mathbb{Z}\delta$.
Se $d \equiv 2, 3 \,(mod\, 4)$. Temos que $\delta = \sqrt{d}$, então é suficiente provar que m e n são pares. Se n é ímpar, temos que $n \equiv 1 \,(mod\, 2)$, assim $n^2 \equiv 1 \,(mod\, 4)$, portanto $m^2 \equiv n^2 d \equiv d \,(mod\, 4)$.
Se m for par, $m^2 \equiv 0 \,(mod\, 4)$, assim $d \equiv 0 \,(mod\, 4)$, contradição . Se m for ímpar, teriamos que $m^2 \equiv 1 \,(mod\, 4)$, assim $d \equiv 1 (mod\, 4)$, e, de novo temos uma contradição . Logo n tem que ser par, e, finalmente como $m^2 \equiv n^2 d \equiv 0 \,(mod\, 4)$ temos que m é par, assim $I_L \subset \mathbb{Z} + \mathbb{Z}\delta$. ■

Observação :
A recíproca do item 4 do teorema 1.5 é falsa. De fato se $L = \mathbb{Q}(\sqrt{-5})$, como $-5 \equiv 3 \,(mod\, 4)$, então $I_L = \mathbb{Z} + \mathbb{Z}(\sqrt{-5})$ e tomando $\alpha = 1 + 2\sqrt{-5}$ em I_L, tem-se que $N_{L|K}(\alpha) = 21$ que não é irredutível em $\mathbb{Z}$. Agora, se $\alpha = \beta\theta$ em I_L, então :

$$21 = N_{L|K}(\beta) N_{L|K}(\theta), \text{ logo } N_{L|K}(\beta) \in \{3, -3, 7, -7\},$$

portanto existem inteiros a e b tais que $a^2 + 5b^2 \in \{3, -3, 7, -7\}$, absurdo.

1.2 Domínios de Dedekind

Seja A um domínio e $K = Q(A)$.

Definição 1.7 *Seja $M \subset K$ um A-módulo. Dizemos que M é um ideal fracionário de A, se existir $a \in A$ não nulo tal que $aM \subset A$. Neste caso é facil ver que aM é um ideal de A.*

Exemplo 1.2 *Quando, $A = \mathbb{Z}$, temos que $K = \mathbb{Q}$, então para $r \in \mathbb{Q}$, $M = r\mathbb{Z}$, é um ideal fracionario de $\mathbb{Z}$. Agora, se M é um ideal fraccionario de $\mathbb{Z}$, existe $a \in \mathbb{Z}$ não nulo tal que aM é um ideal de $\mathbb{Z}$, logo $aM = b\mathbb{Z}$ para algum $b \in \mathbb{Z}$. Assim $M = r\mathbb{Z}$, onde $r = \frac{b}{a}$.*

As seguintes propriedades são facieis de provar.
• Se M e N são ideais fracionários de A, então :

$$MN = \left\{ \sum_{i=1}^{k} m_i n_i \,\middle|\, k \in \mathbb{N},\ m_i \in M \, e \, n_i \in N \right\}$$

é um ideal fracionário de A .
• Se M é ideal fracionário de A, então $MA = M$.

Definição 1.8 *Um anel R é dito noetheriano se satisfaz uma e portanto todas as seguintes condições equivalentes.*

- **Condição de Cadeia ascendente C.C.A**
  Dada uma cadeia ascendente $\mathfrak{U}_1 \subset \mathfrak{U}_2 \subset \cdots \subset \mathfrak{U}_m \subset \cdots$ de ideais de R, existe $n \in \mathbb{N}$ tal que $\mathfrak{U}_n = \mathfrak{U}_t$, para todo $t \geq n$.

- **Condicão Maximal**
  Seja $\mathfrak{m}$ uma família não vazia de ideais de R então $\mathfrak{m}$ tem elemento maximal.

- *Todo ideal de R é um R-módulo finitamente gerado.*

Definição 1.9 *Um domínio A é de Dedekind se:*

- *A é noetheriano.*

- *A é integralmente fechado.*

- *Todo ideal primo não nulo é maximal.*

Exemplo 1.3 • *Pelo teorema 1.4 sabemos que $\mathbb{Z}$ é integralmente fechado. Além disso, todo ideal de $\mathbb{Z}$ é finitamente gerado, logo $\mathbb{Z}$ é noetheriano. Finalmente todo seus ideais primos não nulos são maximais. Assim $\mathbb{Z}$ é um dominío de Dedekind.*

Teorema 1.8 *Seja A um domínio de Dedekind. Então os ideais fracionários de A formam um grupo com a multiplicação .*

Para provar do teorema anterior precisaremos provar primeiramente alguns lemas.

Lema 1.9 *Seja $I \neq (0)$ um ideal de A. Existem ideais primos $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$, tais que $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset I$.*

Demonstração: Suponhamos que a família $\mathfrak{U}$ dos ideais não nulos de A que não satisfazem a tese é não vazia.
Como A é noetheriano, $\mathfrak{U}$ tem elemento maximal $\mathfrak{I}$, e é claro que ele não é primo; portanto, existem d_1 e d_2 em A tais que $d_1 d_2 \in \mathfrak{I}, d_1 \notin \mathfrak{I}$ e $d_2 \notin \mathfrak{I}$. Considerando $\mathfrak{I}_1 = \langle \mathfrak{I}, d_1 \rangle$ (o ideal gerado por $\mathfrak{I}$ e d_1) e $\mathfrak{I}_2 = \langle \mathfrak{I}, d_2 \rangle$, temos que $\mathfrak{I} \subsetneq \mathfrak{I}_1$ e $\mathfrak{I} \subsetneq \mathfrak{I}_2$; mas $\mathfrak{I}$ é elemento maximal de $\mathfrak{U}$, então $\mathfrak{I}_1 \notin \mathfrak{U}$ e $\mathfrak{I}_2 \notin \mathfrak{U}$.
Assim, existem ideais primos $\mathfrak{P}_1, \cdots, \mathfrak{P}_r$ e $\mathfrak{Q}_1, \cdots, \mathfrak{Q}_s$ tais que $\mathfrak{P}_1 \cdots \mathfrak{P}_r \subset \mathfrak{I}_1$ e $\mathfrak{Q}_1 \cdots \mathfrak{Q}_s \subset \mathfrak{I}_2$; como $\mathfrak{I}_1 \mathfrak{I}_2 \subset \mathfrak{I}$, então $\mathfrak{P}_1 \cdots \mathfrak{P}_r \mathfrak{Q}_1 \cdots \mathfrak{Q}_s \subset \mathfrak{I}$, o que é uma contradição . Portanto $\mathfrak{U}$ é vazia. ■

Lema 1.10 *Seja $\mathfrak{p}$ um ideal maximal de A, então existe um ideal fracionário $\mathfrak{n}$ de A tal que $\mathfrak{p}\mathfrak{n} = A$.*

Demonstração: Sejam $K = Q(A)$ e $\mathfrak{n} = \{x \in K \mid x\mathfrak{p} \subset A\}$. Então $\mathfrak{n}$ é um A-submódulo de K e, para $p \in \mathfrak{p}$ não nulo, $p\mathfrak{n} \subset A$. Logo $\mathfrak{n}$ é um ideal fracionário de A. Vamos provar que $\mathfrak{p}\mathfrak{n} = A$.
Sabemos que $\mathfrak{p} \subset \mathfrak{p}\mathfrak{n} \subset A$, logo, como $\mathfrak{p}$ é maximal, temos que $\mathfrak{p} = \mathfrak{p}\mathfrak{n}$ ou $\mathfrak{p}\mathfrak{n} = A$, suponhamos que $\mathfrak{p} = \mathfrak{p}\mathfrak{n}$. Então para todo $\alpha \in \mathfrak{n}$, $\alpha\mathfrak{p} \subset \mathfrak{p}$ e, como A é noetheriano $\mathfrak{p}$ é um A-módulo finitamente gerado. Logo $\alpha \in \mathfrak{n}$ é inteiro sobre A, e, portanto $\mathfrak{n} \subset I_K(A) = A$; mas como $A \subset \mathfrak{n}$, segue que $A = \mathfrak{n}$. Vamos mostrar que $A \neq \mathfrak{n}$.
De fato, considerando $a \in \mathfrak{p}$ não nulo, pelo lema anterior existe $r \in \mathbb{N}$ mínimo e ideais primos $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ de A tais que $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (a)$.
Se $r = 1$, então $\mathfrak{p}_1 \subset (a)$, mas $\mathfrak{p}_1$ é ideal maximal de A, assim temos que $(a) = A$ ou $(a) = \mathfrak{p}_1$. Se $(a) = A$, então $\mathfrak{p} = A$, uma contradição ; se $(a) = \mathfrak{p}_1$, em particular tem-se que $a \in \mathfrak{p}_1$, logo $\mathfrak{p} \subset \mathfrak{p}_1$ assim $\mathfrak{p} = \mathfrak{p}_1 = (a)$ e $\mathfrak{m} = a^{-1}A$ é tal que $\mathfrak{m}\mathfrak{p} = A$.
Suponhamos que $r \geq 2$. Como r é mínimo, tem-se que $\mathfrak{p}_2 \cdots \mathfrak{p}_r \subsetneq (a)$, assim existe $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ tal que $b \notin (a)$. Como $\mathfrak{p}$ é maximal (primo), algum dos $\mathfrak{p}_i$, digamos $\mathfrak{p}_1$, está contido em $\mathfrak{p}$, logo $\mathfrak{p}_1 = \mathfrak{p}$ e podemos concluir que $b\mathfrak{p} \subset \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset (a) = aA$. Assim, $ba^{-1}\mathfrak{p} \subset A$ e $ba^{-1} \in \mathfrak{n}$, mas $b \notin (a)$ desse modo $ba^{-1} \notin A$. Portanto $\mathfrak{n} \neq A$. Conseqüentemente $\mathfrak{p} \neq \mathfrak{p}\mathfrak{n}$ e, portanto $\mathfrak{p}\mathfrak{n} = A$. ■

Lema 1.11 *Todo ideal não nulo é o inverso de um ideal fracionário.*

Demonstração: Suponhamos que a família $\mathfrak{U}$ de ideais de A que não cumprem o lema é não vazia. Seja $\mathfrak{u}$ um elemento maximal dessa família. Pelo lema anterior,

$\mathfrak{u}$ não é maximal em A. Assim, existe $\mathfrak{p}$, ideal maximal de A tal que $\mathfrak{u} \subsetneq \mathfrak{p}$, então $\mathfrak{m}_1 = \{x \in K \mid x\mathfrak{p} \subset A\} \subset \mathfrak{m}_2 = \{x \in K \mid x\mathfrak{u} \subset A\}$, e $\mathfrak{u} \subset \mathfrak{um}_1 \subset \mathfrak{um}_2 \subset A$. Portanto $\mathfrak{um}_1$ é um ideal de A. Vamos mostrar que $\mathfrak{u} \subsetneq \mathfrak{um}_1$.
De fato, se $\mathfrak{u} = \mathfrak{um}_1$, então $\alpha \in m_1$, será algébrico sobre A, e assim $\mathfrak{m}_1 \subset A$; mas como $\mathfrak{p}$ é maximal, na prova do lema anterior mostramos que $\mathfrak{m}_1 \subsetneq A$, logo $\mathfrak{u} \subsetneq \mathfrak{um}_1$, assim $\mathfrak{um}_1 \notin \mathfrak{U}$, portanto existe $\mathfrak{j}$, ideal fracionário de A tal que $(\mathfrak{um}_1)\mathfrak{j} = A$. Logo $\mathfrak{m}_1\mathfrak{j}$ é o inverso de $\mathfrak{u}$, portanto $\mathfrak{u} \notin \mathfrak{U}$, contradição . ■

Lema 1.12 *Seja* $\mathfrak{i}$ *um ideal não nulo de* A *e* $\mathfrak{n}$ *um ideal fracionário de* A *tal que* $\mathfrak{in} = A$*, então* $\mathfrak{n} = \{x \in K \mid x\mathfrak{i} \subset A\}$.

Demonstração: Se $x \in \mathfrak{n}$, então $x \in K$ e $x\mathfrak{i} \subset \mathfrak{ni} = A$, logo $\mathfrak{n} \subset \{x \in K \mid x\mathfrak{i} \subset A\}$. Consideremos agora $x \in K$ tal que $x\mathfrak{i} \subset A$, então , $xA = x\mathfrak{in} \subset A\mathfrak{n} = \mathfrak{n}$, assim $xA \subset \mathfrak{n}$, logo $x = x.1 \in \mathfrak{n}$. ■

Lema 1.13 *Seja* $\mathfrak{m}$ *um ideal fracionário não nulo de* K*, então existe* $\mathfrak{n}$ *ideal fracionário de* K *tal que* $\mathfrak{mn} = A$.

Demonstração: Seja $x \in A$ não nulo tal que $x\mathfrak{m} \subset A$. Como $x\mathfrak{m}$ é um ideal de A, então , pelo lema 1.11 existe $\mathfrak{j}$ ideal fracionário de A tal que $x\mathfrak{m}\mathfrak{j} = A$. Se $\mathfrak{n} = x\mathfrak{j}$, então $\mathfrak{n}$ é um ideal fracionário de A e $\mathfrak{mn} = A$.

Do lema 1.13, obtemos que todo ideal fracionário de A é inversível. Portanto, o conjunto formado pelos ideais fracionarios de A é um grupo com a multiplicação e tem como elemento neutro A. ■

Teorema 1.14 *Se* A *é um domínio de Dedekind, todo ideal de* A *pode ser escrito de modo único como um produto de ideais primos.*

Demonstração: Suponhamos que a família $\mathfrak{U}$ de ideais de A que não verificam o teorema é não vazia. Então $\mathfrak{U}$ tem elemento maximal $\mathfrak{i}$. Logo $\mathfrak{i}$ não é primo, e, portanto não é maximal. Assim, existe $\mathfrak{p}$ ideal maximal de A tal que $\mathfrak{i} \subsetneq \mathfrak{p}$, e, desse modo $\mathfrak{ip}^{-1} \subset \mathfrak{pp}^{-1} = A$. Assim $\mathfrak{ip}^{-1}$ é um ideal de A.
Se $\mathfrak{ip}^{-1} = \mathfrak{i}$, para todo $\alpha \in \mathfrak{p}^{-1}$, $\alpha\mathfrak{i} \subset \mathfrak{i}$ e, como $\mathfrak{i}$ é um A-módulo finitamente gerado, temos que $\alpha \in I_K(A) = A$. Desse modo $\mathfrak{p}^{-1} \subset A$; mas já mostramos que isto não acontece, então $\mathfrak{i} \neq \mathfrak{ip}^{-1}$, e para $x \in \mathfrak{i}$, $x = x.1 \in \mathfrak{i}A \subset \mathfrak{ip}^{-1}$, portanto $\mathfrak{i} \subsetneq \mathfrak{ip}^{-1}$, logo $\mathfrak{ip}^{-1} \notin \mathfrak{U}$, assim existem ideais primos $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ tais que $\mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{ip}^{-1}$, então $\mathfrak{pp}_1 \cdots \mathfrak{p}_n = \mathfrak{i}$, o que é uma contradição , logo $\mathfrak{U}$ é vazia.
Vamos mostrar agora que a fatoração é única. Sejam $\mathfrak{p}_1, \cdots, \mathfrak{p}_r, \mathfrak{q}_1, \cdots, \mathfrak{q}_s$, ideais primos de A tais que $\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$. Então $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subset \mathfrak{p}_1$. Como $\mathfrak{p}_1$ é primo,

existe i, suponhamos $i = 1$, tal que $\mathfrak{q}_i = \mathfrak{q}_1 \subset \mathfrak{p}_1$, como $\mathfrak{q}_1$ é maximal $\mathfrak{q}_1 = \mathfrak{p}_1$, assim temos que $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$. Se $r < s$, teríamos que $A = \mathfrak{q}_{r+1} \cdots \mathfrak{q}_s$, desse modo existiria $i \in \{r+1, \cdots, s\}$ tal que $A \subset \mathfrak{q}_i$, e assim $A = \mathfrak{q}_i$, o que contradiz o fato de que $\mathfrak{q}_i$ é maximal. Analogamente prova-se que $s \nleq r$, donde concluimos $r = s$ e existe $\sigma \in S_r$ (grupo de permutaçoes de r elementos) tal que $\mathfrak{p}_i = \mathfrak{q}_{\sigma(i)}$. ■

Observação :
Decorre do teorema anterior que, se M é um ideal fracionário de A, então existem ideais primos $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ e inteiros $m_1, \cdots, m_r$ tais que $M = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r}$.
Veja [2] p.74.

Definição 1.10 *Seja A um domínio de Dedekind, $\mathfrak{p}_1$ e $\mathfrak{p}_2$ ideais não nulos de A. Dizemos que $\mathfrak{p}_1$ divide $\mathfrak{p}_2$ se existir $\mathfrak{j}$ ideal de A tal que $\mathfrak{p}_1\mathfrak{j} = \mathfrak{p}_2$, nesse caso escrevemos $\mathfrak{p}_1 \mid \mathfrak{p}_2$.*

Corolário 1.15 *Seja A um domínio de Dedekind, $\mathfrak{p}_1$ e $\mathfrak{p}_2$ ideais não nulos de A. Então $\mathfrak{p}_1 \mid \mathfrak{p}_2$, se, e somente se, $\mathfrak{p}_1 \supset \mathfrak{p}_2$.*

Demonstração: Se $\mathfrak{p}_1 \mid \mathfrak{p}_2$ é claro que $\mathfrak{p}_1 \supset \mathfrak{p}_2$. Se $\mathfrak{p}_1 \supset \mathfrak{p}_2$, então
$A = \mathfrak{p}_1^{-1}\mathfrak{p}_1 \supset \mathfrak{p}_1^{-1}\mathfrak{p}_2$, e, portanto, $\mathfrak{j} = \mathfrak{p}_1^{-1}\mathfrak{p}_2$ é um ideal de A, com $\mathfrak{j}\mathfrak{p}_1 = \mathfrak{p}_2$. ■

Vamos agrora establecer um teorema que terá muita impotância no desenvolvimento desta disertação .

Teorema 1.16 *Sejam A um domínio de Dedekind, $K = Q(A)$, L extensão finita e separável de K e $B = I_L(A)$. Então B é um domínio de Dedekind.*

Para sua demostração precisamos de alguns resultados que provaremos em seguida.

Lema 1.17 *Seja A um domínio e L extensão de $Q(A)$, então $Q(I_L(A)) = I_L(Q(A))$. Em particular $Q(I_L(A)) = L$ se, e somente se, L for algébrico sobre $Q(A)$.*

Demonstração: Para provar que $Q(I_L(A)) \subset I_L(Q(A))$, temos que mostrar que $I_L(Q(A))$ é um subcorpo de L que contém $I_L(A)$.
De fato, dados $\alpha, \beta \in I_L(Q(A))$, então $\alpha - \beta$ e $\alpha\beta$ estão em $I_L(Q(A))$.
Suponhamos que $\beta \neq 0$, então existe $f(X) = c_0 + c_1X + \cdots + X^n \in Q(A)[X]$ tal que $f(\beta) = 0$. Como $\beta \neq 0$, então , existe $i = min\{j \in \{1, \cdots, n-1\} \mid c_j \neq 0\}$, e, assim $c_i\beta^i + c_{i+1}\beta^{i+1} + \cdots + \beta^n = 0$. Portanto:

$$\frac{\beta^n}{c_i}\left(\frac{1}{\beta^{n-i}} + \frac{c_{i+1}}{c_i}\frac{1}{\beta^{n-(i+1)}} + \cdots + \frac{1}{c_i}\right) = 0$$

Logo:

$$\frac{1}{\beta^{n-i}} + \frac{c_{i+1}}{c_i}\frac{1}{\beta^{n-(i+1)}} + \cdots \frac{1}{c_i} = 0$$

assim, $\beta^{-1} \in I_L(Q(A))$. Desse modo $I_L(Q(A))$ é corpo. ■

Vamos provar agora que $Q(I_L(A)) \supset I_L(Q(A))$. Seja $\gamma \in I_L(Q(A))$. Então existem $a_1, \cdots, a_n \in A$ e $b_1, \cdots, b_n \in A - \{0\}$ tais que:

$$\gamma^n + \frac{a_1}{b_1}\gamma^{n-1} + \cdots + \frac{a_{n-1}}{b_{n-1}}\gamma + \frac{a_n}{b_n} = 0.$$

Seja $b = \prod_{i=1}^{n} b_i$, então $b \in A$, e $b\gamma^n + \theta_1\gamma^{n-1} + \cdots + \theta_{n-1}\gamma + \theta_n = 0$, onde
$\theta_i = ba_ib_i^{-1} \in A$ para $1 \leq i \leq n$.

Multiplicando por b^{n-1}, tem-se que:

$$(b\gamma)^n + \theta_1(b\gamma)^{n-1} + \theta_2 b(b\gamma)^{n-2} + \cdots + \theta_n b^{n-1} = 0$$

Assim, se $h(X) = X^n + \theta_1 X^{n-1} + \theta_2 bX^{n-2} + \cdots + \theta_n b^{n-1} \in A[X]$, então $h(b\gamma) = 0$, logo $b\gamma = a \in I_L(A)$ e como $b \in A$, tem-se que $\gamma \in Q(I_L(A))$. ■

Lema 1.18 *Seja A um subanel de S e S subanel de um corpo, então* $I_S(A) = I_S(I_S(A))$

Demonstração: Sabemos que $A \subset I_S(A) \subset S$, e, assim $I_S(A) \subset I_S(I_S(A)) \subset S$. Seja $\alpha \in I_S(I_S(A))$, então existe $f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0 \in I_S(A)[X]$, tal que $f(\alpha) = 0$. Desse modo α é inteiro sobre $S' = S[a_1, \cdots, a_{m-1}]$, e, portanto $S'[\alpha]$ é um S'-módulo finitamente gerado. Sabemos que $a_i \in S'$ é inteiro sobre A, logo $S'[\alpha]$ é um A-módulo finitamente gerado. E, finalmente, como $S'[\alpha]$ é subanel de S temos que α é inteiro sobre A. ■

• Sejam A, B, K e L como no teorema 1.16, então B é integralmente fechado.
De fato, como L é extensão finita de K, pelo lema 1.17 temos $Q(B) = Q(I_L(A)) = L$, então $I_{Q(B)}(B) = I_L(B) = I_L(I_L(A)) = I_L(A) = B$, onde a penúltima igualdade é conseqüência do lema 1.18. ■

Lema 1.19 *Sejam A e S domínios tais que S é inteiro sobre A. Então :*

1. *Se* $\mathfrak{u}$ *é um ideal não nulo de S,* $\mathfrak{u} \cap A$*, é um ideal não nulo de A.*

2. $U(S) \cap A = U(A)$.

3. *S é corpo se, e somente se, A é corpo.*

4. *Um ideal primo $\mathfrak{p}$ de S é maximal em S se, e somente se, $\mathfrak{p} \cap A$, é maximal em A.*

Demonstração:
1) Seja $\alpha \in \mathfrak{u}$ não nulo. Então $\alpha \in S = I_S(A)$, e existe $f(X)$ de grau mínimo, $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in A[X]$ tal que $f(\alpha) = 0$. Então $a_0 \neq 0$, mas $a_0 = -\alpha(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1) \in \alpha\mathfrak{u} \cap A \subset \mathfrak{u} \cap A$, logo $\mathfrak{u} \cap A$ é um ideal não nulo de A.
2) É claro que $U(A) \subset U(S) \cap A$. Seja $\alpha \in U(S) \cap A$. Então $\alpha^{-1} \in S$, e existem $c_1, \cdots, c_m \in A$, tais que $\alpha^{-m} + c_1\alpha^{-m+1} + \cdots + c_m = 0$.
Multiplicando por α^{m-1} tem-se que $\alpha^{-1} + c_1 + c_2\alpha + \cdots + c_m\alpha^{m-1} = 0$, e
$\alpha^{-1} = -(c_1 + c_2\alpha + \cdots + c_m\alpha^{m-1}) \in A$.
3) Suponhamos que S é corpo então $U(A) = U(S) \cap A = S^* \cap A = A^*$, e assim A é corpo.
Se S não é corpo existe $\mathfrak{u}$ ideal não nulo de S tal que $\mathfrak{u} \neq S$, logo $1 \notin \mathfrak{u}$, pelo item 1, $\mathfrak{u} \cap A$ é ideal não nulo de A, e como $\mathfrak{u} \cap A \neq A$, A não é corpo.
4) Seja $\mathfrak{p}$ um ideal primo de S. Consideremos $\pi : S \longrightarrow S/\mathfrak{p}$ a projeção canônica, vamos mostrar que $\pi(S)$=$S/\mathfrak{p}$ é inteiro sobre $\pi(A)$. De fato, se $\bar{\gamma} \in \pi(S)$, então $\bar{\gamma} = \pi(\gamma)$ para algum $\gamma \in S$, então existe $h(X) = a_n + a_{n-1}X + \cdots + X^n \in A[X]$ tal que $h(\gamma) = 0$.
Consideremos agora $\bar{h}(X) = \pi(a_n) + \pi(a_{n-1})X + \cdots + X^n \in \pi(A)[X]$, então $\bar{h}(\bar{\gamma}) = \bar{0}$, e $\bar{\gamma}$ é inteiro sobre $\pi(A)$.
Para $r \in A$, $r \in \ker\pi \iff \pi(r) = \mathfrak{p} \iff r \in \mathfrak{p}$; mas $r \in A$, então a restrição de π a A tem como kernel $\mathfrak{p} \cap A$, assim $A/A\cap\mathfrak{p} \cong \pi(A)$.
Agora $\mathfrak{p}$ é maximal em S se, e somente se, $S/\mathfrak{p}$ é corpo, o que por 3 ocorrera se, e somente se, $\dfrac{A}{A \cap \mathfrak{p}}$ for um corpo se, o que equivale a dizer que $A \cap \mathfrak{p}$ é maximal em A. ■

• Sejam A, B, K e L como no teorema 1.16, vamos provar que todo ideal primo não nulo de de B é maximal.
De fato, se $\mathfrak{P}$ é um ideal primo de não nulo de de B, então , pelo item 1) do lema anterior, $\mathfrak{P} \cap A$ é um ideal primo não nulo de A. Como A é domínio de Dedekind, $\mathfrak{P} \cap A$ é um ideal maximal de A. Logo, pelo item 4, $\mathfrak{P}$ é um ideal maximal de B.■

Para mostrar o teorema 1.13 só falta provar o seguinte lema.

Lema 1.20 *B é noetheriano*

Demonstração: Suponhamos que $[L\colon K] = n$ e seja $\{\theta_1, \cdots, \theta_n\}$ uma base de $L \mid K$. Agora para $\theta_j \in \{\theta_1, \cdots, \theta_n\}$, θ_j é algébrico sobre K.
Assim, existem $a_0^j, \cdots, a_{n-1}^j \in A$ e $b_0^j, \cdots, b_{n-1}^j \in A^*$ tais que:

$$\frac{a_0^j}{b_0^j} + \frac{a_1^j}{b_1^j}\theta_j + \cdots + \frac{a_{n-1}^j}{b_{n-1}^j}\theta_j^{n-1} + \theta_j^n = 0$$

Seja $b_j = \prod_{i=1}^{n} b_i^j \in A^*$, então $b_j\theta_j \in I_L(A)$ para $j \in \{1, \cdots, n\}$. Finalmente, se $b = \prod_{j=1}^{n} b_j$ e $w_j = b\theta_j$, temos que $\mathbb{B}$=$\{w_1, \cdots, w_n\}$ é uma base de $L \mid K$, onde cada $w_j \in I_L(A)$.
Se α é um elemento não nulo de L, a função $T_{L|K}(\alpha x)$ definida em L é um elemento do espaço dual de L (considerado como K-espaço vetorial) e induz um homomorfismo ϕ de L no seu espaço dual. Por outro lado, sabemos que $T_{L|K}$ é uma aplicação K-linear não degenerada (Pois $L \mid K$ é separavel). Assim o homomorfismo induzido é um isomorfismo.
Seja agora $\mathbb{B}^* = \{w_1^*, \cdots, w_n^*\}$ a base dual de $\mathbb{B}$, então $\{w_1', \cdots, w_n'\}$ é base de $L \mid K$, onde $\phi(w_i') = w_i^*$, como $w_i^*(w_j) = \delta_{ij}$, então :

$$T_{L|K}(w_i' w_j) = \phi(w_i')(w_j) = w_i^*(w_j) = \delta_{ij}.$$

Consideremos agora $c \in A^*$ tal que cw_i' é inteiro sobre A. Seja $z \in B$, então $zcw_i' \in B$. Logo $T_{L|K}(zcw_i') = cT_{L|K}(zw_i') \in A$. Agora, como $z \in L$, temos que $z = y_1w_1 + \cdots + y_nw_n$, com $y_i \in K$, assim $T_{L|K}(zw_i') = y_i$, conseqüentemente $cy_i \in A$ portanto:

$$z = (y_1c)(c^{-1}w_1) + \cdots + (y_nc)(c^{-1}w_n) \in A(c^{-1}w_1) + \cdots + A(c^{-1}w_n)$$

logo B é um A-submódulo de um A-módulo noetheriano, e, assim todo ideal de B é um submódulo de um módulo noetheriano, portanto sera finitamente gerado.■

Observação : Seja L uma extensão separável de $K = Q(A)$ de grau n.
Se $\{w_1, \cdots, w_n\}$ é uma base de $L \mid K$, sem perdida de generalidade podemos supor que tal que cada w_i é inteiro sobre A.

Teorema 1.21 ***Teorema* Chinês do Resto***:*
Seja A um domínio, $\mathfrak{u}_1, \cdots, \mathfrak{u}_n$ *ideais de A tais que* $\mathfrak{u}_i + \mathfrak{u}_j = A$ *(são comaximais),* $\forall\, i \neq j$. *Dados* $x_1, ...x_n \in A$, *existe* $x \in A$ *tal que* $x \equiv x_i \,(mod\, \mathfrak{u}_i)$.

Veja [3] p.11.

Teorema 1.22 *Seja A um domínio de Dedekind. Se o número de ideais primos de A é finito, então A é um DIP.*

Demonstração: Sejam $\mathfrak{P}_1, \cdots, \mathfrak{P}_n$ os ideais primos de A. Como $\mathfrak{P}_1$ é maximal, $\mathfrak{P}_1^2 \subsetneq \mathfrak{P}_1$, e, assim, existe $r_1 \in \mathfrak{P}_1 - \mathfrak{P}_1^2$. Alem disso $\mathfrak{P}_1^2 \nsubseteq \mathfrak{P}_i$ e cada $\mathfrak{P}_i$ é maximal para qualquer $i \in \{2, \cdots, n\}$. Portanto os ideais $\mathfrak{P}_1^2, \mathfrak{P}_2 \cdots, \mathfrak{P}_n$ são comaximais dois a dois, assim pelo teorema chinês do resto existe $r \in A$ tal que $r \equiv r_1 (mod \mathfrak{P}_1^2)$ e $r \equiv 1 (mod \mathfrak{P}_i)$, com $i \in \{2, \cdots, n\}$. Portanto $r \in \mathfrak{P}_1$, $r \notin \mathfrak{P}_1^2$ e $r \notin \mathfrak{P}_i$ para qualquer $i \in \{2, \cdots, n\}$, logo $(r) \subset \mathfrak{P}_1$,$(r) \nsubseteq \mathfrak{P}_1^2$ e $(r) \nsubseteq \mathfrak{P}_i$, $i \in \{2, \cdots, n\}$.
Como $(r) = \mathfrak{P}_1^{k_1} \cdots \mathfrak{P}_n^{k_n}$, $k_i \in \mathbb{N}$, então para $i \in \{2, \cdots, n\}$ $k_i = 0$ desse modo $(r) = \mathfrak{P}_1^{k_1}$, portanto $k_1 = 1$ e $\mathfrak{P}_1$ é principal. Analogamente prova-se que os outros $\mathfrak{P}_i$ são principais, e, como todo ideal de A é produto de potencias dos $\mathfrak{P}_i$, então todo ideal de A é principal. ■

1.3 Localização

Seja A um domínio contido em um corpo L e K o seu corpo de frações .

Definição 1.11 *Seja S um subconjunto de A. Dizemos que S é um subconjunto multiplicativo, se valem as seguintes condições:*

1. $0 \notin S$, $1 \in S$.
2. $x, y \in S$, *implica* $xy \in S$.

Definição 1.12 *Seja* $K = Q(A)$ *e S um subconjunto multiplicativo de A, definimos* $S^{-1}(A)$ *como o conjunto* $\left\{ \frac{x}{s} \,\middle|\, x \in A, s \in S \right\}$. *Então* $S^{-1}(A)$ *é um subanel de K que contém A.*

Seja M um A-módulo contido em um corpo L que contém K, definimos:

$S^{-1}M = \left\{ \frac{m}{s} \,\middle|\, m \in M, s \in S \right\}$, *assim* $S^{-1}M$ *é um* $S^{-1}A$ *módulo.*

Proposição 1.23 *Sejam A um domínio, B um anel inteiro sobre A e S um subconjunto multiplicativo de A. Então $S^{-1}B$ é inteiro sobre $S^{-1}A$ e, se A é integralmente fechado, então $S^{-1}A$ é integralmente fechado.*

Demonstração: Seja $y \in S^{-1}B$. Então $y = s^{-1}x$, para algum $s \in S$ e $x \in B$; por hipótese, x é inteiro sobre A, e, assim existe um A-módulo $M \subset B$, finitamente gerado tal que $xM \subset M$. Agora $S^{-1}M$ é um $S^{-1}A$-módulo finitamente gerado e $yS^{-1}M = (s^{-1}x)S^{-1}M = s^{-1}S^{-1}xM \subset S^{-1}M$, logo y é inteiro sobre $S^{-1}A$.
Suponhamos agora que A é integralmente fechado. Sabemos que $A \subset S^{-1}A \subset K$, então $K = Q(S^{-1}A)$.
Seja $\alpha \in K$ inteiro sobre $S^{-1}A$. Então existe $f(X) = X^n + b_{n-1}s_{n-1}^{-1}X^{n-1} + \cdots + b_0 s_0^{-1} \in S^{-1}A[X]$ tal que $f(\alpha) = 0$. Agora se $s = \prod_{i=1}^{n} s_i$, então $s \in S$ e $\alpha s \in I_K(A) = A$, logo $\alpha = as^{-1}$, para algum $a \in A$, assim $\alpha \in S^{-1}A$. ■

Proposição 1.24 *Seja $\mathfrak{p}$ um ideal primo de A, então $S_{\mathfrak{p}} = A - \mathfrak{p}$ é um subconjunto multiplicativo de A.*

Demonstração: É claro que $0 \notin S_{\mathfrak{p}}$, $1 \in S_{\mathfrak{p}}$.
Sejam $x, y \in S_{\mathfrak{p}}$, então $x, y \in A$ e $x, y \notin \mathfrak{p}$. É claro que $xy \in A$ se $xy \in \mathfrak{p}$, então $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$, o que é um absurdo, logo $xy \in S_{\mathfrak{p}}$. ■

Proposição 1.25 *Se $\mathfrak{u}$ é um ideal de $S^{-1}A$, então $\mathfrak{u} = S^{-1}(A \cap \mathfrak{u})$.*

Demonstração: Seja $y \in S^{-1}(A \cap \mathfrak{u})$. Então $y = \dfrac{x}{s}$ com $x \in A \cap \mathfrak{u}$ e $s \in S$. Agora, como $x \in \mathfrak{u}$ e $s^{-1} \in S^{-1}A$, $y \in \mathfrak{u}$, portanto $S^{-1}(A \cap \mathfrak{u}) \subset \mathfrak{u}$.
Se $y \in \mathfrak{u}$, $y = \dfrac{x}{s}$ com $x \in A$ e $s \in S$. Logo $x = sy \in \mathfrak{u}$, e, assim $x \in A \cap \mathfrak{u}$. Portanto, $y \in S^{-1}(A \cap \mathfrak{u})$, e $S^{-1}(A \cap \mathfrak{u}) \supset \mathfrak{u}$. ■

Proposição 1.26 *Seja A um domínio de Dedekind e S um subconjunto multiplicativo de A. Então $S^{-1}A$ é um domínio de Dedekind.*

Demonstração: Seja $\mathfrak{u}$ um ideal de $S^{-1}A$. Então $\mathfrak{u} \cap A$ é um ideal de A e, portanto, é um A-módulo finitamente gerado. Assim $\mathfrak{u} \cap A = a_1A + \cdots + a_nA$, com $a_1, \cdots, a_n \in A$. Pela proposição anterior $\mathfrak{u} = S^{-1}(A \cap \mathfrak{u})$, e, desse modo $\mathfrak{u} = a_1S^{-1}A + \cdots + a_nS^{-1}A$. Logo $\mathfrak{u}$ é um $S^{-1}A$ módulo finitamente gerado.
Pela proposição 1.23 sabemos que $S^{-1}A$ é integralmente fechado.
Seja agora $\mathfrak{u}$ um ideal primo não nulo de $S^{-1}A$. Então $\mathfrak{u} \cap A$ é também um ideal primo não nulo de de A pois se $\mathfrak{u} \cap A = (0)$, então $\mathfrak{u} = S^{-1}(A \cap \mathfrak{u}) = (0)$, e, assim,

$\mathfrak{u} \cap A$ é ideal maximal de A. Seja $\mathfrak{n}$ um ideal de $S^{-1}A$ tal que $\mathfrak{u} \subset \mathfrak{n} \subsetneq S^{-1}A$, então $\mathfrak{u} \cap A \subset \mathfrak{n} \cap A \subsetneq A$, pois $1 \notin \mathfrak{n} \cap A$, logo $\mathfrak{u} \cap A = \mathfrak{n} \cap A$, e desse modo $S^{-1}(\mathfrak{u} \cap A) = S^{-1}(\mathfrak{n} \cap A)$. Portanto $\mathfrak{u} = \mathfrak{n}$ e $\mathfrak{u}$ é maximal. ■

Definição 1.13 *Um domínio A é dito local se só tem um ideal maximal.*

Exemplo 1.4 *Seja p primo e $n \in \mathbb{N}$. O anel $\mathbb{Z}_{p^n}$ é um anel local cujo ideal maximal é $\langle p \rangle$.*

De fato, notemos que $\langle p \rangle = p\mathbb{Z}_{p^n} \cong p\mathbb{Z}/\langle p^n \rangle \cong \mathbb{Z}/\langle p^{n-1} \rangle \cong \mathbb{Z}_{p^{n-1}}$, assim $|\langle p \rangle| = p^{n-1}$, portanto $\langle p \rangle$ é ideal maximal de $\mathbb{Z}_{p^n}$.
Seja J um ideal maximal de $\mathbb{Z}_{p^n}$,e suponhamos que existe $x \in J$ tal que $x \notin \langle p \rangle$, então $mdc(x, p) = 1$, desse modo $mdc(x, p^n) = 1$, assim existem $r, s \in \mathbb{Z}$ tais que $rx + sp^n = 1$, logo $rx = 1$ em $\mathbb{Z}_{p^n}$ e consequentemente $J = \mathbb{Z}_{p^n}$ o que é um absurdo. ■

Proposição 1.27 *Se A é local e $\mathfrak{p}$ seu ideal maximal, então $\mathfrak{p} = A - U(A)$.*

Demonstração: Se $x \notin \mathfrak{p}$ é tal que $x \notin U(A)$, então $\langle x \rangle \neq A$, logo $\langle x \rangle$ está contido em um ideal maximal de A e, portanto, $\langle x \rangle \subset \mathfrak{p}$. Em particular, $x \in \mathfrak{p}$, absurdo. Portanto $x \in U(A)$ assim $A - U(A) \subset \mathfrak{p}$. Como $\mathfrak{p} \neq A$, então $x \in \mathfrak{p}$ implica $x \notin U(A)$. Assim $A - U(A) \supset \mathfrak{p}$. ■

Proposição 1.28 *Sejam A um anel e $\mathfrak{p}$ um ideal primo de A. Então o anel $A_\mathfrak{p} = S_\mathfrak{p}^{-1}A$ é um anel local com ideal maximal $m_\mathfrak{p} = A_\mathfrak{p} - U(A_\mathfrak{p})$.*

Demonstração: Temos que $m_\mathfrak{p} = \{ps^{-1} \mid p \in \mathfrak{p}, s \in S_\mathfrak{p}\}$. Como $\mathfrak{p}$ é primo, $m_\mathfrak{p}$ é um ideal de $A_\mathfrak{p}$. Vamos mostrar que é maximal.
Seja I um ideal de $A_\mathfrak{p}$ tal que $m_\mathfrak{p} \subsetneq I \subset A_\mathfrak{p}$. Então existe $xs^{-1} \in I - m_\mathfrak{p}$, portanto $xs^{-1} \in U(A_\mathfrak{p})$, logo $I = A_\mathfrak{p}$ e $m_\mathfrak{p}$ é um ideal maximal de $= A_\mathfrak{p}$.
Vamos provar agora que $m_\mathfrak{p}$ é o unico ideal maximal de $A_\mathfrak{p}$. De fato, se $\widetilde{I} \neq m_\mathfrak{p}$ é um ideal maximal de $A_\mathfrak{p}$, então $\widetilde{I} \nsubseteq m_\mathfrak{p}$ logo existe $xs^{-1} \in \widetilde{I} - m_\mathfrak{p}$ assim temos novamente que $\widetilde{I} = A_\mathfrak{p}$ o que é uma contradição . Por tanto $m_\mathfrak{p}$ é o unico ideal maximal de $A_\mathfrak{p}$ e $A_\mathfrak{p}$ é local. ■

Proposição 1.29 *$m_\mathfrak{p} \cap A = \mathfrak{p}$ e $\mathfrak{p}A_\mathfrak{p} = m_\mathfrak{p}$.*

Demonstração: É claro que $m_\mathfrak{p} \cap A \supset \mathfrak{p}$, reciprocamente se $y = s^{-1}x \in m_\mathfrak{p} \cap A$, então $x \in \mathfrak{p}$ e $s \in S_\mathfrak{p}$, assim $x = sy \in \mathfrak{p}$ e como $\mathfrak{p}$ é primo temos que $y \in \mathfrak{p}$. Portanto $m_\mathfrak{p} \cap A = \mathfrak{p}$ e é claro que $\mathfrak{p}A_\mathfrak{p} = m_\mathfrak{p}$. ■

Definição 1.14 *Seja B um anel que contém A, $\mathfrak{p}$ um ideal primo de A e $\mathfrak{P}$ um ideal primo de B. Dizemos que $\mathfrak{P}$ está acima de $\mathfrak{p}$ se $\mathfrak{P} \cap A = \mathfrak{p}$. Nesse caso escrevemos $\mathfrak{P} \mid \mathfrak{p}$.*

Exemplo 1.5 *Se $\mathfrak{p}$ é ideal primo de um domínio A, pela proposição 1.29 temos que $m_{\mathfrak{p}}$ está acima de $\mathfrak{p}$.*

Lema 1.30 Lema de Nayakama: *Sejam A um domínio e $\mathfrak{n}$ um ideal de A contido em todos os ideais maximais de A. Se M é um A-módulo finitamente gerado e $\mathfrak{n}M = M$, então $M = (0)$.*

Demonstração: Suponhamos que M é gerado por $\{w_1, \cdots, w_n\}$. Então $w_1 \in M = \mathfrak{n}M$, logo $w_1 = \sum_{i=1}^{n} \alpha_i m_i$, com $\alpha_i \in \mathfrak{n}$ e $m_i \in M$. Como M é gerado por $\{w_1, \cdots, w_n\}$ e $\mathfrak{n}$ é ideal de A, tem-se que $w_1 = a_1 w_1 + \cdots + a_n w_n$ com $a_i \in \mathfrak{n}$ e desse modo $(1 - a_1)w_1 = a_2 w_2 + \cdots + a_n w_n$.
Se $1 - a_1 \notin U(A)$, existe $\mathfrak{N}$ ideal maximal de A tal que $(1 - a_1) \subset \mathfrak{N}$, e, em particular, $1 - a_1 \in \mathfrak{N}$; mas $a_1 \in \mathfrak{n} \subset \mathfrak{N}$, logo $1 = (1 - a_1) + a_1 \in \mathfrak{N}$, e, $\mathfrak{N} = A$, absurdo. Por tanto $1 - a_1 \in U(A)$, escrevendo $w_1 = a_2(1 - a_1)^{-1} w_2 + \cdots + a_n(1 - a_1)^{-1} w_n$, temos que M é gerado por $n - 1$ elementos, seguindo esse raciocinio prova-se que M é gerado por um elemento w, e, novamente, como $M = \mathfrak{n}M$, tem-se $w = aw$, com $a \in \mathfrak{n}$, assim $(1 - a)w = 0$ e $1 - a \in U(A)$, portanto $w = 0$, e $M = (0)$. ■

Notação : Seja $\mathfrak{p}$ um ideal primo de um domínio A, e B um domínio que contém A denotamos por $B_{\mathfrak{p}}$ ao anel $S_{\mathfrak{p}}^{-1}B$.

Observação : Se B é inteiro sobre A, pela proposição 1.23, $B_{\mathfrak{p}}$ é inteiro sobre $A_{\mathfrak{p}}$ e $\mathfrak{p}B_{\mathfrak{p}} = \mathfrak{p}S_{\mathfrak{p}}^{-1}B = \mathfrak{p}S_{\mathfrak{p}}^{-1}AB = \mathfrak{p}A_{\mathfrak{p}}B = \mathfrak{p}A_{\mathfrak{p}}B_{\mathfrak{p}} = m_{\mathfrak{p}}B_{\mathfrak{p}}$.

Proposição 1.31 *Sejam A um domínio, B um domínio que é inteiro sobre A e $\mathfrak{p}$ um ideal primo de A então $\mathfrak{p}B \neq B$ e existe $\mathfrak{P}$ ideal primo de B acima de $\mathfrak{p}$.*

Demonstração: Vamos mostrar a primera afirmação no caso em que A é local.
Se $\mathfrak{p}B = B$, então $1 \in \mathfrak{p}B$, logo $1 = \sum_{i=1}^{n} a_i b_i$, com $a_i \in \mathfrak{p}$ e $b_i \in B$.
Seja $B_0 = A[b_1, \cdots, b_n]$, então $1 \in \mathfrak{p}B_0$. Além disso $\mathfrak{p}B_0$ é um ideal de B_0, então $\mathfrak{p}B_0 = B_0$, e como cada b_i é inteiro sobre A para $1 \leq i \leq n$, B_0 é um A-módulo finitamente gerado. Como $\mathfrak{p}$ está contido no único ideal maximal de A, então pelo lema de Nayakama, $B_0 = 0$, o que é absurdo, logo $\mathfrak{p}B_0 \neq B_0$.

No caso geral, se $\mathfrak{p}B = B$, $m_{\mathfrak{p}}B_{\mathfrak{p}} = B_{\mathfrak{p}}$; mas $B_{\mathfrak{p}}$ é inteiro sobre o anel local $A_{\mathfrak{p}}$. Portanto, $m_{\mathfrak{p}}B_{\mathfrak{p}} \neq B_{\mathfrak{p}}$, o que é uma contradição , logo $\mathfrak{p}B \neq B$.
Vamos provar agora que existe $\mathfrak{P}$ ideal primo de B acima de $\mathfrak{p}$. De fato, como $m_{\mathfrak{p}}$ é um ideal primo de $A_{\mathfrak{p}}$ e $B_{\mathfrak{p}}$ é inteiro sobre $A_{\mathfrak{p}}$, pelo que acabamos de mostrar temos que $m_{\mathfrak{p}}B_{\mathfrak{p}}$ é um ideal de $B_{\mathfrak{p}}$ e $m_{\mathfrak{p}}B_{\mathfrak{p}} \neq B_{\mathfrak{p}}$.
Logo $m_{\mathfrak{p}}B_{\mathfrak{p}}$ está contido em um ideal maximal $\mathfrak{n}$ de $B_{\mathfrak{p}}$, e, pelo lema 1.19 item 4, $\mathfrak{n}\cap A_{\mathfrak{p}}$ é um ideal maximal de $A_{\mathfrak{p}}$. Portanto $\mathfrak{n}\cap A_{\mathfrak{p}} = m_{\mathfrak{p}}$. Se $\mathfrak{P}=\mathfrak{n}\cap B$, então $\mathfrak{P}$ é um ideal primo de B e $\mathfrak{P} \cap A=\mathfrak{n}\cap B \cap A=\mathfrak{n}\cap A=\mathfrak{n}\cap A_{\mathfrak{p}} \cap A = m_{\mathfrak{p}} \cap A = \mathfrak{p}$, assim $\mathfrak{P}$ está acima de $\mathfrak{p}$. ■

Capítulo 2

Extensões de Galois

Neste capítulo, mostraremos que, dado um domínio de Dedekind A, K seu corpo de frações e $L \mid K$ uma extensão finita, o número de ideais primos de $B = I_L(A)$ acima de um dado ideal primo $\mathfrak{p}$ de A é finito. Depois mostraremos que se, L é extensão de Galois K, eles serão K-conjugados dois a dois, isto é, dados $\mathfrak{P}_1$ e $\mathfrak{P}_2$ ideais primos de B acima de $\mathfrak{p}$ existe $\sigma \in G(L/K)$ (grupo de Galois) tal que $\sigma\mathfrak{P}_1 = \mathfrak{P}_2$. Estudaremos também certos subgrupos do grupo de Galois $G(L/K)$, cujas ordens refletirão o comportamento da decomposição de $\mathfrak{p}B$ como produto de ideais primos de B.

Definição 2.1 *Seja $L \mid K$ de Galois. $L \mid K$ é dita abeliana (resp. ciclica), se $G(L \mid K)$ é abeliano (resp. cíclico).*

Teorema 2.1 *Sejam A um domínio integralmente fechado no seu corpo de frações K, L uma extensão finita e de Galois de K, $\mathfrak{p}$ ideal maximal de A e $\mathfrak{P}_1$ e $\mathfrak{P}_2$ ideais primos de $I_L(A)$ que estão acima de $\mathfrak{p}$, então existe $\sigma \in G(L \mid K)$ tal que $\sigma\mathfrak{P}_2 = \mathfrak{P}_1$.*

Demonstração: Suponhamos que, para todo $\sigma \in G(L \mid K)$, vale que $\sigma\mathfrak{P}_2 \neq \mathfrak{P}_1$. Como $\mathfrak{P}_1$ e $\sigma\mathfrak{P}_2$ estão acima de $\mathfrak{p}$, eles são ideais maximais de $I_L(A)$, assim $\mathfrak{P}_1 + \sigma\mathfrak{P}_2 = I_L(A) \,\forall\, \sigma \in G(L \mid K)$ e $\sigma_i\mathfrak{P}_2 + \sigma_j\mathfrak{P}_2 = I_L(A) \;\forall\, \sigma_i, \sigma_j \in G(L \mid K)$, com $i \neq j$.
Logo, pelo teorema chinês do resto (Teorema 1.21), existe $\alpha \in I_L(A)$ tal que $\alpha \equiv 0 \,(mod\, \mathfrak{P}_1)$ e $\alpha \equiv 1 \,(mod\, \sigma\mathfrak{P}_2) \;\forall\, \sigma \in G(L \mid K)$, assim $\alpha \in \mathfrak{P}_1$ e $\alpha \notin \sigma\mathfrak{P}_2$ $\forall\, \sigma \in G(L \mid K)$.

Agora, como $N_{L|K}(\alpha) = \prod_{\sigma \in G(L\,/\,K)} \sigma\alpha \in I_L(A) \cap K = I_K(A) = A$, temos que $N_{L|K}(\alpha) \in A$, mas $N_{L|K}(\alpha) = \alpha \prod_{\substack{\sigma \in G(L\,/\,K) \\ \sigma \neq id}} \sigma\alpha \in \mathfrak{P}_1$ pois $\mathfrak{P}_1$ é ideal de $I_L(A)$. Portanto $N_{L|K}(\alpha) \in \mathfrak{P}_1 \cap A = \mathfrak{p}$.
Como $\alpha \notin \sigma\mathfrak{P}_2 \, \forall \, \sigma \in G(L\,/\,K)$ então $\sigma\alpha \notin \mathfrak{P}_2 \; \forall \, \sigma \in G(L\,/\,K)$, e como $\mathfrak{P}_2$ é primo, tem-se que $N_{L|K}(\alpha) \notin \mathfrak{P}_2$, o que contradiz que $N_{L|K}(\alpha) \in \mathfrak{p} = \mathfrak{P}_2 \cap A$. ■

Corolário 2.2 *Sejam A um domínio integralmente fechado no seu corpo de frações K, E uma extensão finita e separável de K, $B = I_E(A)$ e $\mathfrak{p}$ um ideal maximal de A. Então o número de ideais primos de B que estão acima de $\mathfrak{p}$ é finito.*

Demonstração: Seja $L = K(\gamma, \gamma_2, \cdots, \gamma_n)$ onde γ é um elemento primitivo de $E\,/\,K$ e $\gamma_2, \cdots, \gamma_n$ são as outras raízes do polinômio minimal de γ. Temos que L a menor extensão de Galois de K que contém E.
Consideremos agora $\mathfrak{P}_1, \mathfrak{P}_2$ dois ideais primos de B que estão acima de $\mathfrak{p}$ e $C = I_L(A)$. Então $C = I_C(A) \subset I_C(B) \subset C$, logo $C = I_C(B)$, ou seja C é inteiro sobre B. Assim existem $\mathfrak{Q}_1$ e $\mathfrak{Q}_2$ ideais primos de C que estão acima de $\mathfrak{P}_1$ e $\mathfrak{P}_2$ respectivamente. Portanto $\mathfrak{Q}_1 \neq \mathfrak{Q}_2$, pois se $\mathfrak{Q}_1 = \mathfrak{Q}_2$, teriamos que $\mathfrak{Q}_1 \cap B = \mathfrak{Q}_2 \cap B$ e desse modo $\mathfrak{P}_1 = \mathfrak{P}_2$, então o número de ideais primos de B acima de $\mathfrak{p}$ é menor ou igual ao número de ideais primos de C acima de $\mathfrak{p}$ que por sua vez é menor ou igual a $|G(L\,/\,K)|$. ■

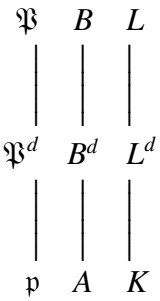
2.1 Grupos de Decomposição e Inércia

Definição 2.2 *Sejam A um domínio de Dedekind, L uma extensão finita e de Galois de K=Q(A), $\mathfrak{p}$ um ideal primo de A e $\mathfrak{P}$ ideal primo de $B = I_L(A)$ que está acima de $\mathfrak{p}$.*
Então $G_{\mathfrak{P}} = \{\sigma \in G(L\,/\,K) \mid \sigma\mathfrak{P}=\mathfrak{P}\}$ é um subgrupo de $G(L\,/\,K)$ chamado grupo de decomposição de $\mathfrak{P}$.

Definição 2.3 *O corpo fixo de $G_{\mathfrak{P}}$ denotado por L^d é chamado corpo de decomposição de $\mathfrak{P}$.*
Temos que $L^d = \{a \in L \mid \sigma(a) = a, \forall \, \sigma \in G_{\mathfrak{P}}\}$.

Proposição 2.3 *Sejam A um domínio integralmente fechado no seu corpo de frações K, L uma extensão finita e de Galois de K, $\mathfrak{p}$ um ideal primo de A e $\mathfrak{P}$ um ideal primo de $B = I_L(A)$ que está acima de $\mathfrak{p}$. Consideremos, $B^d = I_{L^d}(A) = I_L(A) \cap L^d$ e $\mathfrak{P}^d = \mathfrak{P} \cap B^d$. Então $\dfrac{A}{\mathfrak{p}} = \dfrac{B^d}{\mathfrak{P}^d}$.*

Demonstração:



Se $G_{\mathfrak{P}} = G(L\,/\,K)$. Então $L^d = K$, desse modo $B^d = I_{L^d}(A) = I_K(A) = A$ e $\mathfrak{P}^d = \mathfrak{P} \cap B^d = \mathfrak{P} \cap A = \mathfrak{p}$, assim temos o resultado.
Suponhamos então que $G_{\mathfrak{P}} \subsetneq G(L\,/\,K)$. Seja $\sigma \in G(L\,/\,K) - G_{\mathfrak{P}}$, temos que $\sigma\mathfrak{P} \neq \mathfrak{P}$ e $\sigma^{-1}\mathfrak{P} \neq \mathfrak{P}$, como B^d é inteiro sobre A e $\mathfrak{P}^d$ está acima de $\mathfrak{p}$, então $\mathfrak{P}^d$ é um ideal maximal de B^d. Considere $\mathfrak{P}^d_\sigma = \sigma^{-1}\mathfrak{P} \cap B^d$ então $\mathfrak{P}^d \neq \mathfrak{P}^d_\sigma$, pois se $\mathfrak{P}^d = \mathfrak{P}^d_\sigma$ teríamos que $\mathfrak{P}$ e $\sigma^{-1}\mathfrak{P}$, estariam acima de $\mathfrak{P}^d$, logo existiria $\lambda \in G(L/L^d) = G_{\mathfrak{P}}$ tal que $\lambda(\mathfrak{P}) = \sigma^{-1}\mathfrak{P}$ e desse modo $\sigma\mathfrak{P} = \mathfrak{P}$, o que é um absurdo.
Agora como $\mathfrak{P}^d$ e $\mathfrak{P}^d_\sigma$ são ideais maximais distintos de B^d, então $\mathfrak{P}^d + \mathfrak{P}^d_\sigma = B^d$, assim pelo teorema chinês do resto, temos que, para $x \in B^d$ existe $y \in B^d$ tal que $y \equiv x\,(mod\,\mathfrak{P}^d)$ e $y \equiv 1\,(mod\,\mathfrak{P}^d_\sigma)$, logo, em particular $y \equiv x\,(mod\,\mathfrak{P})$ e $y \equiv 1\,(mod\,\sigma^{-1}\mathfrak{P})$, da segunda congruencia temos que $\sigma y \equiv 1\,(mod\,\mathfrak{P})$, para todo $\sigma \notin G_{\mathfrak{P}}$.
Como L^d é extensão separável de K, então $N_{L^d|K}(y) = \prod \tau(y) = y \prod_{\hat{\tau} \notin G_{\mathfrak{P}}} \hat{\tau}(y)$, onde τ_i , são K-imerções de L^d, em subcorpos de $\bar{K}$ e $G(L\,/\,K) = i_d G_{\mathfrak{P}} \cup \tau_2 G_{\mathfrak{P}} \cdots \cup \tau_k G_{\mathfrak{P}}$, onde a união é disjunta.
Logo $N_{L^d|K}(y) \equiv x\,(mod\,\mathfrak{P})$; por outro lado $N_{L^d|K}(y) \in K$ é inteiro sobre A, então $N_{L^d|K}(y) \in A$, dessa manera $N_{L^d|K}(y) \in B^d$ e como $x \in B^d$, $N_{L^d|K}(y) \equiv x\,(mod\,\mathfrak{P} \cap B^d)$ assim $N_{L^d|K}(y) \equiv x\,(mod \mathfrak{P}^d)$.
Seja agora $i\colon A/\mathfrak{p} \longrightarrow B^d/\mathfrak{P}^d$, tal que $i(x + \mathfrak{p}) = x + \mathfrak{P}^d$, como $\mathfrak{p} \subset \mathfrak{P}^d$, i está bem definida e é um monomorfismo, agora para $x \in B^d$ existe $w = N_{L^d|K}(y)$, tal que $w - x \in \mathfrak{P}^d$ logo $i(w + \mathfrak{p}) = x + \mathfrak{P}^d$, assim a inclusão é sobrejetora e portanto é identidade e desse modo $\dfrac{A}{\mathfrak{p}} = \dfrac{B^d}{\mathfrak{P}^d}$. ■

Teorema 2.4 *Seja A um domínio de Dedekind, L uma extensão finita e de Galois de K=Q(A),* $\mathfrak{p}$ *um ideal primo de A e* $\mathfrak{P}$ *ideal primo de* $B = I_L(A)$ *que está acima de* $\mathfrak{p}$*. Então* $\frac{B}{\mathfrak{P}}$ *é um espaço vetorial de dimensão finita sobre* $\frac{A}{\mathfrak{p}}$ *e* $\frac{A}{\mathfrak{p}}$ *pode ser identificado com um subcorpo de* $\frac{B}{\mathfrak{P}}$*.*

Demonstração: A aplicação $\psi\colon \frac{A}{\mathfrak{p}} \longrightarrow \frac{B}{\mathfrak{P}}$, tal que $\psi(a+\mathfrak{p}) = a+\mathfrak{P}$ é um monomorfismo. Então $\frac{A}{\mathfrak{p}}$ pode ser identificado com um subcorpo de $\frac{B}{\mathfrak{P}}$.
Como A é um domínio de Dedekind, B também é, logo, em particular, B é um A-módulo finitamente gerado. Assim $\frac{B}{\mathfrak{P}}$ é um $\frac{A}{\mathfrak{p}}$-módulo finitamente gerado, e, portanto, um espaço vetorial de dimensão finita sobre $\frac{A}{\mathfrak{p}}$. ■

Observações:
Seja A um dominio de Dedekind, K o corpo de frações de A, $L \,/\, K$ Galois finita e $B = I_L(A)$. Então :
• Para todo $\sigma \in G(L \,/\, K)$, $\sigma B = B$.
• Para $\sigma \in G_{\mathfrak{P}}$, seja $\bar{\sigma}\colon \frac{B}{\mathfrak{P}} \longrightarrow \frac{B}{\mathfrak{P}}$ tal que $\bar{\sigma}(x+\mathfrak{P}) = \sigma(x)+\mathfrak{P}$, temos que $\bar{\sigma} \in Aut(B/\mathfrak{P})$ e fixa $A/\mathfrak{p}$.

Portanto, temos que, a cada $\sigma \in G_{\mathfrak{P}}$ podemos associar um automorfismo $\bar{\sigma}$ de $B \,/\, \mathfrak{P}$ sobre $A \,/\, \mathfrak{p}$, e o mapeo dado por $\sigma \mapsto \bar{\sigma}$ é um homomorfismo de grupos.

Teorema 2.5 *Sejam A um domínio de Dedekind, L uma extensão finita e de Galois de K=Q(A),* $\mathfrak{p}$ *um ideal primo de A e* $\mathfrak{P}$ *ideal primo de* $B = I_L(A)$ *que está acima de* $\mathfrak{p}$*.*
Se $\frac{B}{\mathfrak{P}}$ *é uma extensão separável de* $\frac{A}{\mathfrak{p}}$*, então ela é normal e, portanto, de Galois. Além disso a aplicação* $\sigma \mapsto \bar{\sigma}$ *é um epimorfismo de* $G_{\mathfrak{P}}$ *sobre* $G\big((B/\mathfrak{P}) \,/\, (A/\mathfrak{p})\big)$*.*

Demonstração: Como $\frac{B}{\mathfrak{P}}$ é uma extensão finita e separável de $\frac{A}{\mathfrak{p}}$, existe $\bar{\gamma}$, elemento primitivo de $\frac{B}{\mathfrak{P}}$ sobre $\frac{A}{\mathfrak{p}}$. Seja $\bar{\gamma} = \gamma + \mathfrak{P}$, com $\gamma \in B$. Então $\gamma \in L$, e $L \,/\, L^d$ é de Galois.
Seja $h(X) = X^r + a_{r-1}X^{r-1} + \cdots + a_0 \in L^d[X]$, o polinômio minimal de γ sobre L^d,

como $\gamma \in B$, pelo item 1 do Teorema 1.1, os coeficientes de h estão em A.

Além disso, $h(X) = \prod_{\sigma \in G(L\,/\,L^d)} (x - \sigma(\gamma)) = \prod_{\sigma \in G_{\mathfrak{P}}} (x - \sigma(\gamma))$.
Consideremos agora:

$$\bar{h}(X) = (1 + \mathfrak{P})X^r + (a_{r-1} + \mathfrak{P})X^{r-1} + \cdots + (a_0 + \mathfrak{P}) \in (B^d/\mathfrak{P})[X] = (A/\mathfrak{p})[X].$$

Como $\bar{\gamma}$ é elemento primitivo de $B/\mathfrak{P}$ sobre $A/\mathfrak{p}$, as raízes de $\bar{h}$ são da forma $\bar{\sigma}(\bar{\gamma})$ com $\sigma \in G_{\mathfrak{P}}$ então $\bar{h}(X) = \prod_{\sigma \in G_{\mathfrak{P}}} (X - \bar{\sigma}(\bar{\gamma}))$, assim todas as raízes de $\bar{h}$ estão em $\dfrac{B}{\mathfrak{P}}$, logo $\dfrac{B}{\mathfrak{P}}$ é corpo de raízes de $\bar{h}$, e $\dfrac{B}{\mathfrak{P}}$ é extensão normal de $\dfrac{A}{\mathfrak{p}}$.

Seja agora $\phi \in G\big((B/\mathfrak{P})\,/\,(A/\mathfrak{p})\big)$, então ϕ é determinado por sua ação em γ e como todos os conjugados de γ são da forma $\bar{\sigma}(\bar{\gamma})$, com $\sigma \in G_{\mathfrak{P}}$, temos que $\phi = \bar{\sigma}$ para algum $\sigma \in G_{\mathfrak{P}}$. ■

Definição 2.4 *Seja $\psi\colon G_{\mathfrak{P}} \longrightarrow G\big((B/\mathfrak{P})\,/\,(A/\mathfrak{p})\big)$ o epimorfismo do teorema anterior. Então , $T_{\mathfrak{P}} = \ker\psi$ é chamado grupo de inércia de $\mathfrak{P}$ e seu corpo fixo L^t é chamado corpo de inércia de $\mathfrak{P}$.*

Temos assim que:
- $T_{\mathfrak{P}} = \{\sigma \in G_{\mathfrak{P}} \mid \sigma(x) - x \in \mathfrak{P}, \forall\, x \in B\}$
- $L^t = \{x \in L \mid \sigma(x) = x, \forall\, \sigma \in T_{\mathfrak{P}}\}$

• Suponhamos agora que L é separável sobre K. Já mostramos que B é um domínio de Dedekind, pela proposição 1.31, $\mathfrak{p}B$ é um ideal de B diferente de B e assim temos $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$.

Proposição 2.6 *Um primo $\mathfrak{P}$ de B está na fatoração de $\mathfrak{p}B$ se, e somente se, $\mathfrak{P}$ está acima de $\mathfrak{p}$.*

Demonstração: Se $\mathfrak{P}$ está na fatoração de $\mathfrak{p}B$, então $\mathfrak{p}B \subset \mathfrak{P}$ assim $\mathfrak{P} \cap A \supset \mathfrak{p}B \cap A \supset \mathfrak{p} \cap A = \mathfrak{p}$, como $\mathfrak{p}$ é um ideal maximal de A e $\mathfrak{P} \cap A \neq A$ é um ideal de A, então $\mathfrak{p} = \mathfrak{P} \cap A$, desse modo $\mathfrak{P}$ está acima de $\mathfrak{p}$.
Se $\mathfrak{P}$ está acima de $\mathfrak{p}$, $\mathfrak{P} \supset \mathfrak{p}$, logo, pelo corolario 1.15, $\mathfrak{P}$ está na fatoração de $\mathfrak{p}B$.
■

Definição 2.5 *Seja $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, com $\mathfrak{P}_i \neq \mathfrak{P}_j$, para $i \neq j$, cada e_i é chamado índice de ramificação de $\mathfrak{P}_i$ sobre $\mathfrak{p}$ e é denotado por $e(\mathfrak{P}_i|\mathfrak{p})$ ou $e_{\mathfrak{P}_i}$.*

Definição 2.6 *Se $\mathfrak{P}$ é ideal primo de B acima de $\mathfrak{p}$, denotamos por $f_{\mathfrak{P}}$ ou $f(\mathfrak{P}/\mathfrak{p})$ o número $[B/\mathfrak{P} : A/\mathfrak{p}]$. Esse número é chamado grau de inércia de $\mathfrak{P}$ sobre $\mathfrak{p}$.*

Proposição 2.7 *Sejam A um domínio de Dedekind, K=Q(A), $K \subset E \subset L$, uma torre de extensões finitas e separáveis $B = I_E(A)$, $C = I_L(A)$. Seja $\mathfrak{p}$ ideal primo de A, $\mathfrak{P}$ ideal primo de B acima de $\mathfrak{p}$ e $\mathfrak{Q}$ ideal primo de C acima de $\mathfrak{P}$, Então :*

$$e(\mathfrak{Q} \mid \mathfrak{p}) = e(\mathfrak{Q} \mid \mathfrak{P})e(\mathfrak{P} \mid \mathfrak{p})$$

$$f(\mathfrak{Q} \mid \mathfrak{p}) = f(\mathfrak{Q} \mid \mathfrak{P})f(\mathfrak{P} \mid \mathfrak{p})$$

■

Veja [3] P.24

Definição 2.7 *Um anel de valorização discreta A, é um DIP que tem um único ideal primo $\mathfrak{p}$ não nulo.*

Exemplo 2.1 *Se A é um domínio de Dedekind e $\mathfrak{p}$ é um ideal primo não nulo de A então pelo teorema 1.22 e a proposição 1.28 o anel $A_{\mathfrak{p}}$ é um anel de valorização discreta.*

Nosso objetivo é mostrar o seguinte:

Teorema 2.8 *Seja A um domínio de Dedekind, L uma extensão finita e separável de K=Q(A), $\mathfrak{p}$ um ideal primo não nulo de A e $\mathfrak{P}_1, \cdots, \mathfrak{P}_r$ os ideais primos de $B = I_L(A)$ que estão acima de $\mathfrak{p}$. Então :*

$$\sum_{i=1}^{r} e_i f_i = [L\colon K]$$

Para a demonstração desse teorema precisaremos alguns lemas.

Lema 2.9 *Seja A um domínio de Dedekind, $\mathfrak{m}$ um ideal maximal de A e $\mathfrak{u}$ um ideal não nulo de A. Então $\frac{\mathfrak{u}}{\mathfrak{m}\mathfrak{u}}$ é um $\frac{A}{\mathfrak{m}}$-espaço vetorial de dimensão* 1.

Demonstração: $\frac{\mathfrak{u}}{\mathfrak{m}\mathfrak{u}}$ é anulado por $\mathfrak{m}$, então $\frac{\mathfrak{u}}{\mathfrak{m}\mathfrak{u}}$ é um $\frac{A}{\mathfrak{m}}$-espaço vetorial.

Vamos mostrar que não existe $\mathfrak{n}$ ideal de A tal que $\mathfrak{m}\mathfrak{u} \subsetneq \mathfrak{n} \subsetneq \mathfrak{u}$.
Seja $\mathfrak{u} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$, onde $r_i \in \mathbb{N}$. Agora, se $\mathfrak{m} \in \{\mathfrak{p}_1, \cdots, \mathfrak{p}_k\}$ podemos supor que

$\mathfrak{m} = \mathfrak{p}_1$, assim $\mathfrak{n} = \mathfrak{m}^{r_1}\mathfrak{p}_2^{r_2}\cdots\mathfrak{p}_k^{r_k}$.
Como $\mathfrak{u} \supset \mathfrak{n}$, $\mathfrak{u} \mid \mathfrak{n}$, logo, $\mathfrak{n} = \mathfrak{m}^{s_1}\mathfrak{p}_2^{s_2}\cdots\mathfrak{p}_k^{s_k}$ com $s_i \geq r_i$, mas $\mathfrak{mu} = \mathfrak{m}^{r_1+1}\mathfrak{p}_2^{r_2}\cdots\mathfrak{p}_k^{r_k}$, agora $\mathfrak{n} \mid \mathfrak{mu}$, logo $r_1 + 1 = s_1$ e $r_i = s_i$, e desse modo $\mathfrak{n} = \mathfrak{mu}$.
Se $\mathfrak{m} \notin \{\mathfrak{p}_1^{r_1}, \cdots, \mathfrak{p}_k^{r_k}\}$, pode-se provar que $\mathfrak{u} = \mathfrak{n}$. Assim pelo teorema da correspondencia tem-se que $\frac{\mathfrak{u}}{\mathfrak{mu}}$ é um $\frac{A}{\mathfrak{mu}}$ módulo minimal, logo $\frac{\mathfrak{u}}{\mathfrak{mu}}$ é um $\frac{A}{\mathfrak{m}}$-espaço vetorial de dimensão 1. ∎

Definição 2.8 *Seja $[L : K] = n$, e $\beta = \{\beta_1, \cdots, \beta_n\}$ base de L / K. Pela demonstração do lema 1.20 sabemos que existe uma base $\beta' = \{\beta'_1, \cdots, \beta'_n\}$ desta extensão tal que:*

$$T_{L|K}(\beta_i\beta'_j) = \delta_{ij} \text{ e, para todo } \alpha \in L, \ \alpha = \sum_{j=1}^{n} T_{L|K}(\beta_j\alpha)\beta'_j.$$

β' é chamada base dual de β.

Lema 2.10 *Sejam A um domínio integralmente fechado em K=Q(A), L extensão finita e separável de K e $B = I_L(A)$. Então existem M e M' A-módulos livres de posto $n = [L : K]$ tal que $M \subset B \subset M'$.*

Demonstração: Podemos considerar $\beta = \{\beta_1, \cdots, \beta_n\}$ base de L / K tal que $\beta_i \in B$ para todo $i \in \{1, \cdots, n\}$. Seja $M = A\beta_1 + \cdots + A\beta_n$, então M é um A-módulo livre de posto n e $M \subset B$. Consideremos $\beta' = \{\beta'_1, \cdots, \beta'_n\}$ a base dual de β e seja $M' = A\beta'_1 + \cdots + A\beta'_n$. Então M' é um A-módulo livre de posto n. Se $\alpha \in B$, então $\alpha = \sum_{j=1}^{n} T_{L|K}(\beta_j\alpha)\beta'_j$, como A é integralmente fechado e L/K é separável, tem-se que $T_{L|K}(\beta_j\alpha) \in A$, logo $\alpha \in M'$ e $B \subset M'$. ∎

Observação :
Restringido-nos ao caso particular em que L é um corpo de números algébricos e $A = \mathbb{Z}$, temos que I_L é um $\mathbb{Z}$-módulo livre de posto n, pois $\mathbb{Z}$ é um DIP.

Já temos as ferramentas para mostrar o Teorema 2.8.

Demonstração:

a) Vamos mostrar primeiro que $\sum_{i=1}^{r} e_i f_i = [B/\mathfrak{p}B : A/\mathfrak{p}]$. Seja $\mathfrak{p}B = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_r^{e_r}$.
Consideremeos a cadeia descendente de ideais:

$\mathfrak{P} \supset \mathfrak{P}^2 \supset \cdots \supset \mathfrak{P}_1^{e_1} \supset \mathfrak{P}_1^{e_1}\mathfrak{P}_2 \supset \cdots \supset \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2} \supset \cdots \supset \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} = \mathfrak{p}B$, seja agora $\mathfrak{u}$ um ideal dessa cadeia (menos o último), então o ideal seguinte é $\mathfrak{u}\mathfrak{P}_i$, para certo $i \in \{1, \cdots, r\}$. Pelo lema 2.9, $\dfrac{\mathfrak{u}}{\mathfrak{u}\mathfrak{P}_i}$ é um $\dfrac{B}{\mathfrak{P}_i}$ espaço vetorial de dimensão 1, e como $\mathfrak{p}$ anula $\dfrac{\mathfrak{u}}{\mathfrak{u}\mathfrak{P}_i}$ temos que:

$\left[\dfrac{\mathfrak{u}}{\mathfrak{u}\mathfrak{P}_i} : \dfrac{A}{\mathfrak{p}}\right] = \left[\dfrac{\mathfrak{u}}{\mathfrak{u}\mathfrak{P}_i} : \dfrac{B}{\mathfrak{P}_i}\right]\left[\dfrac{B}{\mathfrak{P}_i} : \dfrac{A}{\mathfrak{p}}\right] = \left[\dfrac{B}{\mathfrak{P}_i} : \dfrac{A}{\mathfrak{p}}\right] = f_i$, assim para cada i teremos exactamente e_i quocientes, cada um de dimensão f_i sobre $\dfrac{A}{\mathfrak{p}}$. Além disso:

$$\dim(B/\mathfrak{p}B) = \dim(B/\mathfrak{P}_1) + \dim(\mathfrak{P}_1/\mathfrak{P}_1^2) + \cdots + \dim(\mathfrak{P}_1^{e_1-1}/\mathfrak{P}_1^{e_1}) + \dim(\mathfrak{P}_1^{e_1}/\mathfrak{P}_1^{e_1}\mathfrak{P}_2) +$$

$$\cdots + \dim(\mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2-1}/\mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}) + \cdots + \dim(\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r-1}/\mathfrak{p}B).$$

Assim, $\displaystyle\sum_{i=1}^{r} e_i f_i = \left[\dfrac{B}{\mathfrak{p}B} : \dfrac{A}{\mathfrak{p}}\right]$.

b) Vamos mostrar agora que $\left[\dfrac{B}{\mathfrak{p}B} : \dfrac{A}{\mathfrak{p}}\right] = [L : K]$. Suponhamos primeiramente que B é livre. Pelo lema 2.10 B tem posto $n = [L : K]$.

Sejam $X = \{x_1, \cdots, x_n\}$, uma base de B e $\pi \colon B \longrightarrow \dfrac{B}{\mathfrak{p}B}$ a projeção canônica. Como π é sobrejetora temos que $\{\pi(x_1), \cdots, \pi(x_n)\}$, gera $\dfrac{B}{\mathfrak{p}B}$. Vamos mostrar que eles são L.I sobre $\dfrac{A}{\mathfrak{p}}$. De fato, sejam $a_i \in A, i \in \{1, \cdots, n\}$ tais que:

$$\sum_{i=1}^{n}(a_i + \mathfrak{p})(x_i + \mathfrak{p}B) = \sum_{i=1}^{n}(a_i x_i + \mathfrak{p}B) = \mathfrak{p}B.$$

Então $\displaystyle\sum_{i=1}^{n} a_i x_i \in \mathfrak{p}B$, e, portanto $\displaystyle\sum_{i=1}^{n} a_i x_i = \sum_{j=1}^{m} b_j y_j$, com $b_j \in B, y_j \in \mathfrak{p}$, para $j \in \{1, \cdots, m\}$.

Alem disso, como $b_j = \displaystyle\sum_{i=1}^{n} c_{ji} x_i, c_{ji} \in A$, temos que, $\displaystyle\sum_{i=1}^{n} a_i x_i = \sum_{j=1}^{m} y_j \left(\sum_{i=1}^{n} c_{ji} x_i\right)$.

Agora da independencia linear dos x_i, podemos concluir que $a_i = \displaystyle\sum_{j=1}^{m} y_j c_{ji}$, onde $y_j \in \mathfrak{p}$ e $c_{ji} \in A$. Assim $a_i \in \mathfrak{p}$ e, portanto, $\{\pi(x_1), \cdots, \pi(x_n)\}$ é uma base de $\dfrac{B}{\mathfrak{p}B}$

sobre $\frac{A}{\mathfrak{p}}$. Logo $\left[\frac{B}{\mathfrak{p}B} : \frac{A}{\mathfrak{p}}\right] = [L : K]$.

c) Vamos agora provar o caso geral. Como A é um domínio de Dedekind, $A_{\mathfrak{p}}$ é um anel de valorizacão discreta e seu único ideal primo é $m_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$ (veja exemplo 2.1).
Sabemos que $B = I_L(A)$, de onde $B_{\mathfrak{p}} = I_L(A_{\mathfrak{p}})$ é um $A_{\mathfrak{p}}$-módulo livre. Como $m_{\mathfrak{p}}B_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}B_{\mathfrak{p}} = \mathfrak{p}B_{\mathfrak{p}}$, pelo item b temos:

$$\left[\frac{B_{\mathfrak{p}}}{\mathfrak{p}B_{\mathfrak{p}}} : \frac{A_{\mathfrak{p}}}{m_{\mathfrak{p}}}\right] = [L : K].$$

Por outro lado: $m_{\mathfrak{p}}B_{\mathfrak{p}} = \mathfrak{p}B_{\mathfrak{p}} = S_{\mathfrak{p}}^{-1}\mathfrak{p}B = S_{\mathfrak{p}}^{-1}(\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_r^{e_r}) = (S_{\mathfrak{p}}^{-1}\mathfrak{P}_1)^{e_1}\cdots(S_{\mathfrak{p}}^{-1}\mathfrak{P}_r)^{e_r}$ $= (S_{\mathfrak{p}}^{-1}B\mathfrak{P}_1)^{e_1}\cdots(S_{\mathfrak{p}}^{-1}B\mathfrak{P}_r)^{e_r} = (B_{\mathfrak{p}}\mathfrak{P}_1)^{e_1}\cdots(B_{\mathfrak{p}}\mathfrak{P}_r)^{e_r}$, assim:

$$m_{\mathfrak{p}}B_{\mathfrak{p}} = (B_{\mathfrak{p}}\mathfrak{P}_1)^{e_1}\cdots(B_{\mathfrak{p}}\mathfrak{P}_r)^{e_r}$$

Logo $[L: K] = \left[\frac{B_{\mathfrak{p}}}{\mathfrak{p}B_{\mathfrak{p}}} : \frac{A_{\mathfrak{p}}}{m_{\mathfrak{p}}}\right] = \sum_{i=1}^{r} e_i f(B_{\mathfrak{p}}\mathfrak{P}_i/m_{\mathfrak{p}}) = \sum_{i=1}^{r} e_i[B_{\mathfrak{p}}/B_{\mathfrak{p}}\mathfrak{P}_i : A_{\mathfrak{p}}/m_{\mathfrak{p}}]$.
Vamos mostrar agora que $\frac{B_{\mathfrak{p}}}{\mathfrak{p}B_{\mathfrak{p}}} = \frac{B}{\mathfrak{P}_i}$ e $\frac{A_{\mathfrak{p}}}{m_{\mathfrak{p}}} = \frac{A}{\mathfrak{p}}$.
Seja $i : \frac{B}{\mathfrak{P}_i} : \longrightarrow \frac{B_{\mathfrak{p}}}{B_{\mathfrak{p}}\mathfrak{P}_i}$ a inclusão canônica, provaremos que i é epimorfismo.
De fato, seja $\frac{x}{s} + B_{\mathfrak{p}}\mathfrak{P}_i \in \frac{B_{\mathfrak{p}}}{B_{\mathfrak{p}}\mathfrak{P}_i}$, então $s \notin \mathfrak{p}$ e $(s) \nsubseteq \mathfrak{p}$. Como $\mathfrak{p}$ é ideal maximal de A, tem-se que $A = \mathfrak{p} + (s)$, assim existem $c \in \mathfrak{p}$ e $a \in A$ tais que $1 = c + sa$, então $\frac{1}{s} - a = \frac{c}{s} \in \mathfrak{p}A_{\mathfrak{p}} \subset \mathfrak{P}_iB_{\mathfrak{p}}$, logo $\frac{x}{s} - xa = \frac{xc}{s} \in \mathfrak{P}_iB_{\mathfrak{p}}$, então $i(xa + \mathfrak{P}_i) = xa + \mathfrak{P}_iB_{\mathfrak{p}} = \frac{x}{s} + \mathfrak{P}_iB_{\mathfrak{p}}$, assim a inclusão é epimorfismo, portanto é identidade; desse modo $\frac{B_{\mathfrak{p}}}{B_{\mathfrak{p}}\mathfrak{P}_i} = \frac{B}{\mathfrak{P}_i}$.
Analogamente prova-se que $\frac{A_{\mathfrak{p}}}{m_{\mathfrak{p}}} = \frac{A}{\mathfrak{p}}$ e $\left[\frac{B_{\mathfrak{p}}}{B_{\mathfrak{p}}\mathfrak{P}_i} : \frac{A_{\mathfrak{p}}}{m_{\mathfrak{p}}}\right] = f_i$.
Logo $[L : K] = \sum_{i=1}^{r} e_i f_i$. ∎

Corolário 2.11 *Suponhamos que L/K é de Galois. Então para $\mathfrak{P} \mid \mathfrak{p}$, todos os $e_{\mathfrak{P}}$ (respectivamente $f_{\mathfrak{P}}$) são iguais a e (respectivamente f) e se $\mathfrak{p}B = (\mathfrak{P}_1\cdots\mathfrak{P}_r)^e$, então $efr = [L : K]$.*

Demonstração: Como L é de Galois sobre K e $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. Pelo teorema 2.1, para cada $i \in \{1, \cdots, r\}$ existe $\sigma_i \in G(L\,/\,K)$ tal que $\mathfrak{P}_i = \sigma\mathfrak{P}_1$, desse modo $\mathfrak{P}_i^{e_i} = \sigma\mathfrak{P}_1^{e_i}$, assim $\sigma\mathfrak{P}_1^{e_i}$ divide $\mathfrak{p}B$ então $\mathfrak{P}_1^{e_i}$ divide $\mathfrak{p}B$, logo $e_1 \leq e_i$, analogamente prova-se que $e_i \leq e_1$ para todo i, logo $e_1 = e_i$.

Por outro lado $f_1 = \left[\dfrac{B}{\mathfrak{P}_1} : \dfrac{A}{\mathfrak{p}}\right]$, $f_i = \left[\dfrac{B}{\sigma_i}\mathfrak{P}_1 : \dfrac{A}{\mathfrak{p}}\right]$, e como
$\psi : \dfrac{B}{\mathfrak{P}_1} \longrightarrow \dfrac{B}{\sigma_i\mathfrak{P}_1}$, tal que $\psi(x + \mathfrak{P}_1) = \sigma_i(x) + \sigma_i\mathfrak{P}_1$ é um isomorfismo então $f_1 = f_i, \forall\, i$.

Finalmente, $[L : K] = \displaystyle\sum_{i=1}^{r} e_i f_i = \sum_{i=1}^{r} ef = efr.$ ■

Definição 2.9 *Diremos que um ideal primo $\mathfrak{p}$ de A é:*
• *Totalmente decomposto em L quando $r = n$, ou seja, $e = f = 1$.*
Nesse caso $\mathfrak{p}B = \mathfrak{P}_1 \cdots \mathfrak{P}_n$.
• *Totalmente inerte em L quando $r = e = 1$, ou seja, $f = n$. Nesse caso $\mathfrak{p}B = \mathfrak{P}$.*
• *Totalmente ramificado em L quando $r = f = 1$, ou seja, $e = n$.*
Nesse caso $\mathfrak{p}B = \mathfrak{P}^n$.

Consideremos agora $X = \{\mathfrak{P}_1, \cdots \mathfrak{P}_r\}$, o conjunto dos ideais primos de B acima deum ideal primo $\mathfrak{p}$ de A e seja $G = G(L\,/\,K)$.
Sabemos que G age sobre X pela aplicação $\phi : G \times X \longrightarrow X$, que satisfaz $\phi(\sigma, \mathfrak{P}) = \sigma\mathfrak{P}, \forall\, \sigma \in G, \mathfrak{P} \in X$.
Por outro lado, para $\mathfrak{P} \in X$, a órbita de $\mathfrak{P}$ é $O_{\mathfrak{P}} = \{\sigma\mathfrak{P}\,|\sigma \in G\} = X$, então $|O_{\mathfrak{P}}| = r$ e, o estabilizador de $\mathfrak{P}$ é $stab(\mathfrak{P}) = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\} = G_{\mathfrak{P}}$.
Assim, pelo teorema do índice e do estabilizador temos que:

$$r = |O_{\mathfrak{P}}| = (G : G_{\mathfrak{P}}) = \frac{|G|}{|G_{\mathfrak{P}}|}.$$

Então :

$$|G_{\mathfrak{P}}| = \frac{|G|}{r} = fe.$$

Agora, se $\dfrac{B}{\mathfrak{P}}$ é separável sobre $\dfrac{A}{\mathfrak{p}}$, pelo teorema 2.5 ela é de Galois e
$G((B/\mathfrak{P})/(A/\mathfrak{p})) \cong \dfrac{G_{\mathfrak{P}}}{T_{\mathfrak{P}}}$, portanto $f = \left[\dfrac{B}{\mathfrak{P}} : \dfrac{A}{\mathfrak{p}}\right] = |G((B/\mathfrak{P})/(A/\mathfrak{p}))| = \dfrac{|G_{\mathfrak{P}}|}{|T_{\mathfrak{P}}|}$.
Assim:

$$|T_{\mathfrak{P}}| = \frac{fe}{f} = e.$$

Essas considerações provam o seguinte:

Teorema 2.12 *Seja A um domínio de dedekind com corpo de frações K, L uma extensão finita e de Galois de K,* $\mathfrak{p}$ *ideal primo de A e* $\mathfrak{P}$ *ideal primo de B acima de* $\mathfrak{p}$*. Então* $|G_{\mathfrak{P}}| = ef$ *e, se* $\frac{B}{\mathfrak{P}}$ *e extensão separável de* $\frac{A}{\mathfrak{p}}$, $|T_{\mathfrak{P}}| = e$.

Como conseqüência do teorema anterior temos:
$\mathfrak{p}$ não ramifica em L $(e = 1) \iff T_{\mathfrak{P}}$ é trivial.
$\mathfrak{p}$ é totalmente ramificado em $L \iff T_{\mathfrak{P}} = G_{\mathfrak{P}} = G(L \,/\, K)$.

Vamos considerar agora grupos de decomposição sobre corpos intermediarios. Ou seja se $K \subset K' \subset L$ definimos $G_{\mathfrak{P}|K'} = \{\sigma \in G(L \,/\, K') \mid \sigma\mathfrak{P} = \mathfrak{P}\}$.
Observe que $G_{\mathfrak{P}|K'} = G_{\mathfrak{P}} \cap G(L \,/\, K')$.
De agora em diante vamos sempre supor que $\frac{B}{\mathfrak{P}}$ é separável sobre $\frac{A}{\mathfrak{p}}$.

Proposição 2.13 *Sejam* $A' = B \cap K'$, $\mathfrak{p}' = \mathfrak{P} \cap A' = \mathfrak{P} \cap K'$*. Então o homomorfismo* $\phi' : G_{\mathfrak{P} \,/\, K'} \longrightarrow G((B \,/\, \mathfrak{P}) \,/\, (A' \,/\, \mathfrak{p}'))$*, dado por* $\phi'(\sigma) = \sigma + A'/\mathfrak{p}'$ *é igual a restricão do epimorfismo* $\phi : G_{\mathfrak{P}} \longrightarrow G((B \,/\, \mathfrak{P}) \,/\, (A \,/\, \mathfrak{p}))$*, definido no teorema 2.5 e tem como nucleo o grupo* $T_{\mathfrak{P}|K'} = T_{\mathfrak{P}} \cap G(L \,/\, K')$*.*

Veja [2] p.180.

Observação : Sejam $B^d = B \cap L^d$ e $\mathfrak{P}^d = \mathfrak{P} \cap B^d$. Então $\mathfrak{P}$ é o único ideal primo de B acima de $\mathfrak{P}^d$.

Teorema 2.14 *1) Se* $L^d \subset K' \subset L$*, então* $L^t \subset K'$ *se, e somente se,* $f(\mathfrak{P}|\mathfrak{p}') = 1$.

2) Se $K \subset K' \subset L$*, então* $L^d \subset K'$ *se, e somente se,* $r(\mathfrak{P}|\mathfrak{p}') = 1$.

Demonstração: 1)

$$\begin{array}{ccc} \mathfrak{P} & B & L \\ | & | & | \\ \mathfrak{p}' & A' & K' \\ | & | & | \\ \mathfrak{P}^d & B^d & L^d \end{array}$$

Sejam $\mathfrak{P}^d$ um ideal primo de B^d e $\mathfrak{P}$ o único ideal primo de B acima de $\mathfrak{P}^d$.
Temos que $G_{\mathfrak{P}|K'} = G_{\mathfrak{P}} \cap G(L\,/\,K') = G(L\,/\,L^d) \cap G(L\,/\,K') = G(L\,/\,K')$, onde a última igualdade é verdadeira por hipótese.
Por outro lado, $T_{\mathfrak{P}|K'} = T_{\mathfrak{P}} \cap G(L\,/\,K') = G(L\,/\,L^t) \cap G(L\,/\,K')$.
Agora $f(\mathfrak{P}|\mathfrak{p}') = 1 \iff [B/\mathfrak{P}' : A'/\mathfrak{p}'] = 1 \iff G(B/\mathfrak{P}'/A'/\mathfrak{p}') = \{i_d\} \iff G_{\mathfrak{P}|K'}/T_{\mathfrak{P}|K'} = (\bar{0}) \iff G_{\mathfrak{P}|K'} = T_{\mathfrak{P}|K'} \iff G(L/K') = G(L/L^t) \cap G(L\,/\,K') \iff G(L\,/\,K') \subset G(L\,/\,L^t) \iff L^t \subset K'$.

2) $r(\mathfrak{P}|\mathfrak{p}') = 1 = (G(L/K') : G'_{\mathfrak{P}})$, então $r(\mathfrak{P}|\mathfrak{p}') = 1 \iff G(L\,/\,K') = G'_{\mathfrak{P}} = G_{\mathfrak{P}} \cap G(L\,/\,K') \iff G_{\mathfrak{P}} \supset G(L\,/\,K') \iff L^d \subset K'$. ■

Corolário 2.15 *Sejam $e = e(\mathfrak{P}|\mathfrak{p})$, $f = f(\mathfrak{P}|\mathfrak{p})$ e $r = r(\mathfrak{P}|\mathfrak{p})$. Então :*
- $[L : L^d] = ef, \quad [L^d : K] = r.$
- $e(\mathfrak{P}^d|\mathfrak{p}) = f(\mathfrak{P}^d|\mathfrak{p}) = 1.$
- $e(\mathfrak{P}|\mathfrak{P}^d) = e, \quad f(\mathfrak{P}|\mathfrak{P}^d) = f.$

Demonstração:

$$\begin{array}{ccc} \mathfrak{P} & B & L \\ | & | & | \\ \mathfrak{P}^d & B^d & L^d \\ | & | & | \\ \mathfrak{p} & A & K \end{array}$$

Demonstração: Observemos que $[L : L^d] = |G(L\,/\,L^d)| = |G_{\mathfrak{P}}| = ef$,
$efr = [L : K] = [L : L^d][L^d : K]$, então $[L^d : K] = r$.
Pela proposição 2.3, temos que $B^d/\mathfrak{P}^d = A/\mathfrak{p}$, e então $f(\mathfrak{P}|\mathfrak{p}) = \left[\dfrac{B^d}{\mathfrak{P}^d} : \dfrac{A}{\mathfrak{p}}\right] = 1$.
Assim $f = f(\mathfrak{P}|\mathfrak{P}^d)f(\mathfrak{P}^d|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{P}^d)$, como $r(\mathfrak{P}|\mathfrak{P}^d) = 1$, temos que,
$ef = [L : L^d] = e(\mathfrak{P}|\mathfrak{P}^d)f(\mathfrak{P}|\mathfrak{P}^d) = fe(\mathfrak{P}|\mathfrak{P}^d)$, assim $e(\mathfrak{P}/\mathfrak{P}^d) = e$.
Finalmente $e = e(\mathfrak{P}|\mathfrak{P}^d)e(\mathfrak{P}^d|\mathfrak{p}) = ee(\mathfrak{P}^d|\mathfrak{p})$, então $e(\mathfrak{P}^d|\mathfrak{p}) = 1$. ■

Proposição 2.16 *L^t é de Galois sobre L^d e $\dfrac{G_{\mathfrak{P}}}{T_{\mathfrak{P}}} \cong G(L^t\,/\,L^d)$*

Demonstração: Como $T_{\mathfrak{P}} \lhd G_{\mathfrak{P}}$, então $G(L\,/\,L^t) \lhd G(L/L^d)$, e assim L^t é normal sobre L^d, logo de Galois.

Seja $\phi : G_{\mathfrak{P}} \longrightarrow G(L^T/L^d)$, dada pela restrição $\phi(\sigma) = \sigma|_{L^t}$, $\forall\, \sigma \in G_{\mathfrak{P}}$. Notemos que $\sigma|_{L^t} \in Aut(L^t)$ pois L^t é uma extensão normal de L^d.
• É claro que ϕ é homomorfismo.
• Dado $\tau \in G(L^T \,/\, L^d)$, como L é normal sobre L^t, existe $\lambda \in G(L \,/\, L^d) = G_{\mathfrak{P}}$ tal que $\lambda|_{L^t} = \tau$, desse modo ϕ é epimorfismo.
• $\sigma \in \ker\phi \iff \sigma(x) = x, \forall\, x \in L^t \iff \sigma \in G(L/L^t) = T_{\mathfrak{P}}$.
Assim pelo Teorema fundamental do homomorfismo temos que $G_{\mathfrak{P}}/T_{\mathfrak{P}} \cong G(L^t \,/\, L^d)$.

Corolário 2.17 *Sejam* $B^t = I_L^t(A) = B \cap L^t$, $\mathfrak{P}^t = \mathfrak{P} \cap L^t$, $\mathfrak{P}^d = \mathfrak{P} \cap L^d$, $e = e(\mathfrak{P}|\mathfrak{p}), f = f(\mathfrak{P}|\mathfrak{p})$ *e* $r = r(\mathfrak{P}|\mathfrak{p})$. *Então :*
• $[L : L^t] = e, \quad [L^t : L^d] = f$.
• $r(\mathfrak{P}^t|\mathfrak{P}^d) = e(\mathfrak{P}^t|\mathfrak{P}^d) = 1, \quad f(\mathfrak{P}^t|\mathfrak{P}^d) = f$.
• $r(\mathfrak{P}|\mathfrak{P}^t) = 1, \quad e(\mathfrak{P}|\mathfrak{P}^t) = e, \quad f(\mathfrak{P}|\mathfrak{P}^t) = 1$.

Demonstração:

$$\begin{array}{ccc} \mathfrak{P} & B & L \\ | & | & | \\ \mathfrak{P}^t & B^t & L^t \\ | & | & | \\ \mathfrak{P}^d & B^d & L^d \end{array}$$

$ef = [L\colon L^d] = [L\colon L^t][L^t\colon L^d] = [L\colon L^t]|G(L^t/L^d)| = [L\colon L^t]\frac{|G_{\mathfrak{P}}|}{|T_{\mathfrak{P}}|} = [L\colon L^t]f$, assim $[L\colon L^t] = e$. Por outro lado, $ef = [L\colon L^d] = [L\colon L^t][L^t\colon L^d] = e[L^t\colon L^d]$, então $[L^t\colon L^d] = f$.
Sabemos que $L^d \subset L^t \subset L$, então pelo item 1 do teorema 2.14 temos que $f(\mathfrak{P}|\mathfrak{P}^t) = 1$.
Logo $e = [L : L^t] = e(\mathfrak{P}|\mathfrak{P}^t)r(\mathfrak{P}|\mathfrak{P}^t)$, mas $1 = r(\mathfrak{P}|\mathfrak{P}^d) = r(\mathfrak{P}|\mathfrak{P}^t)r(\mathfrak{P}^t|\mathfrak{P}^d)$. Então :

$$r(\mathfrak{P}|\mathfrak{P}^t) = r(\mathfrak{P}^t|\mathfrak{P}^d) = 1, \text{ e, portanto, } e = e(\mathfrak{P}|\mathfrak{P}^t).$$

Assim $e = e(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{P}^d) = e(\mathfrak{P}|\mathfrak{P}^t)e(\mathfrak{P}^t|\mathfrak{P}^d) = ee(\mathfrak{P}^t|\mathfrak{P}^d)$, logo $e(\mathfrak{P}^t|\mathfrak{P}^d) = 1$.

Finalmente $f = f(\mathfrak{P}|\mathfrak{P}^d) = f(\mathfrak{P}|\mathfrak{P}^t)f(\mathfrak{P}^t|\mathfrak{P}^d) = f(\mathfrak{P}^t|\mathfrak{P}^d)$, então $f(\mathfrak{P}^t|\mathfrak{P}^d) = f$. ■

Observação Como $e(\mathfrak{P}|\mathfrak{P}^t) = [L\colon L^t]$, temos que $\mathfrak{P}^t$ é totalmente ramificado em L. Na próxima seção estudaremos mais detalhadamente a ramificação total de $\mathfrak{P}^t$ em L.

2.2 Grupos de Ramificação

Definição 2.10 *Para $i \in \mathbb{N}$, chamaremos de o i-esimo grupo de ramificação de $\mathfrak{P}$ sobre K, denotado por V_i ou $V_i(\mathfrak{P})$ o conjunto:*

$$\{\sigma \in G_{\mathfrak{P}} \mid \sigma(\alpha) - \alpha \in \mathfrak{P}^{i+1}, \forall\, \alpha \in B\}$$

- Observe-se que $V_0 = T_{\mathfrak{P}}$.

Proposição 2.18 *1. Para todo $i \in \mathbb{N}$, V_i é subgrupo normal de $G_{\mathfrak{P}}$.*

2. Existe $j \in \mathbb{N}$ tal que V_j é trivial.

Demonstração: 1) Para $\sigma \in G_{\mathfrak{P}}$, seja $\bar{\sigma} : B/\mathfrak{P}^{i+1} \longrightarrow B/\mathfrak{P}^{i+1}$ definido por $\bar{\sigma}(x + \mathfrak{P}^{i+1}) = \sigma(x) + \mathfrak{P}^{i+1}$.
Note-se que $\bar{\sigma}$ está bem definida e $\bar{\sigma} \in Aut(B/\mathfrak{P}^{i+1})$. Logo $\phi\colon G_{\mathfrak{P}} \longrightarrow Aut(B/\mathfrak{P}^{i+1})$, onde $\phi(\sigma) = \bar{\sigma}$ para todo $\sigma \in G_{\mathfrak{P}}$, é um homomorfismo e $\ker\phi = V_i$, portanto $V_i \lhd G_{\mathfrak{P}}$.
2) Sabemos que $T_{\mathfrak{P}}$ é um subgrupo de $G_{\mathfrak{P}}$, que é finito, logo $T_{\mathfrak{P}}$ é finito e assim a cadeia $T_{\mathfrak{P}} \supset V_1 \supset \cdots \supset V_m \supset \cdots$ estaciona, então existe $j \in \mathbb{N}$ tal que $V_j = V_{j+1} = \cdots$, se $\sigma \in V_j$, logo $\sigma \in V_i, \forall\, i \in \mathbb{N}$, consequentemente $\sigma(\alpha) - \alpha \in \bigcap_{i\in\mathbb{N}} \mathfrak{P}^{i+1} = (0)$ (pois B é um dominio noetheriano, Veja [5] p.216). Desse modo $\sigma(\alpha) = \alpha, \forall\, \alpha \in B$, e V_j é trivial. ■

- Se $K \subset K' \subset L$, temos $V_i(\mathfrak{P}/K') = V_i \cap G(L/K')$.

Proposição 2.19 *Seja $\mathfrak{p}$ um ideal primo de A tal que $\mathfrak{P}$, ideal de B, está acima dele. Então :*

$$G_{\mathfrak{P}} = \{\sigma \in G(L|K) \mid \sigma(\mathfrak{P}B_{\mathfrak{p}}) = \mathfrak{P}B_{\mathfrak{p}}\}$$

$$V_i = \{\sigma \in G_{\mathfrak{P}} \mid \sigma(\alpha) - \alpha \in \mathfrak{p}^{i+1}B_{\mathfrak{P}}, \forall\, \alpha \in B_{\mathfrak{p}}\}$$

isto é, os grupos de decomposição , inércia e ramificação ficam inalterados quando se substituir $\mathfrak{P}^i$ por $(\mathfrak{P}B_{\mathfrak{p}})^i = \mathfrak{P}^iB_{\mathfrak{p}}$.

Demonstração: Sabemos que $\mathfrak{P}B_\mathfrak{p} = \left\{ \sum_{j=i}^{n} \gamma_j s_j^{-1} \middle| \gamma_j \in \mathfrak{P}, s_j \in S_\mathfrak{p} \right\}$, e, portanto, para $\sigma \in G_\mathfrak{P}$, $\sigma(\mathfrak{P}B_\mathfrak{p}) = \left\{ \sum_{j=i}^{n} \sigma(\gamma_j) s_j^{-1} \middle| \gamma_j \in \mathfrak{P}, s_j^{-1} \in S_\mathfrak{p} \right\} = \sigma(\mathfrak{P})B_\mathfrak{p} = \mathfrak{P}B_\mathfrak{p}$. Assim:

$$G_\mathfrak{P} \subset \{\sigma \in G(L/K) \mid \sigma(\mathfrak{P}B_\mathfrak{p}) = \mathfrak{P}B_\mathfrak{p}\}.$$

Agora, como $\mathfrak{P}B_\mathfrak{p} \cap B = \mathfrak{P}$, se $\sigma \in G(L\,/\,K)$ fixa $\mathfrak{P}B_\mathfrak{p}$, temos que $\sigma(\mathfrak{P}) = \sigma(\mathfrak{P}B_\mathfrak{p} \cap B) = \sigma(\mathfrak{P}B_\mathfrak{p}) \cap \sigma(B) = \mathfrak{P}B_\mathfrak{p} \cap B = \mathfrak{P}$, portanto:

$$G_\mathfrak{P} \supset \{\sigma \in G(L/K)\} \mid \sigma(\mathfrak{P}B_\mathfrak{p}) = \mathfrak{P}B_\mathfrak{p}\}.$$

Vamos mostrar agora a segunda igualdade. Seja $\sigma \in V_i$ e $y = \dfrac{\alpha}{s} \in B_\mathfrak{p}$, então $\sigma(\alpha) - \alpha = \dfrac{1}{s}(\sigma(\alpha) - \alpha) \in \mathfrak{P}^{i+1}B_\mathfrak{p}$, $\forall\, \alpha \in B_\mathfrak{p}$, assim

$$V_i \subset \{\sigma \in G_\mathfrak{P} \mid \sigma(\alpha) - \alpha \in \mathfrak{p}^{i+1}B_\mathfrak{P}\}.$$

Consideremos agora $\sigma \in G_\mathfrak{P}$ tal que $\sigma(\alpha) - \alpha \in \mathfrak{P}^{i+1}B_\mathfrak{p}$ $\forall\, \alpha \in B_\mathfrak{p}$. Seja $\alpha \in B$. Então $\alpha \in B_\mathfrak{p}$. Como $\sigma(\alpha) - \alpha \in B$ e $\mathfrak{P}^{i+1}B_\mathfrak{p} \cap B = \mathfrak{P}^{i+1}$, tem-se que $\sigma(\alpha) - \alpha \in \mathfrak{P}^{i+1}B_\mathfrak{p} \cap B = \mathfrak{P}^{i+1}$, logo

$$V_i \supset \{\sigma \in G_\mathfrak{P} \mid \sigma(\alpha) - \alpha \in \mathfrak{p}^{i+1}B_\mathfrak{P}\},$$

o que completa a prova da proposição . ■

Observação Seja $\mathfrak{p}$ um ideal primo não nulo de A que é totalmente ramificado em L e $\mathfrak{P}$ o único ideal primo de B acima de $\mathfrak{p}$, então :

1. $\mathfrak{p}A_\mathfrak{p}$ é totalmente ramificado em L, sendo $\mathfrak{P}B_\mathfrak{p}$ o único ideal primo de $B_\mathfrak{p}$ que está acima de $\mathfrak{p}A_\mathfrak{p}$.

2. $A_\mathfrak{p}$ e $B_\mathfrak{p}$ são domínios de ideais principais que possuem apenas um ideal primo não nulo, a saber, $\mathfrak{p}A_\mathfrak{p}$ e $\mathfrak{P}B_\mathfrak{p}$ respectivamente.

O seguinte teorema será usado no estudo dos grupos de ramificação .

Teorema 2.20 *Sejam L uma extensão separável de grau n de K, $\mathfrak{p}$ um ideal primo não nulo de A que é totalmente ramificado em L , $\mathfrak{P}$ o único ideal primo de B acima de $\mathfrak{p}$ e π o gerador de $\mathfrak{P}B_\mathfrak{p}$ então :*

1. $L = K(\pi)$.

2. $\{1, \pi, \cdots, \pi^{n-1}\}$ é uma base do $A_\mathfrak{p}$-módulo $B_\mathfrak{p}$.

Demonstração:
1) Temos que $A_\mathfrak{p}$ e $B_\mathfrak{p}$ são anéis de valorização discreta, e, portanto, todo anel fracionário não nulo de $A_\mathfrak{p}$ (respectivamente $B_\mathfrak{p}$) escreve-se como potência $(\mathfrak{p}A_\mathfrak{p})^k$ ($(\mathfrak{P}B_\mathfrak{p})^k = \pi^k B_\mathfrak{p}$), onde $k \in \mathbb{Z}$ é único. Consideremos a aplicação v, tal que para $a \in K$,

$$v(a) = \begin{cases} \infty, \ se\ a = 0. \\ k, \ se\ a \neq 0\ e\ (a) = (\mathfrak{p}A_\mathfrak{p})^k. \end{cases}$$

Para quaisquer $i, j \in \{0, 1, \cdots, n-1\}$, e $a, b \in K^*$, temos $nV(a) + i \neq nV(b) + j$ se $i \neq j$, já que em caso contrario $|i-j| = n|V(a)-V(b)|$, o que contradiz $n > |i-j| > 0$.
Sejam $a_0, a_1, \cdots, a_{n-1} \in K$, não todos nulos e $m = \min\{nv(a_i) + i \mid 0 \leq i \leq n-1\}$, então existe $i_0 \in \{0, 1, \cdots, n-1\}$ tal que $m = nv(a_{i_0}) + i_0$ e $m < nV(a_i) + i$, para $i \neq i_0$.
Como $\mathfrak{p}A_\mathfrak{p}$ é totalmente ramificado em L, temos $\mathfrak{p}A_\mathfrak{p} = \mathfrak{P}^n B_\mathfrak{p} = \pi^n B_\mathfrak{p}$, assim para $a \in K$, $a \neq 0$, $(a) = (\mathfrak{p}A_\mathfrak{p})^{v(a)} = \pi^{nv(a)} B_\mathfrak{p}$, multiplicando por π^i temos,
$\pi^i(a) = \pi^{nv(a)+i} B_\mathfrak{p} \subset \pi^{m+1} B_\mathfrak{p}$, para todo $i \neq i_0$ tal que $a_i \neq 0$ e $\pi^{i_0}(a_{i_0}) = \pi^m B_\mathfrak{p}$.
Agora se $\alpha = \sum_{i=0}^{n-1} a_i \pi^i$, então $\alpha \in \pi^m B_\mathfrak{p}$ e $\alpha \notin \pi^{m+1} B_\mathfrak{p}$, pois $\pi^{i_0} a_{i_0} \notin \pi^{m+1} B_\mathfrak{p}$, logo em particular $\alpha \neq 0$.

Assim se $a_0, a_1, \cdots, a_n \in K$, não são todos nulos segue-se que $\sum_{i=0}^{n-1} a_i \pi^i \neq 0$ portanto o conjunto $\{1, \pi, \cdots, \pi^{n-1}\}$ é L.I e consequentemente $L = K(\pi)$.

2) Seja $\alpha \in B_\mathfrak{p}$. Como $\alpha \in L$, existem $a_1, \cdots, a_n \in K$, tais que, $\alpha = \sum_{i=0}^{n-1} a_i \pi^i$, se $\alpha \neq 0$ os a_i não são todos nulos e temos $\alpha \in \pi^m B_\mathfrak{p}$ e $\alpha \notin \pi^{m+1} B_\mathfrak{p}$, logo $(\alpha) \subset \pi^m B_\mathfrak{p}$ e $\alpha \nsubseteq \pi^{m+1} B_\mathfrak{p}$, onde $m = \min\{nV(a_i) + i \mid 0 \leq i \leq n-1\}$.
Notemos que (α) é um ideal de $B_\mathfrak{p}$, assim $m \geq 0$ e segue que $nV(a_i) + i \geq 0$, para todo $i \in \{0, 1, \cdots, n-1\}$. Logo $V(a_i) > -1$ e portanto $V(a_i) \geq 0$, assim $(a_i) = (\mathfrak{p}A_p)^m$, onde $m \geq 0$. Portanto $(a_i) \subset A_\mathfrak{p}$ e $a_i \in A_\mathfrak{p}$. ∎

Proposição 2.21 *Se $\mathfrak{p}$ for totalmente ramificado em L, tem-se que $V_i = \{\sigma \in G_\mathfrak{P} \mid \sigma(\pi) - \pi \in \mathfrak{P}^{i+1} B_\mathfrak{p}\}$, sendo π o gerador do ideal $\mathfrak{P}^{i+1} B_\mathfrak{p}$.*

Demonstração: Pela proposição 2.19, temos $V_i \subset \{\sigma \in G_\mathfrak{P} \mid \sigma(\pi) - \pi \in \mathfrak{P}^{i+1} B_\mathfrak{p}\}$.
Seja $\sigma \in G(L/K)$ tal que $\sigma(\pi) - \pi \in \mathfrak{P}^{i+1} B_\mathfrak{p}$. Pelo teorema anterior, $\{1, \pi, \cdots, \pi^{n-1}\}$

é uma base do $A_{\mathfrak{p}}$-módulo $B_{\mathfrak{p}}$, então para $\alpha \in B_{\mathfrak{p}}$, $\alpha = \sum_{i=0}^{n-1} a_i \pi^i$. Conseqüentemente $\sigma(\alpha) - \alpha = \sum_{i=0}^{n-1} a_i(\sigma(\pi^i) - \pi^i) = \sum_{i=0}^{n-1} a_i(\sigma(\pi) - \pi) \sum_{j=0}^{i} \sigma(\pi^{i-j})\pi^j \in \mathfrak{P}^{i+1} B_{\mathfrak{p}}$, pois $\sum_{i=0}^{n-1} a_i(\sigma(\pi) - \pi) \in \mathfrak{P}^{i+1} B_{\mathfrak{p}}$ e $\sum_{j=0}^{i} \sigma(\pi^{i-j})\pi^j \in \mathfrak{P}^{i+1} B_{\mathfrak{p}} \in B_{\mathfrak{p}}$.
Assim $V_i \supset \{\sigma \in G_{\mathfrak{P}} \mid \sigma(\pi) - \pi \in \mathfrak{P}^{i+1} B_{\mathfrak{p}}\}$. ■

Teorema 2.22 *Sejam A um domínio local e* $\mathfrak{m}$ *seu ideal maximal; então :*

1. $\forall\, i \geq 1$, $U_i = \{1 + a \mid a \in \mathfrak{m}^i\}$ *é um subgrupo de* $U_0 = U(A)$*, e temos* $U_0 \supset U_1 \supset U_2 \cdots$.
2. $\dfrac{U_0}{U_1} \cong \left(\dfrac{A}{\mathfrak{m}}\right)^*$ *(como grupos multiplicativos).*
3. *Para todo* $i \geq 1$*, temos* $\dfrac{U_i}{U_{i+1}}$ *é isomorfo ao* $\dfrac{A}{\mathfrak{m}}$*-espaço* $\dfrac{\mathfrak{m}^i}{\mathfrak{m}^{i+1}}$.
4. *Se A for domínio de Dedekind, então o grupo aditivo* $\dfrac{\mathfrak{m}^i}{\mathfrak{m}^{i+1}}$ *será isomorfo a* $\dfrac{A}{\mathfrak{m}}$ *(como grupos aditivos).*

Demonstração:
1) Temos que para todo $i \in \mathbb{N}$, $1 = 1 + 0 \in U_i$. Sejam $1 + a, 1 + b \in U_i$, com $a, b \in \mathfrak{m}^i$, então $(1 + a)(1 + b) = 1 + c$, onde $c = a + b + ab \in \mathfrak{m}^i$, portanto $(1 + a)(1 + b) \in U_i$.
Como $a \in \mathfrak{m}^i \subset \mathfrak{m} = A - U(A)$, temos que $1 + a$ é inversível em A.
Agora, $(1 + a)(1 + b) = 1 \iff a + b + ab = 0 \iff b(1 + a) = -a \iff$
$b = -a(1 + a)^{-1} \in \mathfrak{m}^i$, pois $a \in \mathfrak{m}^i$, logo $(1 + a)^{-1} = 1 + b$, onde $b = -a(1 + a)^{-1}$, conseqüentemente $1 + a$ é inversível em U_i. Portanto U_i é subgrupo de $U(A)$.
2) Seja $\phi\colon U(A) \longrightarrow \left(\dfrac{A}{\mathfrak{m}}\right)^*$, tal que $\phi(a) = a + \mathfrak{m}$, para todo $a \in U(A)$. É claro que ϕ é um homomorfismo.
Alem disso se $a+\mathfrak{m} \in \left(\dfrac{A}{\mathfrak{m}}\right)^*$, então $a \notin \mathfrak{m}$, e, portanto, logo $a \in U(A)$ e $\phi(a) = a+\mathfrak{m}$. Conseqüentemente ϕ é um epimorfismo.
Temos que, $\ker\phi = \{a \in U(A) \mid a + \mathfrak{m} = 1 + \mathfrak{m}\} = \{a \in U(A) \mid a - 1 \in \mathfrak{m}\}$, afirmamos que $\ker\phi = U_1$.

De fato, se $1+a \in U_1$ temos $1+a \in U(A)$ e $(1+a)-1 = a \in \mathfrak{m}$, assim $\ker\phi \supset U_1$; por outro lado, se $a \in \ker\phi$, temos $a = 1 + (a-1)$, com $a-1 \in \mathfrak{m}$, assim $a \in U_1$, logo $\ker\phi \subset U_1$.

3) Considere, $\psi\colon \mathfrak{m}^i \longrightarrow \dfrac{U_i}{U_{i+1}}$, tal que $\psi(a) = (1+a)U_{i+1}$, para todo $a \in \mathfrak{m}^i$. Vamos mostrar que ψ é homomorfismo.
De fato, se $a, b \in \mathfrak{m}^i$. Temos que:
$\psi(a+b) = \psi(a)\psi(b) \iff (1+a+b)U_{i+1} = (1+a)(1+b)U_{i+1} \iff$
$(1+a)(1+b)(1+a+b)^{-1} \in U_{i+1} \iff (1+a+b)^{-1}+(a+b)(1+a+b)^{-1}+ab(1+a+b)^{-1} \in U_{i+1}$.
Mas já vimos que $(1+a+b)^{-1} = 1-(a+b)(1+a+b)^{-1}$, então $(a+b)(1+a+b)^{-1} = 1-(1+a+b)^{-1}$; assim $(1+a+b)U_{i+1} = (1+a)(1+b)U_{i+1} \iff 1+ab(1+a+b)^{-1} \in U_{i+1}$ o que é verdadeiro pois $a, b \in \mathfrak{m}^i$, portanto ψ é um homomorfismo, logo um epimorfismo pois claramente é sobrejetora.
Vamos mostrar agora que $\ker\psi = \mathfrak{m}^{i+1}$. $\ker\psi = \{a \in \mathfrak{m}^i \mid 1+a \in U_{i+1}\}$, assim $x \in \mathfrak{m}^{i+1} \iff 1+x \in U_{i+1} \iff x \in \ker\psi$.

4) Como A é um domínio de Dedekind. Pelo lema 2.9, temos $\left[\dfrac{\mathfrak{m}^i}{\mathfrak{m}^{i+1}}\colon \dfrac{A}{\mathfrak{m}}\right] = 1$, e como $\left[\dfrac{A}{\mathfrak{m}}\colon \dfrac{A}{\mathfrak{m}}\right] = 1$, temos $\dfrac{\mathfrak{m}^i}{\mathfrak{m}^{i+1}} \cong \dfrac{A}{\mathfrak{m}}$, como grupos aditivos. ■

Teorema 2.23 *Suponhamos que* $\mathfrak{p}$ *seja totalmente ramificado em L.*
Sejam $U_0 = U(B_\mathfrak{p})$ *e* $U_i = \{1+\alpha \mid \alpha \in \mathfrak{P}^i B_\mathfrak{p}\}$ *e* $\pi \in B_\mathfrak{p}$ *um gerador do ideal* $\mathfrak{P}B_\mathfrak{p}$*, então :*
Para todo $i \in \mathbb{N}$ *a aplicação* $\phi_i\colon V_i \longrightarrow \dfrac{U_i}{U_{i+1}}$ *dada por* $\phi_i(\sigma) = \dfrac{\sigma\pi}{\pi}U_{i+1}$*, independe da escolha de* π *e é um epimorfismo com nucleo* V_{i+1}*.*

Demonstração: Pelo teorema anterior temos que U_i é um subgrupo de U_0 para todo $i \in \mathbb{N}$.
Seja $\epsilon \in U_0$, logo $\epsilon \in B_\mathfrak{p}$, e, assim, para todo $\sigma \in V_i$, $\sigma(\epsilon) - \epsilon \in \mathfrak{P}^{i+1}B_\mathfrak{p}$. Então

$$\frac{\sigma\epsilon}{\epsilon} - 1 = \frac{1}{\epsilon}(\sigma(\epsilon) - \epsilon) \in \mathfrak{P}^{i+1}B_\mathfrak{p}.$$

Segue-se que $\dfrac{\sigma(\epsilon)}{\epsilon} \in U_{i+1}$ para todo $\epsilon \in U_0$. Agora $\sigma(\pi) - \pi \in \mathfrak{P}^{i+1}B_\mathfrak{p}$, portanto existe $y \in B_\mathfrak{p}$ tal que $\sigma(\pi) - \pi = \pi^{i+1}y$. Como $\pi \neq 0$, π é inversível (*em L*), e temos $\dfrac{\sigma(\pi)}{\pi} - 1 = \pi^i y \in \mathfrak{P}^i B_\mathfrak{p}$, desse modo $\dfrac{\sigma(\pi)}{\pi} \in U_i$.

Vamos mostrar que ϕ_i é homomorfismo. Sejam $\sigma, \tau \in V_i$, então :

$\phi_i(\sigma\tau) = \phi_i(\sigma)\phi_i(\tau) \iff \dfrac{\sigma\tau(\pi)}{\pi}U_{i+1} = \dfrac{\sigma(\pi)}{\pi}\dfrac{\tau(\pi)}{\pi}U_{i+1} \iff \dfrac{\sigma\tau(\pi)}{\pi}\dfrac{\pi}{\sigma(\pi)}\dfrac{\pi}{\tau(\pi)} \in$

$U_{i+1} \iff \dfrac{\sigma\tau(\pi)}{\sigma(\pi)}\dfrac{\pi}{\tau(\pi)} \in U_{i+1} \iff \sigma\left(\dfrac{\tau(\pi)}{\pi}\right)\dfrac{\pi}{\tau(\pi)} \in U_{i+1} \iff \dfrac{\sigma(\epsilon)}{\epsilon} \in U_{i+1},$

onde $\epsilon = \dfrac{\tau(\pi)}{\pi}$, assim ϕ_i é um homomorfismo.

Por outro lado, $\ker\phi_i = \left\{\sigma \in V_i \mid \dfrac{\sigma(\pi)}{\pi}U_{i+1} = U_{i+1}\right\} = \left\{\sigma \in V_i \mid \dfrac{\sigma(\pi)}{\pi} \in U_{i+1}\right\} =$

$\left\{\sigma \in V_i \mid \dfrac{\sigma(\pi)}{\pi} - 1 \in \mathfrak{P}^{i+1}B_{\mathfrak{p}}\right\} = \left\{\sigma \in V_i \mid \sigma(\pi) - \pi \in \mathfrak{P}^{i+2}B_{\mathfrak{p}}\right\} = V_{i+1}$, onde a última

igualdade é dada pela proposição 2.19. ■

Corolário 2.24 *Sejam $B^t = B \cap L^t$ e $\mathfrak{P}^t = \mathfrak{P} \cap L^t$.*
Substituindo-se $S_{\mathfrak{p}}$ por $S_{\mathfrak{P}^t} = B^t - \mathfrak{P}^t$, temos que a afirmação do teorema anterior vale sem a hipótese de $\mathfrak{p}$ ser totalmente ramificado em L.

Demonstração:

$$\begin{array}{ccc} \mathfrak{P} & B & L \\ | & | & | \\ \mathfrak{P}^t & B^t & L^t \\ | & | & | \\ \mathfrak{p} & A & K \end{array}$$

Sabemos que $[L\colon L^t] = e(\mathfrak{P}|\mathfrak{P}^t)$, então $\mathfrak{P}^t$ é totalmente ramificado em L, logo o teorema anterior vale para os grupos $V_i(\mathfrak{P}|L^t)$ e os grupos U_i definidos em relação ao anel $B^t_{\mathfrak{P}} = S^{-1}_{\mathfrak{P}^t}B$, assim $\dfrac{V_i(\mathfrak{P}|L^t)}{V_{i+1}(\mathfrak{P}|L^t)}$ é isomorfo a um subgrupo de $\dfrac{U_i}{U_{i+1}}$.

Por outro lado $V_i = V_i \cap T_{\mathfrak{P}} = V_i \cap G(L|L^t) = V_i(\mathfrak{P}|L^t)$, consequentemente $\dfrac{V_i}{V_{i+1}}$ é isomorfo a um subgrupo de $\dfrac{U_i}{U_{i+1}}$, onde $U_i = \{1 + \alpha \mid \alpha \in \mathfrak{P}^i B_{\mathfrak{P}^t}\}$. ■

Corolário 2.25 *1. $\dfrac{T_{\mathfrak{P}}}{V_1}$ é canonicamente isomorfo a um subgrupo do grupo multiplicativo de $\dfrac{B}{\mathfrak{P}}$.*

2. $\forall\, i \geq 1$, $\dfrac{V_i}{V_{i+1}}$ *é isomorfo a um subgrupo do grupo aditivo* $\dfrac{B}{\mathfrak{P}}$.

Demonstração:
1) Sabemos que $\mathfrak{P}^t$ é totalmente ramificado em L, portanto $B_{\mathfrak{P}^t}$ é um dominio de ideais principais e seu ideal maximal é $(\pi) = \mathfrak{P}B_{\mathfrak{P}^t}$.
Para $i \geq 1$, sejam $U_i = \{1 + \alpha \mid \alpha \in \mathfrak{P}^i B_{\mathfrak{P}^t}\}$ e $U_0 = U(B_{\mathfrak{P}^t})$, então temos que $\phi_0 \colon T_{\mathfrak{P}} \longrightarrow \dfrac{U_0}{U_1}$ dada por $\phi_0(\sigma) = \dfrac{\sigma\pi}{\pi}U_1$, independe da escolha de π e tem como nucleo V_1. Portanto, pelo primeiro teorema fundamental do homomorfismo, temos, $\dfrac{T_{\mathfrak{P}}}{V_1} \cong \phi_0(T_{\mathfrak{P}})$ que é subgrupo de $\dfrac{U_0}{U_1}$.
Por outro lado, pelo teorema 2.22, $\dfrac{U_0}{U_1} \cong \left(\dfrac{B_{\mathfrak{P}^t}}{\mathfrak{P}B_{\mathfrak{P}^t}}\right)^*$, e, como já provamos que $\psi \colon \dfrac{B}{\mathfrak{P}} \longrightarrow \dfrac{B_{\mathfrak{P}^t}}{\mathfrak{P}B_{\mathfrak{P}^t}}$, tal que $\psi(x+\mathfrak{P}) = x + \mathfrak{P}B_{\mathfrak{P}^t}$, para todo $x + \mathfrak{P} \in \dfrac{B}{\mathfrak{P}}$ é um isomorfismo, temos que $\dfrac{T_{\mathfrak{P}}}{V_1}$ é isomorfo a um subgrupo do grupo multiplicativo de $\dfrac{B}{\mathfrak{P}}$.
2) Análoga. ∎

2.3 O Compositum

Vamos em seguida complementar a teoria com alguns resultados que serão uteis para o estudo de corpos ciclotômicos.

Definição 2.11 *Sejam F_1 e F_2 subcorpos de um corpo K, o compositum de F_1 e F_2, denotado por F_1F_2 é definido como o menor subcorpo de K que contém F_1 e F_2. Pode-se provar que* $F_1F_2 = \left\{ \dfrac{\sum a_i b_i}{\sum a'_j b'_j} \middle| a_i, a'_j \in F_1, b_i, b'_j \in F_2, \sum a'_j b'_j \neq 0 \right\}$.

Teorema 2.26 *Sejam K e F extensões de um corpo E contidas num corpo L.*
Se K/E for Galois finita, então KF/F e $K/K \cap F$ são galoisianas finitas e a aplicação $G(KF \,/\, F) \longrightarrow G(K \,/\, K \cap F)$ dada por $\sigma \longrightarrow \sigma_{|K}$ é um isomorfismo.

Demonstração: Como K/E é finita e separável, existe $\gamma \in K$ separável sobre E, tal que $K = E(\gamma)$, portanto $KF = F(\gamma)$ sendo γ separável sobre F, assim KF/F é finita e separável.
É claro que KF/F é algébrica. Agora consideremos $\sigma \colon KF \longrightarrow \overline{F}$ uma imersão que deixa fixo F, então $\sigma_{|K} \colon K \longrightarrow \overline{F}$ é uma imersão que deixa fixo E (pois

$E \subset F$), assim $\sigma(K) = K$, portanto $\sigma(KF) = \sigma(K)\sigma(F) = KF$, assim KF/F é normal.
Por outro lado, como temos que $E \subset K \cap F \subset K$ e K/E é Galois finita, então $K/K \cap F$ é Galois finita.
Consideremos agora o homomorfismo $res\colon G(KF \,/\, F) \longrightarrow G(K \,/\, E)$ dado por $\sigma \longrightarrow \sigma_{|K}$, se $res(\sigma)$ for a identidade de K como σ fixa F, então σ fixa KF, portanto res é injetora.
Seja $H = im(res) < G(K \,/\, E)$. É facil ver que todo elemento de $K \cap F$ é fixado por H. Se $x \in K$ é fixado por H, então , para $\sigma \in G(KF \,/\, F)$, temos $\sigma(x) = \sigma_{|K}(x) = x$, assim $x \in F$. Logo $x \in K \cap F$, portanto, o corpo fixo de H é $K \cap F$, logo $G(KF \,/\, F) \cong G(K/K \cap F)$. ■

Teorema 2.27 *Se K/E e F/E são galoisianas finitas, então KF/E é Galois finita e o homomorfismo $R\colon G(KF/E) \longrightarrow G(K/E)\times G(F/E)$, tal que $R(\sigma) = (\sigma_{|K}, \sigma_{|F})$ para todo $\sigma \in G(KF/E)$ satisfaz : $im(R) \supset G(K/K \cap F) \times G(F/K \cap F)$.*

Demonstração: Sabemos que $[KF : F] = \{KF : F\}$ e que $[F : E] = \{F : E\}$, portanto $\{KF : E\} = \{KF : F\}\{F : E\} = [KF : F][F : E] = [KF : E]$, assim KF/E é finita e separável.
É claro que KF/E é algébrica, consideremos $\sigma\colon KF \longrightarrow \overline{E}$ uma imersão que deixa E fixo, então $\sigma_{|K}\colon K \longrightarrow \overline{E}$ e $\sigma_{|F}\colon F \longrightarrow \overline{E}$, são imersões que deixam E fixo, assim $\sigma(K) = K$ e $\sigma(F) = F$, logo $\sigma(KF) = KF$ e portanto KF/E é normal.
Do teorema anterior temos que:

$$G(KF/F) \cong G(K/K \cap F) \text{ e } G(KF/K) \cong G(F/K \cap F).$$

Alem disso $G(KF/F)$ e $G(KF/K)$ são subgrupos de $G(KF/E)$, portanto:

$$R(G(KF/F)) = G(K/K \cap F) \times \{id_F\} \text{ e } R(G(KF/K)) = \{id_K\} \times G(F/K \cap F).$$

Conseqüentemente $im(R) \supset G(K/K \cap F) \times G(F/K \cap F)$. ■

Definição 2.12 *Sejam G_1, G_2 e H grupos e $f\colon G_1 \longrightarrow H$, $g\colon G_2 \longrightarrow H$ dois homomorfismos. O produto fibrado de G_1 e G_2 sobre H é é dado por:*

$$G_1 \times_H G_2 = \{(a, b) \in G_1 \times G_2 \mid f(a) = g(b)\}$$

- Observemos que $G_1 \times_H G_2$ é subgrupo de $G_1 \times G_2$

Teorema 2.28 *Sejam F/E e K/E extensões de Galois finitas,com $F, K \subset L$ e L corpo, então $K \cap F/E$ é de Galois finita e $G(KF/E) \cong G(K/E) \times_{G(K\cap F/E)} G(F/E)$.*

Demonstração: Seja R o homomorfismo do teorema anterior, se $(\sigma, \tau) \in imR$, existe $\lambda \in G(KF/E)$ tal que $\lambda\big|_K = \sigma$ e $\lambda\big|_F = \tau$, portanto para $x \in K \cap F$, temos $\sigma(x) = \lambda(x) = \tau(x)$.
Sejam agora $\sigma \in G(K/E)$ e $\tau \in G(F/E)$, tais que $\sigma\big|_{K\cap F} = \tau\big|_{K\cap F}$, como $KF/K \cap F$ é algébrica e KF/E é normal, podemos considerar a extensão $\theta \in G(KF/E)$ de $\sigma\big|_{K\cap F}$, então $\mu_1 = \theta^{-1}\big|_K \sigma \in G(K/E)$, $\mu_2 = \theta^{-1}\big|_F \tau \in G(F/E)$ e $\mu_1\big|_{K\cap F} = \mu_2\big|_{K\cap F} = id_{K\cap F}$, logo pelo teorema anterior existe $\lambda \in G(KF/E)$ tal que $R(\lambda) = (\mu_1, \mu_2)$ isto é $\lambda\big|_K = \mu_1$ e $\lambda\big|_F = \mu_2$, então $\theta\lambda \in G(KF/E)$ e $(\theta\lambda)\big|_K = \theta\big|_K \lambda\big|_K = \theta\big|_K \mu_1 = \sigma$ e $(\theta\lambda)\big|_F = \theta\big|_F \lambda\big|_F = \theta\big|_F \mu_2 = \tau$.

Isso prova a nossa afirmação . ■

Capítulo 3

Corpos de Números Algébricos

Uma noção central na teoria dos números algébricos é a de anel dos inteiros algébricos, I_L, de um corpo de números algébricos L, que foi introduzida no capítulo 1, num contexto mais geral, através da noção de elemento inteiro sobre um dominio A. Já provamos que I_L sempre é um $\mathbb{Z}$-módulo livre, ou seja, que L possui uma base integral. Neste capítulo introduziremos a noção de discriminante, que representará um papel importante na caracterização das suas bases. Além disso o discriminante de uma base integral de L, denotada por d_L, terá muita importancia na teoria de ramificação , pois mostraremos que os divisores primos de d_L são exactamente aqueles que ramificam em L. Usaremos também o chamado *Metodo Geométrico*, para mostrar que no caso $[L\colon \mathbb{Q}] \geq 2$, $|d_L| > 1$, e assim garantir a existência de tais primos .

3.1 Discriminante

Definição 3.1 *Sejam A um domínio de Dedekind, K o corpo de frações de A, L uma K-álgebra de grau n e $\alpha_1, \cdots, \alpha_n \in L$, definimos o discriminante de $\alpha_1, \cdots, \alpha_n$ como:*

$$disc_{L|K}(\alpha_1, \cdots, \alpha_n) = det(T_{L|K}(\alpha_i \alpha_j))$$

Note que:

- $disc_{L|K}(\alpha_1, \cdots, \alpha_n) \in K$.
- *Se $\alpha_1, \cdots, \alpha_n \in I_L(A)$, então $disc_{L|K}(\alpha_1, \cdots, \alpha_n) \in A$.*

Lema 3.1 *Sejam L uma extensão separavel de K e* $\sigma_1, \cdots, \sigma_n$ *os K-monomorfismos de L em* $\bar{K}$*. Então :*

$$disc_{L|K}(\alpha_1, \cdots, \alpha_n) = [det(\sigma_i(\alpha_j))]^2.$$

Demonstração: Sabemos que:

$$T_{L|K}(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j),$$

consideremos a matriz $H = (\sigma_i(\alpha_j))$, então $disc_{L|K}(\alpha_1, \cdots, \alpha_n) = detHH^T = [det(\sigma_i(\alpha_j))]^2$. ■

Proposição 3.2 *Sejam* $L = K(\alpha)$*, f o polinômio minimal de* α *sobre K e* $\alpha = \alpha_1, \cdots, \alpha_n$ *as raízes de f sobre um corpo de raízes de K, então :*

$$disc_{L|K}(1, \alpha, \cdots, \alpha^{n-1}) = \prod_{i<j} (\alpha_i - \alpha_j)^2 = \triangle(f)$$

Demonstração: Seja $\sigma_i \colon L \longrightarrow K$ dada por $\sigma_i(\alpha) = \alpha_i$, então $\sigma_i(\alpha^j) = \alpha_i^j$, $0 \leq j \leq n-1$, logo:

$$disc_{L|K}(1, \alpha, \cdots, \alpha^{n-1}) = \det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix} = \triangle(f). \quad ■$$

Lema 3.3 *Sejam* $\beta_1, \cdots, \beta_n \in L$ *e* $C \in M_n(K)$ *tal que* $\beta_i = C\alpha_i$ *para* $i \in \{1, \cdots, n\}$*. Então :*

$$disc_{L|K}(\beta_1, \cdots, \beta_n) = (detC)^2 disc_{L|K}(\alpha_1, \cdots, \alpha_n)$$

Demonstração: Seja $C = (c_{ij})$, então para $k \in \{1, \cdots, n\}$, $\beta_k = \sum_{i=1}^{n} c_{ki}\alpha_i$, assim $\beta_k\beta_m = \sum_{i,j} c_{ki}c_{mj}\alpha_i\alpha_j$, portanto $T_{L|K}(\beta_k\beta_m) = \sum_{i,j} c_{ki}T_{L|K}(\alpha_i\alpha_j)c_{mj}$.
Logo $[T_{L|K}(\beta_k\beta_m)] = C[T_{L|K}(\alpha_i\alpha_j)]C^T$, consequentemente :

$$disc_{L|K}(\beta_1, \cdots, \beta_n) = (detC)^2 disc_{L|K}(\alpha_1, \cdots, \alpha_n).$$

■

Teorema 3.4 *Sejam L uma extensão separavel de K e $\alpha_1, \cdots, \alpha_n \in L$, então $\{\alpha_1, \cdots, \alpha_n\}$ é uma dase de $L \mid K$ se, e sómente se, $disc_{L|K}(\alpha_1, \cdots, \alpha_n) \neq 0$.*

Demonstração: Sejam γ um elemento primitivo de L/K e $\sigma_1, \cdots, \sigma_n$ as K-imersões de L em $\bar{K}$, se P_γ é o polinômio minimal de γ temos que $\partial P_\gamma = [L\colon K]$, então $\sigma_1(\gamma), \cdots, \sigma_n(\gamma)$ são todas distintas, logo:

$$disc_{L|K}(1, \gamma, \cdots, \gamma^{n-1}) = \prod_{i<j}(\gamma_i - \gamma_j)^2 = \prod_{i<j}(\sigma_i(\gamma) - \sigma_j(\gamma))^2 \neq 0.$$

Agora para $j \in \{1, \cdots, n\}$,

$$\alpha_j = \sum_{i=0}^{n} c_{ij}\gamma^j$$

Então $disc_{L|K}(\alpha_1, \cdots, \alpha_n) = (detC)^2 disc_{L|K}(1, \gamma, \cdots, \gamma^{n-1})$, assim
$disc_{L|K}(\alpha_1, \cdots, \alpha_n) \neq 0 \iff (detC)^2 \neq 0 \iff \{\alpha_1, \cdots, \alpha_n\}$ é uma dase de $L \mid K$.
■

• Consideremos agora R um anel tal que $A \subset R \subset I_L(A)$ e $\alpha_1, \cdots, \alpha_n \in R$, assim $disc_{L|K}(\alpha_1, \cdots, \alpha_n) \in A$.

Definição 3.2 *O ideal $\delta_{R|A} =< disc_{L|K}(\alpha_1, \cdots, \alpha_n) \mid \alpha_i \in R >$, é um ideal de A chamado ideal discriminante de $R \mid A$*

Proposição 3.5 *Seja $A \subset R \subset I_L(A)$ e suponhamos que R, considerado como A-módulo, possui uma base $\{\beta_1, \cdots, \beta_n\}$, então :*

1. $\delta_{R|A} =< disc_{L|K}(\beta_1, \cdots, \beta_n) >$.

   Alem disso, para quaisquer $\alpha_1, \cdots, \alpha_n \in R$ temos que:

2. $disc_{L|K}(\alpha_1, \cdots, \alpha_n) = a^2 disc_{L|K}(\beta_1, \cdots, \beta_n)$, *para algum $a \in A$.*

3. $\{\alpha_1, \cdots, \alpha_n\}$ *é uma base de R se, e só se, $a \in U(A)$.*

Demonstração:

1. Seja $\alpha_i \in R$. Então $\alpha_i = \sum_{i=1}^{n} c_{ij}\beta_j$,com $c_{ij} \in A$, se $C = (c_{ij})$ tem-se que $disc_{L|K}(\alpha_1, \cdots, \alpha_n) = (\det C)^2 disc_{L|K}(\beta_1, \cdots, \beta_n)$, assim:

$$\delta_{R|A} =< disc_{L|K}(\beta_1, \cdots, \beta_n >.$$

2. Tomamos $a = detC$.

3. $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de $R \Longleftrightarrow$ existem $C, Z \in M_n(A)$ tais que $\alpha_i = C\beta_i$ e $\beta_i = Z\alpha_i$ para $i \in \{1, \cdots, n\}$, logo $\zeta = (ZC)\zeta$ para todo $\zeta \in R$, assim $ZC = I$, e como $a = \det C$, temos que a é inversível. ■

Proposição 3.6 *Sejam A um dominio, L uma extensão de grau n de K=Q(A) e* $\alpha \in I_L(A)$*, são equivalentes:*

1. $L = K(\alpha)$.

2. $\{1, \alpha, \cdots, \alpha^{n-1}\}$ *é uma base do A-módulo* $A[\alpha]$.

Demonstração:
1) $\Longrightarrow$ 2)
$\{1, \alpha, \cdots, \alpha^{n-1}\}$ são L.I sobre K, logo sobre A. Se $\beta \in A[\alpha]$, então $\beta = g(\alpha)$, com $g(X) \in A[X]$. Como K é corpo temos que $K[X]$ é um domínio euclidiano, e assim existem $a(X)$ e $h(X)$ em $K[X]$ tais que $g(X) = P_\alpha(X)a(X) + h(X)$ onde $h(X) = 0$ ou $\partial h < \partial P_\alpha$, logo $\beta = g(\alpha) = h(\alpha)$, assim $\beta = a_1 + a_2\alpha + \cdots + a_k\alpha^k$, com $a_i \in A$ e $k < n$.
2) $\Longrightarrow$ 1)
Sejam $c_0, \cdots, c_{n-1} \in K$ tais que $\sum_{i=0}^{n-1} c_i\alpha^i = 0$, onde $c_i = \frac{a_i}{b_i}$, com $a_i, b_i \in A$ e $b_i \neq 0$.
Consideremos agora $b = \prod_{i=1}^{n-1} b_i \in A^*$, então $bc_i \in A$ e $\sum_{i=0}^{n-1} bc_i\alpha^i = 0$, portanto $bc_i = 0$ e assim $c_i = 0$. Portanto $\{1, \alpha, \cdots, \alpha^{n-1}\}$ é L.I sobre K e como $[L\colon K] = n$, temos que $L = K(\alpha)$. ■

Vamos agora estudar a demonstração de um teorema devido a *Kummer*, que nos permitirá indicar explicitamente a decomposição de um ideal primo $\mathfrak{p}$ de A a partir da fatoração de $\bar{P}_\beta$ em $\frac{A}{\mathfrak{p}}$, sendo β um elemento de $B = I_L(A)$ tal que $B = A[\beta]$.
Observemos que:
• Se $\beta \in B$ é tal que $B = A[\beta]$, então $L = I_L(K) = Q(I_LA) = Q(B) = Q(A[\beta]) = K(\beta)$, assim pela proposição anterior $B = A[\beta] \Longleftrightarrow \{1, \beta, \cdots, \beta^{n-1}\}$ é uma base do A-módulo B.

• Seja $\mathfrak{p}$ um ideal primo de A, e $f(X) = \sum_{i=1}^{n} a_i X^i \in A[X]$, denotaremos por $\bar{f}(X)$ o polinômio $\sum_{i=1}^{n} (a_i + \mathfrak{p})X^i$.

Teorema 3.7 (Teorema de Kummer) *Suponhamos $B = A[\theta]$, sejam $P_1, \cdots, P_k$ polinômios mônicos em $A[X]$ tais que $\bar{P} = \bar{P_1}^{e_1} \cdots \bar{P_r}^{e_r}$ ($P = P_\theta$) seja a fatoração de $\bar{P}$ em polinômios irredutiveis distintos em $\left(\frac{A}{\mathfrak{p}}\right)[X]$. Então :*

1. *$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, onde $\mathfrak{P}_j = \mathfrak{p}B + P_j(\theta)B$ são os ideais primos de B acima de $\mathfrak{p}$, logo $e(\mathfrak{P}_j|\mathfrak{p}) = e_j$, $j \in \{1, \cdots, r\}$.*
2. *$\frac{B}{\mathfrak{P}_j} = \frac{A}{\mathfrak{p}}(\bar{\theta}_j)$, sendo $\bar{\theta}_j$ uma raíz de $\bar{P}_j$, logo $f(\mathfrak{P}_j|\mathfrak{p}) = \partial P_j$, $j \in \{1, \cdots, r\}$.*

Demonstração: 2)Sabemos que $\bar{P} = \bar{P_1}^{e_1} \cdots \bar{P_r}^{e_r}$. Para $j \in \{1, \cdots, r\}$, seja $\tilde{\theta}_j \in \frac{A}{\mathfrak{p}}$ uma raíz de $\bar{P}_j$, como $\bar{P}_j$ é irredutivel então $\bar{P}_j$ é o polinômio minimal de $\tilde{\theta}_j$ sobre $\frac{A}{\mathfrak{p}}$, consideremos agora o epimorfismo $\mu_j \colon A[\theta] \longrightarrow \frac{A}{\mathfrak{p}}(\tilde{\theta}_j)$ dado por $\mu_j(f(\theta)) = \bar{f}(\tilde{\theta}_j)$, como $\frac{A}{\mathfrak{p}}(\tilde{\theta}_j)$ é um corpo temos que $\mathfrak{P}_j = \ker \mu_j$ é um ideal maximal de $B = A[\theta]$ e temos um isomorfismo $\bar{\mu}_j \colon \frac{A[\theta]}{\mathfrak{P}_j} \longrightarrow \left(\frac{A}{\mathfrak{p}}\right)(\tilde{\theta}_j)$, dado por $\bar{\mu}_j(f(\theta) + \mathfrak{P}_j) = \bar{f}(\tilde{\theta}_j)$.
Agora como $\mathfrak{p} \subset \mathfrak{P}_j$, então $\mathfrak{p} \subset \mathfrak{P}_j \cap A \neq A$ e como $\mathfrak{p}$ é maximal, tem-se que $\mathfrak{p} = \mathfrak{P}_j \cap A \neq A$, assim $\mathfrak{P}_j$ está acima de $\mathfrak{p}$; por outro lado $\mu_j(A) = \frac{A}{\mathfrak{p}}$, então $\bar{\mu}_j$ deixa $\frac{A}{\mathfrak{p}}$ fixo.
Consideremos $\bar{\theta}_j \in \frac{A[\theta]}{\mathfrak{P}_j}$ tal que $\bar{\mu}_j(\bar{\theta}_j) = \tilde{\theta}_j$. Então $\bar{P}_j(\bar{\theta}_j) = \bar{\mu}^{-1}(\bar{P}_j(\tilde{\theta}_j)) = \bar{0}$ e para $\bar{x} \in \frac{A[\theta]}{\mathfrak{P}_j}$, temos $\bar{x} = \bar{\mu}^{-1}(\bar{c_0} + \bar{c_1}\tilde{\theta}_j + \cdots \bar{c}_{k-1}\tilde{\theta}_j^{k-1}) = \bar{c_0} + \bar{c_1}\bar{\theta}_j + \cdots \bar{c}_{k-1}\bar{\theta}_j^{k-1}$, assim $\frac{B}{\mathfrak{P}_j} = \frac{A}{\mathfrak{p}}(\bar{\theta}_j)$ e $f(\mathfrak{P}_j|\mathfrak{p}) = \left[\frac{B}{\mathfrak{P}_j} : \frac{A}{\mathfrak{p}}\right] = \left[\frac{A}{\mathfrak{p}}(\bar{\theta}_j) : \frac{A}{\mathfrak{p}}\right] = \partial \bar{P}_j = \partial P_j$, $j \in \{1, \cdots, r\}$.

1) Vamos mostrar que $\mathfrak{P}_j = \mathfrak{p}B + P_j(\theta)B$, seja $\alpha \in \mathfrak{P}_j = \ker \mu_j$, então $\alpha = g(\theta)$ para algum $g(X) \in A[X]$ e $\mu_j(\alpha) = \mu_j(g(\theta)) = \bar{g}(\tilde{\theta}_j) = \bar{0}$.

Como $\bar{P}_j$ é o polinômio minimal de $\tilde{\theta}_j$ sobre $\left(\frac{A}{\mathfrak{p}}\right)[X]$, existe $h(X) \in A[X]$ tal que $\bar{g}(X) = \bar{P}_j(X)\bar{h}(X)$, assim $g - P_j h$ tem seus coeficientes em $\mathfrak{p}$ e:

$$\alpha = (g - P_j h)(\theta) + P_j(\theta)h(\theta) \in \mathfrak{p}B + P_j(\theta)B.$$

Portanto:

$$\mathfrak{P}_j \subset \mathfrak{p}B + P_j(\theta)B.$$

Agora como $\mu_j(P_j(\theta)) = \bar{P}_j(\tilde{\theta}_j) = \bar{0}$, então $P_j(\theta)B \subset \mathfrak{P}_j$ e é claro que $\mathfrak{p}B \subset \mathfrak{P}_j$ assim:

$$\mathfrak{P}_j \supset \mathfrak{p}B + P_j(\theta)B.$$

Falta mostrar que $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$.
Como $\mathfrak{P}_j = \mathfrak{p}B + P_j(\theta)B$, temos que $\mathfrak{P}_j^2 \subset (\mathfrak{p}B)^2 + (P_j(\theta)B)^2 \subset (\mathfrak{p}B) + (P_j(\theta)B)^2$, consequentemente $\mathfrak{P}_j^{e_j} \subset (\mathfrak{p}B) + (P_j(\theta)B)^{e_j}$, logo

$$\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \subset (\mathfrak{p}B) + (P_1(\theta)B)^{e_1} \cdots (P_r(\theta)B)^{e_r} \subset \mathfrak{p}B + \gamma B.$$

Sendo $\gamma = P_1(\theta)^{e_1} \cdots P_r(\theta)^{e_r}$.
O polinômio $P - P_1 \cdots P_r$ tem seus coeficientes em $\mathfrak{p}$ e $P(\theta) = 0$, então
$\gamma = P_1(\theta)^{e_1} \cdots P_r(\theta)^{e_r} - P(\theta) \in \mathfrak{p}B$, assim:

$$\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \subset \mathfrak{p}B.$$

Portanto $\mathfrak{p}B \mid \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ e como $\mathfrak{p}B = \mathfrak{P}_1^{e(\mathfrak{P}_1|\mathfrak{p})} \cdots \mathfrak{P}_r^{e(\mathfrak{P}_r|\mathfrak{p})}$, temos $e(\mathfrak{P}_i|\mathfrak{p}) \leq e_i$, mas pelo teorema 2.8, $n = \sum_{i=1}^{r} e(\mathfrak{P}_i|\mathfrak{p}) f(\mathfrak{P}_i|\mathfrak{p}) \leq \sum_{i=1}^{r} e_i \partial\bar{P}_i = \partial\bar{P} = \partial P = n$, assim $\sum_{i=1}^{r} e(\mathfrak{P}_i|\mathfrak{p}) f(\mathfrak{P}_i|\mathfrak{p}) = \sum_{i=1}^{r} e_i f(\mathfrak{P}_i|\mathfrak{p})$, com $e(\mathfrak{P}_i|\mathfrak{p}) \leq e_i$, portanto $e(\mathfrak{P}_i|\mathfrak{p}) = e_i$ e $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. ∎

Definição 3.3 *Seja $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r}$, diremos que $\mathfrak{p}$ é ramificado em L se $e_i > 1$ para algum $i \in \{1, \cdots, r\}$.*

Corolário 3.8 *Com a hipótese e as notações do teorema anterior são equivalentes:*

1. *$\mathfrak{p}$ é ramificado em L.*

2. *O polinômio $\bar{P}_\theta$ é inseparável.*

3. $disc(P_\theta) \in \mathfrak{p}$.

4. $\mathfrak{p}$ *divide* $\delta_{B|A}$.

Demonstração: Seja $P = P_\theta$.
1) $\Longleftrightarrow$ 2) $\mathfrak{p}$ é ramificado em $L \Longleftrightarrow e_i > 1$ para algum $i \in \{1, \cdots, r\} \Longleftrightarrow$ na fatoração $\bar{P} = \bar{P}_1^{\,e_1} \cdots \bar{P}_r^{\,e_r}$ $e_i > 1$ para algum $i \in \{1, \cdots, r\} \Longleftrightarrow \bar{P}$ tem raízes multiplas $\Longleftrightarrow \bar{P}$ é inseparável.
2) $\Longleftrightarrow$ 3) Sejam $P(X) = (X - \theta_1) \cdots (X - \theta_n)$, onde $\theta_1, \cdots, \theta_n \in \bar{K}$ e $g(X_1, \cdots, X_n) = \prod_{i<j}(X_i - X_j)^2 \in \mathbb{Z}[X_1, \cdots, X_n]$, então $discP = g(\theta_1, \cdots, \theta_n)$ e portanto $disc\bar{P} = g(\bar{\theta}_1, \cdots, \bar{\theta}_n) = g(\theta_1, \cdots, \theta_n) + \mathfrak{p} = discP + \mathfrak{p}$ assim:

$$discP \in \mathfrak{p} \Longleftrightarrow disc\bar{P} = \mathfrak{p} \Longleftrightarrow \prod_{i<j}(\bar{\theta}_i - \bar{\theta}_j)^2 = \bar{0} \Longleftrightarrow \bar{\theta}_i = \bar{\theta}_j, \text{ para } i \neq j \Longleftrightarrow \bar{P} \text{ é}$$

inseparável.
3) $\Longleftrightarrow$ 4) Como $B = A[\theta]$, temos $L = K(\theta)$, assim $\delta_{B|A} =< disc_{L|K}(1, \theta, \cdots, \theta^{n-1}) >$

$=< discP >$, portanto $\mathfrak{p}$ divide $\delta_{B|A} \Longleftrightarrow \mathfrak{p} \supset \delta_{B|A} =< discP > \Longleftrightarrow discP \in \mathfrak{p}$. ■

Exemplo 3.1 *Seja* $L = \mathbb{Q}(\sqrt{5})$, *como* $5 \equiv 1 (mod\, 4)$, *temos* $I_L = \mathbb{Z}\left[\dfrac{1 + \sqrt{5}}{2}\right]$, *seja* $\gamma = \dfrac{1 + \sqrt{5}}{2}$, *então* $P_\gamma(X) = X^2 - X - 1$.
Consideremos $\mathfrak{p} = \langle 5 \rangle$, *então* $\bar{P}_\gamma(X) = \bar{X}^2 - \bar{X} - \bar{1} = (\bar{X} - \bar{3})^2 = \bar{P}_1^2$, *onde* $P_1(X) = X - 3$, *então :*

$$\langle 5 \rangle I_L = \mathfrak{P}_1^2,$$

onde $\mathfrak{P}_1 = 5I_L + \left(\dfrac{1 + \sqrt{5}}{2}\right) I_L$. *Em particular* $\langle 5 \rangle$ *é totalmente ramificado em* L. ■

Corolário 3.9 *Seja* $\gamma \in B$ *tal que* $L = K(\gamma)$ *e* $\mathfrak{p}$ *um ideal primo não nulo de* A *tal que* $discP_\gamma \notin \mathfrak{p}$ *então :*

1. $\{1, \gamma, \cdots, \gamma^{n-1}\}$ *é uma base do* $A_\mathfrak{p}$*-módulo* $B_\mathfrak{p}$

2. $\mathfrak{p}$ *não ramifica em L.*

Demonstração: 1) Sabemos que $B_\mathfrak{p} = I_L(A_\mathfrak{p})$. Como A é de Dedekind $A_\mathfrak{p}$ é um DIP, portanto $B_\mathfrak{p}$ é um $A_\mathfrak{p}$-módulo livre de posto $n = [L\colon K]$; seja $\{\beta_1, \cdots, \beta_n\}$ uma base de $B_\mathfrak{p}$ sobre $A_\mathfrak{p}$, então para $1 \leq i \leq n$, temos $\gamma^{i-1} = \sum_{j=1}^{n} a_{ij}\beta_i$, assim :

$$discP_\gamma = disc_{L|K}(1, \gamma, \cdots, \gamma^{n-1}) = \det(a_{ij})^2 disc_{L|K}(\beta_1, \cdots, \beta_n)$$

Por hipótese $discP_\gamma \in A - \mathfrak{p} \subset A_\mathfrak{p} - m_\mathfrak{p}$, pois $m_\mathfrak{p} \cap A = \mathfrak{p}$, logo temos que $discP_\gamma$ é inversível em $A_\mathfrak{p}$, consequentemente $\det(a_{ij})^2$ também é e portanto $\{1, \gamma, \cdots, \gamma^{n-1}\}$ é uma base do $A_\mathfrak{p}$-módulo $B_\mathfrak{p}$, e assim $B_\mathfrak{p} = A_\mathfrak{p}(\gamma)$.
Portanto podemos aplicar o corolario e o teorema anterior a $A_\mathfrak{p}$, $B_\mathfrak{p}$ e γ.
2) Como $discP_\gamma \notin m_\mathfrak{p}$ pelo corolario anterior parte 1, $\mathfrak{p}$ não é ramificado em L. ■

Observação :
Se L é um corpo de números algébricos de grau n sobre $\mathbb{Q}$, então I_L é um $\mathbb{Z}$-módulo livre de posto n pois $\mathbb{Z}$ é um DIP.

Corolário 3.10 *Para todas as bases do $\mathbb{Z}$-módulo I_L, os discriminantes coincidem.*

Demonstração: Sejam $\{\alpha_1, \cdots, \alpha_n\}$ e $\{\beta_1, \cdots, \beta_n\}$ duas bases do $\mathbb{Z}$-módulo I_L. Pela proposição 3.5, existe $a \in U(\mathbb{Z}) = \{1, -1\}$ tal que $disc_{L|\mathbb{Q}}(\alpha_1, \cdots, \alpha_n) = a^2 disc_{L|\mathbb{Q}}(\beta_1, \cdots, \beta_n)$, portanto os discriminantes coincidem. ■

Definição 3.4 *Definimos o discriminante do corpo L como $d_L = disc_{L|\mathbb{Q}}(\alpha_1, \cdots, \alpha_n)$ sendo $\{\alpha_1, \cdots, \alpha_n\}$ uma base do $\mathbb{Z}$-módulo I_L.*

O seguinte teorema será util para saber quais são os primos de $\mathbb{Z}$ que ramificam numa extensão finita de $\mathbb{Q}$.

Teorema 3.11 *Seja L uma extensão finita de $\mathbb{Q}$. Então o número de primos que ramificam em L é finito. De fato, para p primo, p ramifica em L se, e somente se, $p \mid d_L$.*

Para a demonstração do teorema anterior precisamos de alguns lemas.

Lema 3.12 *Seja $B = I_L$ um $\mathbb{Z}$-módulo livre com base $\{e_1, e_2, \cdots, e_m\}$, para qualquer ideal (n) de $\mathbb{Z}$, $\{\bar{e}_1, \cdots, \bar{e}_m\}$ é uma base do $\mathbb{Z}_n$-módulo $\dfrac{B}{nB}$ e*

$$d(\bar{e}_1, \bar{e}_2, \cdots, \bar{e}_m) \equiv d(e_1, e_2, \cdots, e_m)\,(mod\, nB)$$

Demonstração: Para $\hat{a} \in \mathbb{Z}_n$ e $\bar{x} \in \dfrac{B}{nB}$, temos que $\hat{a}\bar{x} = ax + nB = a(x + nB) = a\bar{x}$. Sejam $\hat{a}_1, \cdots, \hat{a}_m \in \mathbb{Z}_n$, tais que $a_1\bar{e}_1 + \cdots + a_m\bar{e}_m = \bar{0}$, então $a_1e_1 + \cdots + a_me_m \in nB$, assim existem $b_1, \cdots, b_m \in \mathbb{Z}$ tais que:

$$a_1e_1 + \cdots + a_me_m = n(b_1e_1 + \cdots + b_me_m).$$

O que implica que, $a_i = nb_i$ e assim $\hat{a}_i = \hat{0}$, logo $\{\bar{e}_1, \cdots, \bar{e}_m\}$ e LI e é claro que é um conjunto gerador de $\dfrac{B}{nB}$. Portanto é uma base.

Por outro lado temos que $d(\bar{e}_1, \bar{e}_2, \cdots, \bar{e}_m) = \det(T(e_ie_j + nB)) = \det(T(e_ie_j)) + nB$ o que completa a prova do lema. ■

Lema 3.13 *Seja A um domínio de Dedekind com corpo de frações K e L uma extensão separavel de K. Suponhamos que existem $B_1, \cdots, B_n$, A-modulos livres contidos todos no corpo L, se $\epsilon_i = \{\epsilon_{i1}, \cdots, \epsilon_{ik_i}\}$ é uma A-base de B_i, então :*

$$\Delta = \{(\epsilon_{11}, 0, \cdots, 0), \cdots, (\epsilon_{1k_1}, 0, \cdots, 0), \cdots, (0, 0, \cdots, \epsilon_{n1}) \cdots, (0, 0, \cdots, \epsilon_{nk_n})\}$$

é uma A-base de $\prod B_i$ e $d_{L^n|\mathbb{Q}}(\Delta) = \prod_i d_{L|\mathbb{Q}}(\epsilon_i)$.

Demonstração: É claro que Δ, e uma A-base de $\prod B_i$.
Para provar a outra afirmação do lema faremos indução sobre n, começaremos no caso $n = 2$, assim temos que se $\epsilon_1 = \{e_1, \cdots, e_m\}$ é A-base de B_1 e $\epsilon_2 = \{v_1, \cdots, v_k\}$ é A base de B_2, assim $\Delta = \{(e_1, 0), \cdots, (e_m, 0), (0, v_1), \cdots, (0, v_k)\}$.
Então : $d_{L^2|K}(\Delta) =$

$$\det\begin{pmatrix} T_{L^2|K}(e_1e_1, 0) & \cdots & T_{L^2|K}(e_1e_m, 0) & T_{L^2|K}(0,0) & \cdots & T_{L^2|K}(0,0) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ T_{L^2|K}(e_me_1, 0) & \cdots & T_{L^2|K}(e_me_m, 0) & T_{L^2|K}(0,0) & \cdots & T_{L^2|K}(0,0) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ T_{L^2|K}(0,0) & \cdots & T_{L^2|K}(0,0) & T_{L^2|K}(0, v_1v_1) & \cdots & T_{L^2|K}(0, v_1v_k) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ T_{L^2|K}(0,0) & \cdots & T_{L^2|K}(0,0) & T_{L^2|K}(0, v_kv_1) & \cdots & T_{L^2|K}(0, v_kv_k) \end{pmatrix} =$$

$$\det\begin{pmatrix} T_{L^2|K}(e_1e_1,0) & \cdots & T_{L^2|K}(e_1e_m,0) \\ \vdots & \vdots & \vdots \\ T_{L^2|K}(e_me_1,0) & \cdots & T_{L^2|K}(e_me_m,0) \end{pmatrix} \det\begin{pmatrix} T_{L^2|K}(0,v_1v_1) & \cdots & T_{L^2|K}(0,v_1v_k) \\ \vdots & \vdots & \vdots \\ T_{L^2|K}(0,v_kv_1) & \cdots & T_{L^2|K}(0,v_kv_k) \end{pmatrix}.$$

Vamos provar que para $\alpha \in L$, $T_{L^2|K}(\alpha,0) = T_{L|K}(\alpha)$.

De fato, $T_{L|K}(\alpha) = T_r(A)$, onde $A = (a_{ij})$ é a matriz tal que, $\alpha e_i = \sum_{j=1}^{m} a_{ij}e_j$.

Calculemos agora $T_{L^2|K}(\alpha,0)$. Temos que:

$$(\alpha,0)(e_i,0) = (\alpha e_i,0) = a_{i1}(e_1,0) + \cdots + a_{in}(e_m,0) + 0(0,v_1) + \cdots + 0(0,v_k)$$

$$(\alpha,0)(0,v_j) = (0,0) = 0(e_1,0) + \cdots + 0(e_m,0) + 0(0,v_1) + \cdots + 0(0,v_k)$$

Para todo $1 \leq i \leq m$ e todo $1 \leq j \leq k$.

Assim, $T_{L^2|K}(\alpha,0) = Tr\begin{pmatrix} A & 0_n \\ 0_{n\times k} & 0_k \end{pmatrix} = T_rA$, logo $T_{L^2|K}(\alpha,0) = T_{L|K}(\alpha)$.

Analogamente para $\beta \in L$, temos que $T_{L^2|K}(0,\beta) = T_{L|K}(\beta)$. Logo, podemos concluir que, $d_{L^2|K}(\Delta) = d_{L/K}(\epsilon_1)d_{L|K}(\epsilon_2)$.
Seja agora $n > 2$ e suponhamos o lema é valido para $n-1$.
Como $L^n = L^{n-1}\times L$, temos que $d_{L^n|K}(\Delta) = d_{L^{n-1}|K}(\Delta_1)d_{L|K}(\epsilon_n) = d_{L|K}(\epsilon_1)\cdots d_{L|K}(\epsilon_n)$.
Sendo Δ_1 A-base de $\prod_{1}^{n-1} B_i$. ■

Lema 3.14 *Seja B um dominio de integridade e K um corpo tal que $B \supset K$, se todo elemento de B é algebrico sobre K, então B é um corpo.*

Demonstração: Seja $\beta \in B$, como β é algebrico sobre K, temos que $K[\beta]$ é um K-espaço vetorial de dimensão finita e como B é um dominio de integridade a aplicacão $\phi\colon K[\beta] \longrightarrow K[\beta]$ tal que $\phi(x) = x\beta$ para todo $x \in K[\beta]$ é injetora, e, portanto sobrejetora; assim existe $\alpha \in K[\beta]$ tal que $\alpha\beta = 1$. ■

Definição 3.5 *Um elemento α num anel é dito nilpotente se $\alpha^m = 0$ para algum inteiro positivo m e um anel é dito reduzido se não tem elementos nilpotentes não nulos.*

Lema 3.15 *Sejam K um corpo perfeito e $B \supset K$ uma K-álgebra de dimensão finita, então B é reduzido se, e somente se:*

$$d_{B|K}(e_1, \cdots, e_m) = \det[T_{B|K}(e_i e_j)] \neq 0$$

Para toda $\{e_1, \cdots, e_m\}$ *base de* B *sobre* K.

Demonstração: Seja $\beta \neq 0$ um elemento idempotente de B. Pelo lema 3.3 e a proposição 3.5 podemos considerar uma base $\{e_1, \cdots, e_m\}$ de B tal que $e_1 = \beta$, então βe_i é nilpotente para todo i, assim a transformação K-linear $T_i \colon B \longrightarrow B$, tal que $T_i(x) = \beta e_i x$ é nilpotente, portanto tem traço nulo e assim $T_r(\beta e_i) = 0$ para todo i, logo a matriz $[T_r(e_i e_j)]$ tem a primera linha nula, consequentemente determinante nulo, logo $d_{B|K}(e_1, \cdots, e_m) = 0$.
Suponhamos agora que B é reduzido, como B é noetheriano e não tem nenhum elemento nilpotente temos que a interseção de todos seus ideais primos é nula. Agora para $\mathfrak{p}$ ideal primo de B, temos que $B/\mathfrak{p}$ é um dominio de integridade, alem disso é uma K-álgebra de dimensão finita, logo todos seus elementos são inteiros sobre K, assim pelo lema anterior $B/\mathfrak{p}$ é um corpo e $\mathfrak{p}$ é um ideal maximal.
Sejam agora $\mathfrak{p}_1, \cdots, \mathfrak{p}_g$ ideais primos de B, como eles são maximais temos que $\mathfrak{p}_i + \mathfrak{p}_j = B$, para $i \neq j$, assim pelo teorema chinês do resto temos que:

$$\frac{B}{\cap \mathfrak{p}_i} \cong \prod \frac{B}{\mathfrak{p}_i}$$

Por outro lado se $\{e_1, \cdots, e_m\}$ é base de B sobre K, então $\{e_1 + \cap\mathfrak{p}_i, \cdots, e_m + \cap\mathfrak{p}_i\}$, gera $\dfrac{B}{\cap \mathfrak{p}_i}$ como K-espaço, assim:

$$[B \colon K] \geq \left[\frac{B}{\cap \mathfrak{p}_i} \colon K\right] = \left[\prod_{i=1}^{g} \frac{B}{\mathfrak{p}_i} \colon K\right] \geq \sum_{i=1}^{g} \left[\frac{B}{\mathfrak{p}_i} \colon K\right] \geq g$$

Então o número de ideais primos de B é finito, e se B tem r ideais primos segue-se que:

$$B \cong \frac{B}{\cap_{i=1}^{r} \mathfrak{p}_i} \cong \prod_{i=1}^{r} \frac{B}{\mathfrak{p}_i}$$

Como $\dfrac{B}{\mathfrak{p}_i}$ é uma extensão finita de K, temos que ela é uma extensão separável, logo $d(e_{i1}, \cdots, e_{ik_i}) \neq 0$, onde $\{e_{i1}, \cdots, e_{ik_i}\}$ é uma base de $\dfrac{B}{\mathfrak{p}_i}$ sobre K, assim pelo lema anterior $d_{B|K}(e_1, \cdots, e_m) \neq 0$. ∎

Vamos agora provar o teorema 3.11. Seja $\{e_1, \cdots, e_m\}$ uma $\mathbb{Z}$-base de $B = I_L$; pelo lema 3.12, temos que $d_L = d(e_1, \cdots, e_m) \equiv d(\bar{e}_1, \cdots, \bar{e}_m)\,(mod pB)$, onde $\bar{x} = x + pB$, para todo $x \in B$. Agora:

$p \mid d_L \iff (p) \supset d_L \iff d(\bar{e}_1, \cdots, \bar{e}_m) = 0 \iff \dfrac{B}{pB}$ não é reduzido.

Por outro lado, se $pB = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, então $\dfrac{B}{pB} = \dfrac{B}{\cap \mathfrak{P}_i^{e_i}} \cong \prod \dfrac{B}{\mathfrak{P}_i^{e_i}}$, assim:

$$\frac{B}{pB} \cong \prod \frac{B}{\mathfrak{P}_i^{e_i}} \text{ é reduzido} \iff \frac{B}{\mathfrak{P}_i^{e_i}} \text{ é reduzido} \iff e_i = 1\ \forall i\,.$$

Logo como $\dfrac{B}{pB}$ não é reduzido, existe i tal que $e_i > 1$, assim p ramifica em L. ■

3.2 Método Geométrico

Nosso objetivo agora será mostrar que não existem extensões proprias de $\mathbb{Q}$ não ramificadas, isto é: se L é um corpo de números algebricos com $[L\colon \mathbb{Q}] \geq 2$, existirá $\mathfrak{p}$ ideal primo de $\mathbb{Z}$ que ramifica em L. Para isso usaremos a chamada *Cota de Minkowsky* que sera obtida usando o *Método geométrico*.

Definição 3.6 *Sejam $v_1, \cdots, v_m$ vetores LI no $\mathbb{R}^n$. O subgrupo $E = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$ de $(\mathbb{R}^n, +)$ é chamado rede de dimensão m gerado por $\{v_1, \cdots, v_m\}$.*

Caraterização Topologica

Dados $X = (x_1, \cdots, x_n)$, $Y = (y_1, \cdots, y_n) \in \mathbb{R}^n$ definimos:

- **Produto Interno**: $X.Y = \displaystyle\sum_{i=1}^{n} x_i y_i$.
- **Distancia**: $d(X, Y) = ||X - Y|| = \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2}$.
- **Bola de centro X e radio** $r > 0$: $B_r(X) = \{Y \in \mathbb{R}^n \mid d(X, Y) \leq r\}$.
- $S \subset \mathbb{R}^n$ é **limitado** se existe $r > 0$ tal que $S \subset B_r(0)$.
- $S \subset \mathbb{R}^n$ é **discreto** se $|S \cap B_r(0)| < +\infty\ \forall r > 0$.

- Chamamos de **Domínio fundamental** associado a $\{v_1, \cdots, v_m\}$ ao conjunto $T_E = \left\{ \sum_{i=1}^{m} a_i v_i \,\middle|\, 0 \leq a_i < 1, \forall i \in \{1, \cdots, m\} \right\}$.

Proposição 3.16 *Seja $E = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ uma rede em $\mathbb{R}^n$. Suponhamos que para $i \in \{1, \cdots, n\}$, $v_i = (a_{1i}, \cdots, a_{ni}) = \sum_{j=1}^{n} a_{ji} e_j$, onde $\{e_1, \cdots, e_n\}$ é a base canônica de $\mathbb{R}^n$; então $Vol\, T_E = |\det(a_{ij})|$.*

Demonstração: Sabemos que $Vol\, T_E = \int_{T_E} dx_1 \cdots dx_n$, sendo
$T_E = \left\{ \sum_{i=1}^{n} y_i v_i \,\middle|\, 0 \leq y_i < 1 \right\} = \left\{ \sum_{i=1}^{n} y_i \left(\sum_{j=1}^{n} a_{ji} e_i \right) \,\middle|\, 0 \leq y_i < 1 \right\}$. Para $i \in \{1, \cdots, n\}$, seja $x_i = \sum_{j=1}^{n} a_{ij} y_j$, então $\dfrac{\partial x_i}{\partial y_j} = a_{ij}$, portanto o jacobiano dessa transformação é $|\det(a_{ij})|$.
Assim $Vol\, T_E = \int_{T_E} |\det(a_{ij})|\, dy_1 \cdots dy_n = |\det(a_{ij})| \int_0^1 dy_1 \cdots \int_0^1 dy_n = |\det(a_{ij})|$

Proposição 3.17 *O volume do domínio fundamental não depende da escolha da base da rede.*

Demonstração: Suponhamos que $E = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_n$, onde $\{v_1, \cdots, v_n\}$ e $\{w_1, \cdots, w_n\}$ são duas bases da rede E, então existem inteiros c_{ij} e b_{ij} tais que $v_i = \sum_{j=1}^{n} c_{ij} w_j$ e $w_i = \sum_{j=1}^{n} b_{ij} v_j$.
Se consideramos as matrizes $C = (c_{ij})$ e $B = (b_{ij})$, então $CB = I_n$ e como $\det C$ e $\det B$ são inteiros, temos que $\det C = \det B \in \{1, -1\}$, agora como
$w_i = \sum_{j=1}^{n} b_{ij} \left(\sum_{k=1}^{n} a_{ki} e_i \right) = \sum_{j,k} b_{ij} a_{ki} e_i$, então $Vol\,(T_{E_w}) = |\det B||\det(a_{ij})| = |\det(a_{ij})|$.
■

Teorema 3.18 *Um subgrupo aditivo de $\mathbb{R}^n$ é uma rede se, e somente se, é discreto.*

Demonstração: ($\Longrightarrow$) Seja E uma rede gerada por $\{\beta_1, \cdots, \beta_m\}$. Consideremos $\{\beta_{m+1}, \cdots, \beta_n\}$ tal que $\{\beta_1, \cdots, \beta_n\}$ é uma base do $\mathbb{R}^n$.
Seja agora $E' = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n$. Vamos mostrar que E' é discreto.

De fato, para $r > 0$ e $\sum_{i=1}^{n} a_i\beta_i \in E' \cap B_r(0)$, temos que $\mid a_i \mid \leq r$ para $i \in \{1, \cdots, n\}$; mas o número de inteiros que verificam a desigualdade anterior é finito, portanto E' é discreto, e assim E é discreto.
($\Longleftarrow$) Seja $(G, +)$ um subgrupo aditivo de $\mathbb{R}^n$ e consideremos $\{g_1, \cdots, g_m\}$ um sistema maximal de elementos de G que são LI sobre $\mathbb{R}$, então eles formam uma base da rede $G_0 = \mathbb{Z}g_1 + \cdots + \mathbb{Z}g_m$. Seja T_{G_0} o domínio fundamental associado a $\{g_1, \cdots, g_m\}$, então $(G \cap T_{G_0}) + G_0 \subset G$, por outro lado para $x \in G$, o conjunto $\{x, g_1, \cdots, g_m\}$ é LD sobre $\mathbb{R}$, então $x = \sum_{i=1}^{m} \alpha_i g_i = \sum_{i=1}^{m} (\alpha_i - [\alpha_i])g_i + \sum_{i=1}^{m} [\alpha_i]g_i$ com $\alpha_i \in \mathbb{R}$, portanto $x \in (G \cap T_{G_0}) + G_0$, consequentemente $(G \cap T_{G_0}) + G_0 = G$.

Agora se $\pi\colon G \longrightarrow \dfrac{G}{G_0}$ é a projeção canônica, então $\pi(G \cap T_{G_0}) = \dfrac{G}{G_0}$; como G é discreto e T_{G_0} é limitado, $G \cap T_{G_0}$ é finito, portanto $\dfrac{G}{G_0}$ é finito.

Consideremos agora $g = \left|\dfrac{G}{G_0}\right|$. Assim para $x \in G$, $gx \in G_0$, portanto $G \subset g^{-1}G_0 = \mathbb{Z}g_1' + \cdots + \mathbb{Z}g_m'$, onde $g_i' = g^{-1}g_i$, como $\mathbb{Z}$ é um DIP e $g^{-1}G_0$ é livre tem-se que G é livre de posto $k \leq m$, logo possui uma base $\{v_1, \cdots, v_k\}$ mas $G_0 \subset G \subset g^{-1}G_0$ então os $\mathbb{R}$-espaços gerados por estes $\mathbb{Z}$-módulos coincidem, isto é $\mathbb{R}g_1' + \cdots \mathbb{R}g_m' = \mathbb{R}v_1 + \cdots \mathbb{R}v_k$, portanto $k = m$, assim $\{v_1, \cdots, v_m\}$ é LI sobre $\mathbb{R}$ e $G = \mathbb{Z}v_1 + \cdots \mathbb{Z}v_m$. ■

Lema 3.19 *Seja E uma rede de dimensão m em $\mathbb{R}^n$, são equivalentes:*

1. *m=n.*
2. $\mathbb{R}^n = \dot{\bigcup_{z \in E}} (z + T_E)$.

Demonstração: 1) $\Longrightarrow$ 2) Seja $E = \mathbb{Z}v_1 + \cdots \mathbb{Z}v_n$. Então para $x \in \mathbb{R}^n$, temos $x = \sum_{i=1}^{n} \alpha_i v_i = \sum_{i=1}^{n} (\alpha_i - [\alpha_i])v_i + \sum_{i=1}^{n} [\alpha_i]v_i$ com $\alpha_i \in \mathbb{R}$, assim $x = z + t$, sendo $z = \sum_{i=1}^{n} [\alpha_i]v_i \in E$ e $t = \sum_{i=1}^{n} (\alpha_i - [\alpha_i])v_i \in T_E$, logo $x \in z + T_E$, portanto:

$$\mathbb{R}^n = \bigcup_{z \in E} (z + T_E).$$

Agora se $z_1 + T_E = z_2 + T_E$, com $z_1, z_2 \in E$, temos que:

$$\sum_{i=1}^{n} a_i v_i + \sum_{i=1}^{n} \rho_i v_i = \sum_{i=1}^{n} a'_i v_i + \sum_{i=1}^{n} \rho'_i v_i$$

Como $\{v_1, \cdots, v_n\}$ é LI, temos $a_i + \rho_i = a'_i + \rho'_i$ para $i \in \{1, \cdots, n\}$,
logo $a_i - a'_i = \rho_i - \rho'_i$, mas $-1 < \rho_i - \rho'_i < 1$ e $a_i - a'_i \in \mathbb{Z}$, então $a_i = a'_i$ e $\rho_i = \rho'_i$,
logo $\mathbb{R}^n = \dot{\bigcup_{z \in E}}(z + T_E)$.
2) $\Longrightarrow$ 1) Suponhamos $m < n$ e $E = \mathbb{Z}v_1 + \cdots \mathbb{Z}v_m$. Então $E^T \neq (0)$, consideremos $y \in E^T$ não nulo, como $\mathbb{R}^n = \dot{\bigcup_{z \in E}}(z + T_E)$, temos que $y = z + t$, con $z \in E$ e $t \in T_E$ mas $y \perp z$ e $y \perp t$, logo $y \perp y$ assim $y = 0$ o que é uma contradição , portanto $m = n$.

Lema 3.20 *Seja $\{v_1, \cdots, v_n\}$ uma base da rede E e C um subconjunto limitado de $\mathbb{R}^n$, então $C \cap (z + T_E) = \emptyset$, para quase todo $z \in L$.*

Demonstração: Para $t = \sum_{i=1}^{n} \rho_i v_i \in T_E$, temos $\|t\| \leq \sum_{i=1}^{n} |\rho_i| \|v_i\| \leq \tau$, sendo $\tau = \sum_{i=1}^{n} \|v_i\|$. Por hipótese, existe $r > 0$ tal que $C \subset B_r(0)$, consideremos $z \in E$ que satisfaz $B_r(0) \cap (z + T_E) \neq \emptyset$, então , existe $t \in T_E$ tal que $z + t = x \in B_r(0)$, portanto $\|z\| = \|x - t\| \leq \|x\| + \|t\| \leq r + \tau$ assim $z \in B_{r+\tau}(0)$.
Como E é discreto, $E \cap B_{r+\tau}(0)$ é finito, e como $z \in E$ tal que $B_r(0) \cap (z + T_E) \neq \emptyset$ satisfaz $z \in B_{r+\tau}(0)$, temos que $B_r(0) \cap (z + T_E)$ é finito e assim $C \cap (z + T_E) = \emptyset$ para quase todo $z \in L$. ■

Teorema 3.21 *Sejam $C \subset \mathbb{R}^n$ tal que Vol C este definido e E uma rede de dimensão n. Se os conjuntos (z+C) ($z \in E$) são disjuntos dois a dois, então $Vol\, C \leq Vol\, T_E$.*

Demonstração: Pelo lema 3.19, temos que $\mathbb{R}^n = \dot{\bigcup_{z \in E}}(z + T_E)$, portanto $C = C \cap \mathbb{R}^n = \dot{\bigcup_{z \in E}}(C \cap (z + T_E))$ e pelo lema anterior existem $z_1, \cdots, z_r \in L$ tais que $C \cap (z + T_E) = \emptyset$, para todo $z \notin \{z_1, \cdots, z_r\}$, assim $C = \dot{\bigcup_{i=1}^{r}}(C \cap (z_i + T_E)$.
Como por hipótese os conjuntos $-z_i + C$ são disjuntos, a reunião

$\bigcup_{i=1}^{r}((-z_i+C)\cap T_E)$ também é disjunta, finalmente $C\cap(z_i+T_E) = ((-z_i+C)\cap T_E)+z_i$,

assim: $Vol\, C = Vol\Big(\bigcup_{i=1}^{r}(C\cap(z_i+T_E)\Big) = Vol\Big(\bigcup_{i=1}^{r}((-z_i+C)\cap T_E)+z_i\Big) =$

$Vol\Big(\bigcup_{i=1}^{r}((-z_i+C)\cap T_E)\Big) = Vol\Big(\Big(\bigcup_{i=1}^{r}(-z_i+C)\Big)\cap T_E\Big) \leq Vol\, T_E.$ ■

Teorema de Minkowsky sobre pontos de Rede

Definição 3.7 *$C \subset \mathbb{R}^n$ é simétrico se, para qualquer $c \in C$, tivermos $-c \in C$. Dizemos que C é convexo se, para quaisquer $c_1, c_2 \in C$, o conjunto:*

$$\{\rho c_1 + (1-\rho)c_2 \mid 0 \leq \rho \leq 1\}$$

está contido em C.

Teorema 3.22 *Sejam C um conjunto simétrico e convexo de $\mathbb{R}^n$ tal que $Vol\, C$ é definido e E uma rede de dimensão n. Se $Vol\, C > 2^n Vol\, T_E$, então :*

$$C \cap (E - \{0\}) \neq \emptyset.$$

Demonstração: Como $Vol\Big(\frac{1}{2}C\Big) = 2^{-n}VolC > VolT_E$, pelo teorema 3.21 os conjuntos $z + \frac{1}{2}C$, $z \in E$, não são disjumtos dois a dois, isto é, existem $z_1, z_2 \in E$, $z_1 \neq z_2$ e $c_1, c_2 \in C$ tais que $\frac{1}{2}c_1 + z_1 = \frac{1}{2}c_2 + z_2$, como C é simétrico e convexo, $-c_1 \in C$ e $z_1 - z_2 = \frac{1}{2}c_2 + (1-\frac{1}{2})(-c_1) \in C \cap (E - \{0\})$. ■

Exemplo 3.2 *Sejam n=2, $e_1 = (1,0)$, $e_2 = (0,1)$ e $E = \mathbb{Z}e_1 + \mathbb{Z}e_2$.*
Neste caso $T_E = \{(x,y) \mid 0 \leq x < 1, 0 \leq y < 1\}$, considerando
$C = \{(x,y) \in \mathbb{R}^2 \mid |x| < 1, |y| < 1)\}$, temos que $VolC = 4VolT_E$ e $C \cap (E - \{0\}) = \emptyset$.

Norma de ideais

Se L é uma extensão finita de $\mathbb{Q}$ e $\mathfrak{p}$ é um ideal primo de I_L, já vimos que $\frac{I_L}{\mathfrak{p}} = p^f$, onde $(p) = \mathfrak{p} \cap \mathbb{Z}$ e $f = \Big[\frac{I_L}{\mathfrak{p}} : \mathbb{Z}_p\Big]$

Definição 3.8 *Seja* $\mathfrak{a}$ *um ideal não nulo de* I_L*, definimos* $\mathfrak{N}(\mathfrak{a})$ *como o número (cardinal)* $\left|\frac{I_L}{\mathfrak{a}}\right|$

Proposição 3.23 *1. Para todo ideal* $\mathfrak{a}$ *não nulo de* I_L *temos* $\mathfrak{N}(\mathfrak{a}) \in \mathbb{N} - \{0\}$ *e* $\mathfrak{N}(\mathfrak{a}) = 1$ *se, e somente se,* $\mathfrak{a} = I_L$*.*

2. Para $\mathfrak{a}$ *e* $\mathfrak{b}$ *ideais não nulos de* I_L *temos* $\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$*.*

Demonstração:
1) Como I_L é um domínio de Dedekind, temos que $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, sendo $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ ideais primos de I_L. Vamos provar por indução que $\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1) \cdots \mathfrak{N}(\mathfrak{p}_r)$.
Se $r = 1$, é claro. Suponhamos que $r > 1$ e que a afirmação seja válida para qualquer produto de $r - 1$ ideais. Seja $\mathfrak{n} = \mathfrak{p}_2 \cdots \mathfrak{p}_r$, então $\mathfrak{a} = \mathfrak{p}_1\mathfrak{n} \subset \mathfrak{n}$; por outro lado sabemos que $\frac{I_L}{\mathfrak{n}} \cong \frac{\frac{I_L}{\mathfrak{a}}}{\frac{\mathfrak{n}}{\mathfrak{a}}}$, e pelo lema 2.9 temos que $\frac{\mathfrak{n}}{\mathfrak{a}} = \frac{\mathfrak{n}}{\mathfrak{p}_1\mathfrak{n}}$ é um $\frac{I_L}{\mathfrak{p}_1}$-espaço vetorial de dimensão 1, consequentemente $\left|\frac{\mathfrak{n}}{\mathfrak{a}}\right| = \left|\frac{I_L}{\mathfrak{p}_1}\right|$, então :

$$\mathfrak{N}(\mathfrak{a}) = \left|\frac{I_L}{\mathfrak{a}}\right| = \left|\frac{n}{\mathfrak{a}}\right|\left|\frac{I_L}{\mathfrak{n}}\right| = \mathfrak{N}(\mathfrak{p}_1) \cdots \mathfrak{N}(\mathfrak{p}_r) \in \mathbb{N} - \{0\}$$

2) $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ e $\mathfrak{b} = \mathfrak{q}_1 \cdots \mathfrak{q}_r$, assim $\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}(\mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{q}_1 \cdots \mathfrak{q}_r) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$. ■

Proposição 3.24 *Seja* $\mathfrak{a}$ *um ideal não nulo de* I_L*, então :*

1. Se $\mathfrak{N}(\mathfrak{a})$ *é primo, então* $\mathfrak{a}$ *é primo.*

2. $\mathfrak{N}(\mathfrak{a}) \in \mathfrak{a}$*, e, portanto,* $\mathfrak{a}$ *divide* $\mathfrak{N}(\mathfrak{a})$ *(em* I_L*).*

3. Se $\mathfrak{a}|\mathfrak{b}$ *e* $\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{b})$*, então* $\mathfrak{a} = \mathfrak{b}$*.*

Demonstração: 1) Se $\mathfrak{a}$ não é primo, então $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, com $r \geq 2$, então $\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p})_1 \cdots \mathfrak{N}(\mathfrak{p})_r$, também não é primo.

2) Por definição $\mathfrak{N}(\mathfrak{a}) = \left|\frac{I_L}{\mathfrak{a}}\right|$; então , para todo $x \in I_L$, $x\mathfrak{N}(\mathfrak{a}) \in \mathfrak{a}$. Em particular, para $x = 1$, temos $\mathfrak{N}(\mathfrak{a}) \in \mathfrak{a}$.

3) Seja $\mathfrak{c}$ um ideal de I_L tal que $\mathfrak{ac} = \mathfrak{b}$. Então $\mathfrak{N}(\mathfrak{ac}) = \mathfrak{N}(\mathfrak{b})$, assim $\mathfrak{N}(\mathfrak{c}) = 1$, e portanto $\mathfrak{c} = I_L$, logo $\mathfrak{a} = \mathfrak{b}$. ■

O seguinte teorema nos dá uma relação entre a norma de ideais e o discriminante e mostra também que ela generaliza a norma absoluta $|N_{L|\mathbb{Q}}|$.

Teorema 3.25 *1. Todo ideal não nulo $\mathfrak{a}$ de I_L é um $\mathbb{Z}$-módulo livre de posto n e se $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de $\mathfrak{a}$, então $disc_{L|\mathbb{Q}}(\alpha_1, \cdots, \alpha_n) = \mathfrak{N}(\mathfrak{a})^2 d_L$*

2. Para $\alpha \in I_L$, $\mathfrak{N}(\alpha) = |N_{L|\mathbb{Q}}(\alpha)|$

Na demonstração do teorema usaremos o seguinte resultado da Teoria de Módulos:

Teorema 3.26 *Todo submódulo N de um $\mathbb{Z}$-módulo livre M de posto n, é livre de posto $q \leq n$. Alem disso, existe uma base $\{\epsilon_1, \cdots, \epsilon_n\}$ de M e inteiros positivos $a_1, \cdots, a_n$ tais que $\{a_1\epsilon_1, \cdots a_q\epsilon_q\}$ é base de N.*

(Veja [2], p. 48)

Demonstração: (Teorema 3.25)
1) Se $[L\colon \mathbb{Q}] = n$, temos que I_L é um $\mathbb{Z}$-módulo livre de posto n. Seja $\mathfrak{a}$ um ideal de I_L, como $\mathfrak{a}$ é um $\mathbb{Z}$-submódulo de I_L. Pelo teorema anterior 3.26, existe uma base $\{\epsilon_1, \cdots, \epsilon_n\}$ de I_L e inteiros positivos $a_1, \cdots, a_n$, tais que $\{a_1\epsilon_1, \cdots, a_q\epsilon_q\}$, é uma base de $\mathfrak{a}$, sendo $q \leq n$.
Consideremos agora o isomorfismo $\varphi\colon \mathbb{Z} \times \cdots \times \mathbb{Z} \longrightarrow I_L$, dado por:

$$\varphi(z_1, \cdots, z_n) = \sum_{i=1}^{n} z_i\epsilon_i, \qquad \forall (z_1, \cdots, z_n) \in \mathbb{Z} \times \cdots \times \mathbb{Z}$$

Agora $x = \sum_{i=1}^{n} z_i\epsilon_i \in \mathfrak{a} \iff z_{q+1} = \cdots = z_n = 0$ e $z_i\epsilon_i = \alpha_i(a_i\epsilon_i)$, com $\alpha_i \in \mathbb{Z}$ e $i \in \{1, \cdots, q\} \iff z_{q+1} = \cdots = z_n = 0$ e $z_i \in a_i\mathbb{Z}$, para $i \in \{1, \cdots, q\}$.
Então temos que: $\bar{\varphi}\colon \dfrac{\mathbb{Z}}{a_1\mathbb{Z}} \times \cdots \times \dfrac{\mathbb{Z}}{a_q\mathbb{Z}} \times \mathbb{Z} \times \cdots \times \mathbb{Z} \longrightarrow \dfrac{I_L}{\mathfrak{a}}$, dado por

$$\bar{\varphi}(\bar{z}_1, \cdots, \bar{z}_q, z_{q+1}, \cdots, z_n) = \sum_{i=1}^{n} z_i\epsilon_i + \mathfrak{a}.$$

Para todo $(\bar{z}_1, \cdots, \bar{z}_q, z_{q+1}, \cdots, z_n) \in \dfrac{\mathbb{Z}}{a_1\mathbb{Z}} \times \cdots \times \dfrac{\mathbb{Z}}{a_q\mathbb{Z}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ é um isomorfismo.
Assim $\mathfrak{N}(\mathfrak{a}) = \left|\dfrac{\mathbb{Z}}{a_1\mathbb{Z}} \times \cdots \times \dfrac{\mathbb{Z}}{a_q\mathbb{Z}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}\right| < +\infty$, portanto $n - q = 0$,

logo $n = q$ e $\mathfrak{a}$ é um $\mathbb{Z}$-módulo livre de posto n.

Agora $\mathfrak{N}(\mathfrak{a}) = \left|\frac{\mathbb{Z}}{a_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{a_n\mathbb{Z}}\right| = |a_1 \cdots a_n|$ e como para $i \in \{1, \cdots, n\}$,

$a_i\epsilon_i = 0\epsilon_1 + \cdots + a_i\epsilon_i + \cdots + 0\epsilon_n$, temos que:

$disc_{L|\mathbb{Q}}(a_1\epsilon_1, \cdots, a_n\epsilon_n) = (\det A)^2 disc_{L|\mathbb{Q}}(\epsilon_1, \cdots, \epsilon_n)$, onde $A = diag(a_1, \cdots, a_n)$.

Consequentemente, $disc_{L|\mathbb{Q}}(a_1\epsilon_1, \cdots, a_n\epsilon_n) = \mathfrak{N}(\mathfrak{a})^2 d_L$.

Seja agora $\{\alpha_1, \cdots, \alpha_n\}$ uma base de $\mathfrak{a}$, então $\alpha_i = \sum_{j=1}^{n} c_{ij}(a_j\epsilon_j)$, portanto

$disc_{L|\mathbb{Q}}(\alpha_1, \cdots, \alpha_n) = (\det C)^2 disc_{L|\mathbb{Q}}(\epsilon_1, \cdots, \epsilon_n)$, onde $C = (c_{ij}) \in M_n(\mathbb{Z})$, como

$\{a_1\epsilon_1, \cdots, a_n\epsilon_n\}$ é uma $\mathbb{Z}$-base de $\mathfrak{a}$, $\det C$ é inversível em $\mathbb{Z}$ assim:

$$disc_{L|\mathbb{Q}}(\alpha_1, \cdots, \alpha_n) = disc_{L|\mathbb{Q}}(\epsilon_1, \cdots, \epsilon_n) = \mathfrak{N}(\mathfrak{a})^2 d_L.$$

2) Seja $\{\beta_1, \cdots, \beta_n\}$ uma base integral de L e $\alpha \in I_L$, então $\{\alpha\beta_1, \cdots, \alpha\beta_n\}$ é uma base de $< \alpha >$, pela parte anterior $disc_{L|\mathbb{Q}}(\alpha\beta_1, \cdots, \alpha\beta_n) = (\mathfrak{N}(\alpha))^2 d_L$.

Por outro lado $\alpha\beta_i = \sum_{j=1}^{n} a_{ij}\beta_j$, $a_{ij} \in \mathbb{Z} \subset \mathbb{Q}$ e $\{\beta_1, \cdots, \beta_n\}$ é base de $L/\mathbb{Q}$, então pela definição de norma temos $N_{L|\mathbb{Q}}(\alpha) = \det(a_{ij})$ e pelo lema 3.3, temos que

$disc_{L|\mathbb{Q}}(\alpha\beta_1, \cdots, \alpha\beta_n) = (\det(a_{ij})^2) disc_{L|\mathbb{Q}}(\beta_1, \cdots, \beta_n) = (N_{L|\mathbb{Q}}(\alpha))^2 d_L$.

Portanto $\mathfrak{N}(\alpha) = |N_{L|\mathbb{Q}}(\alpha)|$. ■

Exemplo 3.3 *Seja* $L = \mathbb{Q}(\sqrt{-17})$*, como* $-17 \equiv 3\ (mod\ 4)$ *temos que* $I_L = \mathbb{Z}[\sqrt{-17}]$ *não é fatorial, pois* $18 = 2.3.3 = (1 + \sqrt{-17})(1 - \sqrt{-17})$*, que são irredutiveis em* I_L*.*
Consideremos os ideais (distintos)

$$\mathfrak{p} = 2I_L + (1 + \sqrt{-17})I_L,\ \mathfrak{q} = 3I_L + (1 + \sqrt{-17})I_L \text{ e } \mathfrak{r} = 3I_L + (1 - \sqrt{-17})I_L$$

Temos que $\mathfrak{p}, \mathfrak{q}$ *e* $\mathfrak{r}$ *são ideais primos de* I_L *e* $18I_L = \mathfrak{p}^2\mathfrak{q}^2\mathfrak{r}^2$.

De fato, para $x \in \mathfrak{p}$, existem $a, b, c, d \in \mathbb{Z}$ tais que:
$x = 2(a+b\sqrt{-17}) + (1+\sqrt{-17})(c+d\sqrt{-17}) = (2a+c-17d) + (2b+c+d)\sqrt{-17} = m + n\sqrt{-17}$,sendo $m = 2a + c - 17d$ e $n = 2b + c + d$.
Então $m - n = 2(a-b) - 18d$ que é par, portanto $\mathfrak{p} = \{m + n\sqrt{-17} \mid m \equiv n\ (mod 2)\}$, logo $\mathfrak{p} \subsetneq I_L$.
Agora para $y \in I_L$, $y = a + b\sqrt{-17}$, se $a - b$ é par temos de $y \in \mathfrak{p}$ e se $a - b$ é ímpar $y - 1 = (a - 1) + b\sqrt{-17}$ e $(a - 1) - b$ é par, assim $y - 1 \in \mathfrak{p}$, logo:

$$\frac{I_L}{\mathfrak{p}} = \{\mathfrak{p}, 1 + \mathfrak{p}\}$$

Analogamente pode-se mostrar que

$$\frac{I_L}{\mathfrak{q}} = \{\mathfrak{q}, 1 + \mathfrak{q}, 2 + \mathfrak{q}\} \text{ e que } \frac{I_L}{\mathfrak{r}} = \{\mathfrak{r}, 1 + \mathfrak{r}, 2 + \mathfrak{r}\}$$

Portanto, $\mathfrak{N}(\mathfrak{p}) = 2$ e $\mathfrak{N}(\mathfrak{q}) = \mathfrak{N}(\mathfrak{r}) = 3$. Assim pelo item 1 da proposição 3.24 temos que, $\mathfrak{p}$, $\mathfrak{q}$ e $\mathfrak{r}$ são ideais primos de I_L.
Vamos mostrar agora que $18I_L = \mathfrak{p}^2\mathfrak{q}^2\mathfrak{r}^2$.
De fato, $1-\sqrt{-17} \in \mathfrak{p}$ pois $1-\sqrt{-17} = 2(1)+(1+\sqrt{-17})(-1)$, também $1+\sqrt{-17} \in \mathfrak{p}$, portanto $18 = (1+\sqrt{-17})(1-\sqrt{-17}) \in \mathfrak{p}^2$, logo $\mathfrak{p}^2| < 18 >$.
$3 \in \mathfrak{q}$, então $3.3 \in \mathfrak{q}^2$ assim $18 = 2.3.3 \in \mathfrak{q}^2$, consequentemente $\mathfrak{q}^2 | < 18 >$, analogamente $\mathfrak{r}^2 | < 18 >$, e como I_L é um domínio de Dedekind, tem-se que $\mathfrak{p}^2\mathfrak{q}^2\mathfrak{r}^2| < 18 >$, assim $< 18 > \subset \mathfrak{p}^2\mathfrak{q}^2\mathfrak{r}^2$.
Pelo teorema anterior $\mathfrak{N}(< g >) = N_{L|\mathbb{Q}}(18) = 18^2$, por outro lado $\mathfrak{N}(\mathfrak{p}^2\mathfrak{q}^2\mathfrak{r}^2) = 2^2 3^2 3^2 = 18^2$, assim pela proposição 3.24 parte 3, temos que $18I_L = \mathfrak{p}^2\mathfrak{q}^2\mathfrak{r}^2$. ■

3.3 O espaço Ł^{s,t}

Seja $L = \mathbb{Q}(\theta)$, onde θ é inteiro sobre $\mathbb{Z}$ e $\sigma_1, \cdots, \sigma_n$ os monomorfismos $L \longrightarrow \mathbb{C}$ que deixam $\mathbb{Q}$ fixo.

- Se $\sigma_i(L) \subset \mathbb{R}$ ($\sigma_i(\theta) \in \mathbb{R}$), dizemos que σ_i é *real*.
- Se $\sigma_i(L) \nsubseteq \mathbb{R}$, dizemos que σ_i é *complexo*.
- Como a conjugação complexa é um automorfismo de $\mathbb{C}$, temos que $\bar{\sigma}_i$ é um monomorfismo de $L \longrightarrow \mathbb{C}$, então $\bar{\sigma}_i = \sigma_j$ para algum $j \in \{1, \cdots, n\}$ e sabemos que $\bar{\sigma}_i = \sigma_i$ se, e somente se, σ_i é real.
  Então $n = s+2t$, onde s é o número de monomorfismos reais e $2t$ é o número de monomorfismos complexos e eles são :
  $\sigma_1, \cdots, \sigma_s, \sigma_{s+1}, \bar{\sigma}_{s+1} \cdots, \sigma_{s+t}, \bar{\sigma}_{s+t}$.
- Definimos Ł$^{s,t} = \mathbb{R}^s \times \mathbb{C}^t$, notemos que Ł$^{s,t} \cong \mathbb{R}^n$, como $\mathbb{R}$-espaço. Se $\alpha = (\alpha_1, \cdots, \alpha_n)$, e $\beta = (\beta_1, \cdots, \beta_n) \in$ Ł^{s,t}, definimos:

$$\alpha + \beta = (\alpha_1 + \beta_1, \cdots, \alpha_n + \beta_n) \quad \text{e} \quad \alpha\beta = (\alpha_1\beta_1, \cdots, \alpha_n\beta_n)$$

Consideremos agora o monomorfismo $\sigma\colon L \longrightarrow Ł^{s,t}$ dado por:
$\sigma(\alpha) = (\sigma_1(\alpha), \cdots, \sigma_s(\alpha), \sigma_{s+1}(\alpha), \cdots, \sigma_{s+t}(\alpha))$, $\forall \alpha \in L$, então para $\alpha, \beta \in L$ temos:

- $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$.
- $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$.
- Dado $r \in \mathbb{Q}$, $\sigma(r\alpha) = r\sigma(\alpha)$.

Teorema 3.27 *Se $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de $L \,/\, \mathbb{Q}$, então $\sigma(\alpha_1), \cdots, \sigma(\alpha_n)$ são LI sobre $\mathbb{R}$.*

Demonstração: Para $k \in \{1, \cdots, s\}$, seja $\sigma_k(\alpha_l) = x_k^{(l)}$, e para $j \in \{1, \cdots, t\}$, seja $\sigma_j(\alpha_l) = y_j^{(l)} + iz_j^{(l)}$, onde $x_k^{(l)}, y_j^{(l)}$ e $z_j^{(l)}$ são números reais para todo $l \in \{1, \cdots, n\}$, então : $\sigma(\alpha_l) = (x_1^{(l)}, \cdots, x_s^{(l)}, y_1^{(l)} + iz_1^{(l)}, \cdots, y_t^{(l)} + iz_t^{(l)})$.
Vamos mostrar que:

$$D = \begin{vmatrix} x_1^{(1)} & \cdots & x_s^{(1)} & y_1^{(1)} & z_1^{(1)} & \cdots & y_t^{(1)} & z_t^{(1)} \\ x_1^{(2)} & \cdots & x_s^{(2)} & y_1^{(2)} & z_1^{(2)} & \cdots & y_t^{(2)} & z_t^{(2)} \\ \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ x_1^{(n)} & \cdots & x_s^{(n)} & y_1^{(n)} & z_1^{(n)} & \cdots & y_t^{(n)} & z_t^{(n)} \end{vmatrix} \neq 0.$$

De fato, multiplicando $\begin{pmatrix} z_k^{(1)} \\ z_k^{(2)} \\ \vdots \\ z_k^{(n)} \end{pmatrix}$ por i e somando a $\begin{pmatrix} y_k^{(1)} \\ y_k^{(2)} \\ \vdots \\ y_k^{(n)} \end{pmatrix}$ temos

$$D = i^{-t} \begin{vmatrix} x_1^{(1)} & \cdots & x_s^{(1)} & y_1^{(1)} + iz_1^{(1)} & iz_1^{(1)} & \cdots & y_t^{(1)} + iz_t^{(1)} & iz_t^{(1)} \\ x_1^{(2)} & \cdots & x_s^{(2)} & y_1^{(2)} + iz_1^{(2)} & iz_1^{(2)} & \cdots & y_t^{(2)} + iz_t^{(2)} & iz_t^{(2)} \\ \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ x_1^{(n)} & \cdots & x_s^{(n)} & y_1^{(n)} + iz_1^{(n)} & iz_1^{(n)} & \cdots & y_t^{(n)} + iz_t^{(n)} & iz_t^{(n)} \end{vmatrix}$$

Agora multiplicando

$\begin{pmatrix} y_k^{(1)} + iz_k^{(1)} \\ y_k^{(2)} + iz_k^{(2)} \\ \vdots \\ y_k^{(n)} + iz_k^{(2)} \end{pmatrix}$ por $\frac{1}{2}$ e fazendo a diferença com $\begin{pmatrix} iz_k^{(1)} \\ iz_k^{(2)} \\ \vdots \\ iz_k^{(n)} \end{pmatrix}$ temos:

$$D = i^{-t}\begin{vmatrix} x_1^{(1)} & \cdots & x_s^{(1)} & y_1^{(1)} + iz_1^{(1)} & \dfrac{y_1^{(1)} - iz_1^{(1)}}{-2} & \cdots & y_t^{(1)} + iz_t^{(1)} & \dfrac{y_t^{(1)} - iz_t^{(1)}}{-2} \\ x_1^{(2)} & \cdots & x_s^{(2)} & y_1^{(2)} + iz_1^{(2)} & \dfrac{y_1^{(2)} - iz_1^{(2)}}{-2} & \cdots & y_t^{(2)} + iz_t^{(2)} & \dfrac{y_t^{(2)} - iz_t^{(2)}}{-2} \\ \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ x_1^{(n)} & \cdots & x_s^{(n)} & y_1^{(n)} + iz_1^{(n)} & \dfrac{y_1^{(n)} - iz_1^{(n)}}{-2} & \cdots & y_t^{(n)} + iz_t^{(n)} & \dfrac{y_t^{(n)} - iz_t^{(n)}}{-2} \end{vmatrix}$$

$$= (-2i)^{-t}\begin{vmatrix} x_1^{(1)} & \cdots & x_s^{(1)} & y_1^{(1)} + iz_1^{(1)} & y_1^{(1)} - iz_1^{(1)} & \cdots & y_t^{(1)} + iz_t^{(1)} & y_t^{(1)} - iz_t^{(1)} \\ x_1^{(2)} & \cdots & x_s^{(2)} & y_1^{(2)} + iz_1^{(2)} & y_1^{(2)} - iz_1^{(2)} & \cdots & y_t^{(2)} + iz_t^{(2)} & y_t^{(2)} - iz_t^{(2)} \\ \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ x_1^{(n)} & \cdots & x_s^{(n)} & y_1^{(n)} + iz_1^{(n)} & y_1^{(n)} - iz_1^{(n)} & \cdots & y_t^{(n)} + iz_t^{(n)} & y_t^{(n)} - iz_t^{(n)} \end{vmatrix}.$$

Por tanto $D = (-2i)^{-t}[\det(\sigma_k(\alpha_l))]$, mas como $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de $L/\mathbb{Q}$, temos que $\det(\sigma_k(\alpha_l))^2 = disc_{L|\mathbb{Q}}(\alpha_1, \cdots, \alpha_n) \neq 0$, assim $D \neq 0$ e o conjunto $\{\sigma(\alpha_1), \cdots, \sigma(\alpha_n)\}$ é LI sobre $\mathbb{R}$. ■

Teorema 3.28 *Sejam L um corpo de números de grau $n = s + 2t$ e $\mathfrak{a}$ um ideal não nulo de I_L, então o volume do domínio fundamental de $\sigma(\mathfrak{a})$ em $\mathbb{L}^{s,t}$ é $2^{-t}\mathfrak{N}(\mathfrak{a})\sqrt{|d_L|}$.*

Demonstração: Seja $\{\alpha_1, \cdots, \alpha_n\}$ uma $\mathbb{Z}$-base de $\mathfrak{a}$. Como σ é um monomorfismo, temos que $\{\sigma(\alpha_1), \cdots, \sigma(\alpha_n)\}$ é uma $\mathbb{Z}$-base de $\sigma(\mathfrak{a})$.
Com as notações do teorema anterior temos:

$$\sigma(\alpha_l) = (x_1^{(l)}, \cdots, x_s^{(l)}, y_1^{(l)} + iz_1^{(l)}, \cdots, y_t^{(l)} + iz_t^{(l)}).$$

Então , pela proposição 3.16, tem-se que:

$$Vol\, T_\sigma(\mathfrak{a}) = |D| = |(-2i)^{-t}[\det(\sigma_k(\alpha_l))]| = 2^{-t}|\det(\sigma_k(\alpha_l))| = 2^{-t}\sqrt{|disc_{L|\mathbb{Q}}(\alpha_1, \cdots, \alpha_n)|}\,.$$

Como $\{\alpha_1, \cdots, \alpha_n\}$ é uma $\mathbb{Z}$-base de $\mathfrak{a}$, pelo teorema 3.25 temos que $disc_{L|\mathbb{Q}}(\alpha_1, \cdots, \alpha_n) = \mathfrak{N}(\mathfrak{a})^2 d_L$, assim, $Vol\, T_\sigma(\mathfrak{a}) = 2^{-t}\mathfrak{N}(\mathfrak{a})\sqrt{|d_L|}$. ■

Um pouco de Cálculo

Lema 3.29 *Para $a_i > 0$, seja $I(a_1, \cdots, a_m; c) = \int_{Z(c)} x_1^{a_1} \cdots x_m^{a_m} dx_1 \cdots dx_m$, sendo* $Z(c) = \left\{ X \in R^n \middle| \, x_i \geq 0, \sum_{i=1}^{m} x_i \leq c \right\}$, *então :*

$$I(a_1, \cdots, a_m; c) = c^{\beta_m} \frac{\Gamma(a_1 + 1) \cdots \Gamma(a_m + 1)}{\Gamma(a_1 + \cdots a_m + 1)}.$$

Onde $\Gamma(x) = \int_0^\infty e^{-t} t^{x-1} dt \quad e \quad \beta_m = \sum_{i=1}^{m} a_i + m.$

Demonstração: Seja $x_i' = cx_i$, então $\frac{\partial x_i'}{\partial x_j} = \begin{cases} c, \ se \ i = j. \\ 0, \ se \ i \neq j. \end{cases}$

Portanto $I(a_1, \cdots, a_m; c) = \int_{Z(1)} c^m (cx_1')^{a_1} \cdots (cx_m')^{a_m} dx_1' \cdots dx_m' =$

$\int_{Z(1)} c^{\beta_m} x_1' \cdots x_m' dx_1' \cdots dx_m' = c^{\beta_m} I(a_1, \cdots, a_m; 1).$

Então , e suficiente mostrar que :

$I(a_1, \cdots, a_m; 1) = \frac{\Gamma(a_1 + 1) \cdots \Gamma(a_m + 1)}{\Gamma(a_1 + \cdots a_m + 1)}$; para isso usaremos indução sobre m.

Se $m = 1$, $I(a_1; 1) = \int_0^1 x^{a_1} dx = \frac{1}{a_1 + 1} = \frac{\Gamma(a_1 + 1)}{\Gamma(a_1 + 2)}$, seja agora $m > 1$ e

suponhamos a formula valida para $m - 1$.

Consideremos o conjunto $Z(x_m)' = \left\{ X \in \mathbb{R}^{m-1} \middle| \, x_i \geq 0, \sum_{i=1}^{m-1} x_i \leq 1 - x_m \right\}$, então

$I(a_1, \cdots, a_m; 1) = \int_0^1 x_m^{a_m} \left(\int_{Z(x_m)'} x_1^{a_1} \cdots x_{m-1}^{a_{m-1}} dx_1 \cdots dx_{m-1} \right) dx_m =$

$\int_0^1 x_m^{a_m} I(a_1, \cdots, a_{m-1}; 1 - x_m) dx_m.$

Mas $I(a_1, \cdots, a_{m-1}; 1 - x_m) = (1 - x_m)^{\beta_{m-1}} I(a_1, \cdots, a_{m-1}; 1).$

Portanto:
$I(a_1, \cdots, a_m; 1) = I(a_1, \cdots, a_{m-1}; 1) \int_0^1 x_m^{a_m}(1 - x_m)^{\beta_{m-1}} dx_m$, e como:

$$\int_0^1 x^{m-1}(1-x)^{n-1}dx = B(m,n) = \frac{\Gamma(m)\Gamma(n)}{\Gamma(m+n)}$$

Temos, $I(a_1, \cdots, a_m; 1) = I(a_1, \cdots, a_{m-1}; 1)\dfrac{\Gamma(a_m+1)\Gamma(a_1+\cdots a_{m-1}+m)}{\Gamma(a_1+\cdots a_m+m+1)} =$

$$\frac{\Gamma(a_1+1)\cdots\Gamma(a_{m-1}+1)\Gamma(a_m+1)\Gamma(a_1+\cdots+a_{m-1}+m)}{\Gamma(a_1+\cdots+a_{m-1}+m)\Gamma(a_1+\cdots+a_m+m+1)} = \frac{\Gamma(a_1+1)\cdots\Gamma(a_m+1)}{\Gamma(a_1+\cdots+a_m+1)}.$$

■

Lema 3.30 *Para qualquer número real $c > 0$, consideremos o conjunto*
$X(c) = \left\{(x_1, \cdots, x_s, z_{s+1}, \cdots, z_{s+t}) \mid \sum_{i=1}^{s} |x_i| + 2\sum_{i=s+1}^{s+t} |z_i| \leq c\right\}$, *então :*

$$Vol(X(c)) = 2^s\left(\frac{\pi}{2}\right)^t \frac{1}{n!}c^n.$$

Demonstração: Como $X(c)$ é simétrico em relação à origem, tem-se que $Vol(X(c)) = 2^s Vol(Y(c))$, onde $Y(c) = \{(x_1, \cdots, x_s, z_{s+1}, \cdots, z_{s+t}) \in X(c) \mid x_i \geq 0\}$.
Para as variaveis complexas fazemos a seguinte mudança de variaveis:
$z_j = x_j + iy_j = \dfrac{1}{2}\rho_j(\cos\theta_j + isen\theta_j)$, com $\rho_j \geq 0$ e $0 \leq \theta_j \leq 2\pi$, o jacobiano dessa transformação é $\dfrac{1}{4^t}\rho_{s+1}\cdots\rho_{s+t}$, depois de integrar sobre os θ_j, temos:

$$Vol(X(c)) = 2^s 4^{-t}(2\pi)^t \int_Z \rho_{s+1}\cdots\rho_{s+t}dx_1\cdots dx_s d\rho_{s+1}\cdots d\rho_{s+t}$$

Sendo $Z = \left\{(X,\rho) \in \mathbb{R}^{r+t} \mid x_i, \rho_i \geq 0, \sum_{i=1}^{s} x_i + \sum_{i=s+1}^{s+t} \rho_i \leq c\right\}$, logo pelo lema anterior com $m = s+t$, $a_i = 0$ para $i \in \{1, \cdots, s\}$ e $a_i = 1$ para $i \in \{s+1, \cdots, m\}$, temos:

$$Vol(X(c)) = 2^s 4^{-t}(2\pi)^t c^{t+s+t}\frac{\Gamma(1)\cdots\Gamma(1)\Gamma(2)\cdots\Gamma(2)}{\Gamma(1+\cdots+1+s+t+1)} =$$

$$2^s 4^{-t}(2\pi)^t c^{t+s+t}\frac{1}{\Gamma(s+2t+1)} = 2^s\left(\frac{\pi}{2}\right)^t c^{t+s+t}\frac{1}{\Gamma(n+1)} = 2^s\left(\frac{\pi}{2}\right)^t c^n\frac{1}{n!}.$$ ■

Exemplo 3.4 • *Quando $s = 2$ e $t = 0$, temos* $X(c) = \{(x, y) \in \mathbb{R}^2 \mid |x| + |y| \leq c\}$, *que é um cuadrado de lados com comprimento* $\sqrt{2}c$ *e portanto:* $A(X(c)) = 2c^2$.

• *No caso $s = 0$ e $t = 1$, $X(c)$ é um círculo de radio* $\frac{c}{2}$, *que tem área* $\frac{\pi c^2}{4}$.

Lema 3.31 *Sejam $a_1, \cdots, a_n$ números reais não negativos, então :*

$$\left(\prod_{i=1}^{n} a_i\right)^{\frac{1}{n}} \leq \frac{\sum_{i=1}^{n} a_i}{n}$$

Teorema 3.32 *Sejam L um corpo de números algébricos de grau n=s+2t e $\mathfrak{a} \neq 0$ um ideal de I_L, então existe $\alpha \in \mathfrak{a}$ não nulo tal que* $|N_{L|\mathbb{Q}}(\alpha)| \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|d_L|}\mathfrak{N}\mathfrak{a}$.

Demonstração: Para $c > 0$, seja $X(c)$ definido como no lema anterior; sabemos que $X(c)$ é simétrico, convexo e $Vol(X(c)) = 2^s\left(\frac{\pi}{2}\right)^t \frac{1}{n!}c^n$.
Seja $T_{\sigma(\mathfrak{a})}$ o domínio fundamental de $\mathfrak{a}$, então pelo teorema 3.28 temos:

$$Vol(T_{\sigma(\mathfrak{a})}) = 2^{-t}\mathfrak{N}(\mathfrak{a})\sqrt{|d_L|}$$

Pelo teorema de Minkowsky para pontos de rede, $X(c) \cap (\sigma(\mathfrak{a}) - 0) \neq \emptyset$, quando $Vol(X(c)) > 2^n Vol(T_{\sigma(\mathfrak{a})})$, isto é $2^s\left(\frac{\pi}{2}\right)^t \frac{1}{n!}c^n > 2^n 2^{-t}\mathfrak{N}(\mathfrak{a})\sqrt{|d_L|}$ ou seja, quando $2^s\left(\frac{\pi}{2}\right)^t \frac{1}{n!}c^n > 2^{s+2t}2^{-t}\mathfrak{N}(\mathfrak{a})\sqrt{|d_L|}$, ou equivalentemente quando $c^n > \left(\frac{4}{\pi}\right)^t n!\mathfrak{N}(\mathfrak{a})\sqrt{|d_L|}$.
Dado $\epsilon > 0$, escolhemos c_ϵ, tal que $c_\epsilon^n = \left(\frac{4}{\pi}\right)^t n!\mathfrak{N}(\mathfrak{a})\sqrt{|d_L|} + \epsilon$, portanto pelo teorema de Minkowski, existe $\alpha \in \mathfrak{a}$ não nulo tal que $\sigma(\alpha) \in X(c_\epsilon)$, pelo lema anterior temos que $|N_{L|\mathbb{Q}}(\alpha)| = \prod_{i=1}^{n} |\sigma_i(\alpha)| \leq \left(\frac{\sum_{i=1}^{n} |\sigma_i(\alpha)|}{n}\right)^n$, mas sabemos que:

$$|\sigma_{s+1}(\alpha)| = |\sigma_{s+2}(\alpha)|, \cdots, |\sigma_{s+2t-1}(\alpha)| = |\sigma_{s+2t}(\alpha)|$$

Portanto:

$$|N_{L|\mathbb{Q}}(\alpha)| \leq \frac{1}{n^n}\left(\sum_{i=1}^{n} |\sigma_i(\alpha)| + 2(|\sigma_{s+1}(\alpha)| + |\sigma_{s+3}(\alpha)| + \cdots |\sigma_{s+2t-1}(\alpha)|)\right) < \left(\frac{c_\epsilon}{n}\right)^n,$$
$$\text{pois } \sigma(\alpha) \in X(c_\epsilon)$$

Por outro lado, como $\mathfrak{a}$ é discreto, temos que $A_\epsilon = \left\{\alpha \in \mathfrak{a} \,\middle|\, |N_{L|\mathbb{Q}}(\alpha)| \leq \left(\frac{c_\epsilon}{n}\right)^n\right\}$ é finito, além disso $A_\epsilon \neq \emptyset, \forall \epsilon > 0$. Assim, $A = \bigcap_{\epsilon>0} A_\epsilon \neq \emptyset$.

Se escolhemos $\alpha \in A$, obtemos $|N_{L|\mathbb{Q}}(\alpha)| \leq \left(\frac{c_\epsilon}{n}\right)^n = \frac{\left(\frac{4}{\pi}\right)^t n!\mathfrak{N}(\mathfrak{a})\sqrt{|d_L|} + \epsilon}{n^n}$, para todo $\epsilon > 0$, portanto $|N_{L|\mathbb{Q}}(\alpha)| \leq \left(\frac{c}{n}\right)^n$, onde $c^n = \left(\frac{4}{\pi}\right)^t n!\mathfrak{N}(\mathfrak{a})\sqrt{|d_L|}$.

Assim $|N_{L|\mathbb{Q}}(\alpha)| \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\mathfrak{N}(\mathfrak{a})\sqrt{|d_L|}$. ∎

Definição 3.9 *Sejam L um corpo de números algébricos de dimensão n=s+2t, $\mathscr{F}$ o grupo multiplicativo dos ideais fracionários de I_L e $\mathscr{P}$ o subgrupo de $\mathscr{F}$ formado por seus ideais principais, isto é:*

$$\mathscr{P} = \{c\mathfrak{a} \mid c \in L \text{ e } \mathfrak{a} \text{ é ideal principal de } I_L\}$$

Definimos o grupo de classes, como o quociente $\mathscr{H} = \frac{\mathscr{F}}{\mathscr{P}}$.

- $\mathscr{H}$ é um grupo com a operação $(\mathfrak{m}\mathscr{P})(\mathfrak{n}\mathscr{P}) = (\mathfrak{m}\mathfrak{n})\mathscr{P}, \forall \mathfrak{m}, \mathfrak{n} \in \mathscr{F}$.
- Dizemos que, $\mathfrak{m}$ e $\mathfrak{n}$ são equivalentes se: $\mathfrak{m}\mathscr{P} = \mathfrak{n}\mathscr{P}$, isto é, quando existe $\mathfrak{j} \in \mathscr{P}$ tal que $\mathfrak{m} = \mathfrak{j}\mathfrak{n}$.
- A anterior relação entre ideais de $\mathscr{F}$ é de equivalência e se $\mathfrak{m}$ é equivalente a $\mathfrak{n}$, então $\mathfrak{m}^{-1}$ é equivalente a $\mathfrak{n}^{-1}$.

Podemos establecer agora um corolario do teorema anterior.

Corolário 3.33 *Todo ideal $\mathfrak{a}$ de I_L é equivalente a um ideal $\mathfrak{b}$ não nulo de I_L cuja norma é $\leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|d_L|}$.*

Demonstração: Seja $\mathfrak{a}$ um ideal não nulo de I_L e seja $\mathfrak{a}^{-1} \in \mathscr{F}$, então $\mathfrak{a}^{-1} = c\mathfrak{c}$, onde $c \in L^*$ e $\mathfrak{c}$ é um ideal não nulo de I_L.
Como $\langle c\rangle \in \mathscr{P}$, temos que $\mathfrak{c}$ é equivalente a $\mathfrak{a}^{-1}$, pelo teorema anterior existe $\alpha \in \mathfrak{c}$ não nulo tal que $|N_{L|\mathbb{Q}}(\alpha)| \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\mathfrak{N}(\mathfrak{c})\sqrt{|d_L|}$, como $\alpha \in \mathfrak{c}$ temos que $\mathfrak{c} \,|\langle\alpha\rangle$, e portanto existe $\mathfrak{b}$ ideal não nulo de I_L, tal que $\mathfrak{b}\mathfrak{c} = \langle\alpha\rangle$, assim

$\mathfrak{N}(\mathfrak{bc}) = \mathfrak{N}(\alpha) = |N_{L|\mathbb{Q}}(\alpha)|$, consequentemente $\mathfrak{N}(\mathfrak{b}) = \dfrac{\mathfrak{N}(<\alpha>)}{\mathfrak{N}(\mathfrak{c})} \leq \left(\dfrac{4}{\pi}\right)^t \dfrac{n!}{n^n}\sqrt{|d_L|}$. ■

Vamos agora establecer o teorema mais importante desta seção .

Teorema 3.34 Teorema de Minkowsky *Seja L um corpo de números algébricos tal que* $[L:\mathbb{Q}] \geq 2$*, então* $|d_L| > 1$*. Em particular existe* $\mathfrak{p}$ *ideal primo de* $\mathbb{Z}$ *que ramifica em L.*

Demonstração: Seja $\mathfrak{a}$ um ideal não nulo de L tal que $\mathfrak{N}(\mathfrak{a}) \leq \left(\dfrac{4}{\pi}\right)^t \dfrac{n!}{n^n}\sqrt{|d_L|}$.

Então $\sqrt{|d_L|} \geq \left(\dfrac{\pi}{4}\right)^t \dfrac{n^n}{n!}\mathfrak{N}(\mathfrak{a}) \geq \left(\dfrac{\pi}{4}\right)^t \dfrac{n^n}{n!}$, como $s + 2t = n$, temos $\dfrac{s}{2} + t = \dfrac{n}{2}$, e daí $t \leq \dfrac{n}{2}$.

Agora como $\dfrac{\pi}{4} < 1$, temos $\left(\dfrac{\pi}{4}\right)^t \geq \left(\dfrac{\pi}{4}\right)^{\frac{n}{2}}$, portanto $\sqrt{|d_L|} \geq \dfrac{n^n}{n!}\left(\dfrac{\pi}{4}\right)^{\frac{n}{2}} = s_n$.

Por outro lado, $\dfrac{s_{n+1}}{s_n} = \dfrac{\frac{(n+1)^{n+1}}{(n+1)!}\left(\frac{\pi}{4}\right)^{\frac{n}{2}}}{\frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{\frac{n}{2}}} = \dfrac{n!(n+1)^{n+1}}{(n+1)!n^n}\left(\dfrac{\pi}{4}\right)^{\frac{1}{2}} =$

$\dfrac{1}{n+1}\left(\dfrac{n+1}{n}\right)^n (n+1)\left(\dfrac{\pi}{4}\right)^{\frac{1}{2}} = \left(1+\dfrac{1}{n}\right)^n \left(\dfrac{\pi}{4}\right)^{\frac{1}{2}} > 1$, pois $\left(1+\dfrac{1}{n}\right)^n > \dfrac{2}{\sqrt{\pi}}$.

Assim (s_n) é crescente e como $s_2 > 1$, temos $1 < \lim\limits_{n\to\infty} s_n \leq \sqrt{|d_L|}$, logo $|d_L| > 1$.
Portanto, temos que $d_l \notin \{1,-1\} = U(\mathbb{Z})$, logo existe $\mathfrak{p}$ ideal primo de $\mathbb{Z}$ tal que $\mathfrak{p} \supset < d_L >$, assim $\mathfrak{p}$ ramifica em L.

3.4 Automorfismo de Frobenius

Lema 3.35 *Seja K um corpo de números algébricos e* $\mathfrak{p}$ *um ideal primo não nulo de* I_K*, então* $\dfrac{I_K}{\mathfrak{p}}$ *é finito.*

Demonstração: De fato, considerando $\mathfrak{p}_1 = \mathfrak{p} \cap \mathbb{Z}$, temos que $\mathfrak{p}_1$ é um ideal primo não nulo de $\mathbb{Z}$, e que $\mathfrak{p}$ está acima de $\mathfrak{p}_1$, como K é extensão de Galois de $\mathbb{Q}$, pelo teorema 2.4 temos que $\left[\dfrac{I_K}{\mathfrak{p}} : \dfrac{\mathbb{Z}}{\mathfrak{p}_1}\right]$ é finito e, como $\dfrac{\mathbb{Z}}{\mathfrak{p}_1} \cong \mathbb{Z}_{\mathfrak{p}_1}$, temos que $\dfrac{I_K}{\mathfrak{p}}$ é finito.
■

Consideremos agora agora L uma extensão de Galois de K e $\mathfrak{p}$ um ideal primo de $B = I_L$ que está acima de $\mathfrak{p}$

$$\begin{array}{ccc} \mathfrak{P} & B = I_L & L \\ | & | & | \\ \mathfrak{p} & A = I_K & K \\ & | & | \\ & \mathbb{Z} & \mathbb{Q} \end{array}$$

Temos que:

- A é um domínio de Dedekind.
- $B = I_L(A)$
- L é extensão de Galois de $K = Q(A)$

Assim, pelo teorema 2.4, $\dfrac{B}{\mathfrak{P}}$ é extensão finita de $\dfrac{A}{\mathfrak{p}}$, logo separável e portanto normal, consequentemente $G((B/\mathfrak{P})/(A/\mathfrak{p})) \cong \dfrac{G_{\mathfrak{P}}}{T_{\mathfrak{P}}}$.
Suponhamos que $\left|\dfrac{A}{\mathfrak{p}}\right| = q$ e $\left[\dfrac{B}{\mathfrak{P}} : \dfrac{A}{\mathfrak{p}}\right] = f$, então $\left|\dfrac{B}{\mathfrak{P}}\right| = q^f$.
Consideremos agora:

$$\bar{\sigma} : \frac{B}{\mathfrak{P}} \longrightarrow \frac{B}{\mathfrak{P}}, \text{ dado por } \bar{\sigma}(x + \mathfrak{P}) = x^q + \mathfrak{P}.$$

Então , $\bar{\sigma}$ é um automorfismo tal que $< \bar{\sigma} >= G((B/\mathfrak{P})/(A/\mathfrak{p}))$, ese automorfismo é chamado *Automorfismo de Frobenius*. ■

Observação : Como consequência do corolário 2.25 temos que $\dfrac{T_{\mathfrak{P}}}{V_1}$ é isomorfo a um subgrupo do grupo multiplicativo $\left(\dfrac{B}{\mathfrak{P}}\right)^*$ de $\dfrac{B}{\mathfrak{P}}$. Portanto, $\dfrac{T_{\mathfrak{P}}}{V_1}$ é cíclico e sua ordem divide $q^f - 1$

Teorema 3.36 *Se $\dfrac{G_{\mathfrak{P}}}{V_1}$ é abeliano, então $\dfrac{T_{\mathfrak{P}}}{V_1}$ é um grupo cíclico cuja ordem divide $q - 1$.*

Demonstração: Suponhamos primeiramente que B é um DIP e consideremos π um gerador de $\mathfrak{P}$. Seja $\sigma \in T_{\mathfrak{P}}$, então $\sigma \in G_{\mathfrak{P}}$, logo $\sigma(\pi) = a_\sigma \pi$, com $a_\sigma \in B$ e $a_\sigma \notin \mathfrak{P}$.
De fato, de $a_\sigma \in \mathfrak{P}$, temos que $\sigma(\pi) \in \mathfrak{P}^2$, logo $\pi = \sigma^{-1}(\sigma\pi) \in \mathfrak{P}^2 = (\pi^2)$, assim existe $\alpha \in \mathfrak{P}$ tal que $\pi = \pi^2\alpha$, consequentemente $\pi\alpha = 1$ o que implica $\mathfrak{P} = B$, absurdo.
Agora para $\rho \in T_{\mathfrak{P}}$, temos $\sigma(\rho\pi) = \sigma(a_\rho\pi) = \sigma(a_\rho)a_\sigma\pi$ e $\sigma\rho(\pi) = a_{\sigma\rho}\pi$, assim:

$$\sigma(a_\rho)a_\sigma\pi = a_{\sigma\rho}\pi.$$

Como $\sigma \in T_{\mathfrak{P}}$, temos que $\sigma(a_\rho) - a_\rho \in \mathfrak{P}$, portanto $a_{\sigma\rho} - a_\rho a_\sigma = \sigma(a_\rho)a_\sigma - a_\rho a_\sigma = (\sigma(a_\rho) - a_\rho)a_\sigma \in \mathfrak{P}$, isto é:

$$a_{\rho\sigma} \equiv a_\rho a_\sigma \,(mod\, \mathfrak{P}).$$

Portanto, $\overline{a_{\rho\sigma}} = \overline{a_\rho}\,\overline{a_\sigma}$ onde $\bar{x} = x + \mathfrak{P}$, para todo $x \in B$, logo a aplicação $\sigma \mapsto \overline{a_\sigma}$ é um homomorfismo de $T_{\mathfrak{P}}$ no grupo multiplicativo $\left(\frac{B}{\mathfrak{P}}\right)^*$, seu kernel é o conjunto dos $\sigma \in T_{\mathfrak{P}}$ tais que $a_\sigma \equiv 1\,(mod\,\mathfrak{P})$ isto é $a_\sigma\pi \equiv \pi\,(mod\,\mathfrak{P}^2)$, afirmamos que este conjunto é V_1.
De fato, se $z \in \mathfrak{P}$, $z = a\pi$ para algum $a \in B$, então $\sigma(z) - z = \sigma(a\pi) - a\pi = (\sigma(a) - a)\pi + \sigma(a)(\sigma(\pi) - \pi) \in \mathfrak{P}^2$, assim $\sigma(z) - z \in \mathfrak{P}^2$, por outro lado como $f(\mathfrak{P}|\mathfrak{P}^t) = 1$, então $\frac{B^t}{\mathfrak{P}^t} = \frac{B}{\mathfrak{P}}$, assim dado $x \in B$ existem $y \in B^t$ e $z \in \mathfrak{P}$ tais que $x = y + z$, portanto $\sigma(x) - x = \sigma(y) - y + \sigma(z) - z$, como $B^t = B \cap L^t$ e L^t é o corpo fixo de $T_{\mathfrak{P}}$, temos que $\sigma(y) = y$, assim $\sigma(x) - x = \sigma(z) - z \in \mathfrak{P}^2$ o que prova a nossa afirmação .
Portanto, a aplicação $\sigma \mapsto \overline{a_\sigma}$ induz um isomorfismo de $\frac{T_{\mathfrak{P}}}{V_1}$ num subgrupo de $\left(\frac{B}{\mathfrak{P}}\right)^*$.
Sejam agora $\tau \in T_{\mathfrak{P}}$ tal que sua coclase $mod\, V_1$ gera $\frac{T_{\mathfrak{P}}}{V_1}$ e $\sigma \in G_{\mathfrak{P}}$ tal que σ induz o automorfismo de Frobenius $\xi + \mathfrak{P} \mapsto \xi^q + \mathfrak{P}$ de $\frac{B}{\mathfrak{P}}$ sobre $\frac{A}{\mathfrak{p}}$, para simplificar notações escrevamos:

$$\sigma\pi = a\pi, \quad \tau\pi = b\pi \quad \text{e} \quad \sigma\tau\sigma^{-1}\pi = c\pi$$

Como por hipótese $\frac{G_{\mathfrak{P}}}{V_1}$ é abeliano, temos que $\sigma\tau\sigma^{-1}V_1 = \tau V_1$ e ja vimos que $\frac{T_{\mathfrak{P}}}{V_1}$ é isomorfo a um subgrupo de $\left(\frac{B}{\mathfrak{P}}\right)^*$, com isomorfismo dado por a aplicação $\rho V_1 \mapsto \overline{a_\rho}$, então $\bar{c} = \bar{b}$.
Por outro lado, temos que $\pi = \sigma^{-1}(a\pi) = \sigma^{-1}(a)\sigma^{-1}(\pi)$, assim:

$$\sigma^{-1}(\pi) = \sigma^{-1}(a)^{-1}\pi.$$

Observemos que, $\sigma^{-1}(a)^{-1} = \sigma^{-1}(\pi)\pi^{-1} \in B$. De fato $\sigma^{-1}(\pi) \in \mathfrak{P}$, $\pi \in \mathfrak{P}$, assim $\sigma^{-1}(\pi) - \pi = y\pi$, $y \in B$, logo:

$$\sigma^{-1}(\pi)\pi^{-1} = 1 + y \in B$$

Vamos agora calcular o c acima. Temos que, $c\pi = \sigma\tau\sigma^{-1}\pi = \sigma\tau(\sigma^{-1}(a)^{-1}\pi) = \sigma(\tau\sigma^{-1}(a)^{-1}b\pi) = \sigma\tau(\sigma^{-1}(a)^{-1})\sigma(b)a\pi$, portanto:

$$c = \sigma\tau(\sigma^{-1}(a)^{-1})\sigma(b)a$$

Reduzindo *mod* $\mathfrak{P}$ e lembrando que $\overline{\tau(x)} = \bar{x}$ para todo $x \in B$, temos que:

$$\bar{c} = \overline{\sigma\tau(\sigma^{-1}(a)^{-1})\sigma(b)a} = \overline{\sigma\sigma^{-1}(a)^{-1}\sigma(b)a} = \overline{a^{-1}\sigma(b)a} = \overline{\sigma(b)} = \overline{b}^q.$$

Assim $\bar{b}^q = \bar{c}$, portanto $\bar{b}^{q-1} = 1$, logo $o(\bar{b})$ divide $q - 1$.
Sabemos que $\tau V_1 \mapsto \bar{b}$ via um isomorfismo, assim $o(\tau V_1) = o(b)$ o que prova o teorema nesse caso particular.
No caso geral, consideremos $S_{\mathfrak{p}} = A - \mathfrak{p}$, $A_{\mathfrak{p}} = S_{\mathfrak{p}}^{-1}A$ e $B_{\mathfrak{p}} = S_{\mathfrak{p}}^{-1}B$, então pelas proposições 1.26 e 1.28 $A_{\mathfrak{p}}$ é um dominio de Dedekind com um único ideal maximal $\mathfrak{p}A_p$, logo pelo teorema 1.16 $B_{\mathfrak{p}}$ também é um dominio de Dedekind e como o número de ideais primos de $B_{\mathfrak{p}}$ (que são da forma $\mathfrak{P}B_{\mathfrak{p}}$) é finito, temos pelo teorema 1.22 que $B_{\mathfrak{p}}$ é um DIP, mas pela proposição 2.19 sabemos que $G_{\mathfrak{P}} = G_{\mathfrak{P}B_{\mathfrak{p}}}$ e para $i \geq 0$, $V_i(\mathfrak{P}) = V_i(\mathfrak{P}B_{\mathfrak{p}})$, portanto aplicando todos estes resultados temos a prova do teorema no caso geral. ■

Capítulo 4

Extensões Ciclotômicas

4.1 Fatos e definições elementares

- Seja $\overline{\mathbb{Q}} \subset \mathbb{C}$ o fecho algébrico de $\mathbb{Q}$ e $m \in \mathbb{Z}^+$. O polinômio $X^m - 1 \in \mathbb{Q}[X]$ tem m raízes distintas $\zeta_1, \cdots, \zeta_m \in \overline{\mathbb{Q}}$, que são chamadas *raízes m-ésimas da unidade*.

- Se $G = \{\zeta_1, \cdots, \zeta_m\}$, então $(G, \cdot)$ é um grupo cíclico e se $\zeta \in G$ é um gerador, ζ é chamado *raíz primitiva m-ésima da unidade*.

- Temos que, para $a \in \mathbb{Z}$, ζ^a é uma raíz primitiva m-ésima da unidade se, e somente se, $(a, m) = 1$. Portanto para cada $m \in \mathbb{Z}^+$ temos, $\phi(m)$ raízes primitivas m-ésimas da unidade.

- $L = \mathbb{Q}(\zeta_1, \cdots, \zeta_m) = \mathbb{Q}(\zeta)$ é chamado *corpo das raízes m-ésimas da unidade* e uma *extensão ciclotômica* de $\mathbb{Q}$ é, por definição , um subcorpo de L que contém $\mathbb{Q}$.

Proposição 4.1 *$L = \mathbb{Q}(\zeta)$ é uma extensão abeliana de grau $\phi(m)$ sobre $\mathbb{Q}$, pois dado $\sigma \in G(L/\mathbb{Q})$, $\sigma(\zeta) = \zeta^a$, onde $(a, m) = 1$ e a aplicação $G(L/\mathbb{Q}) \longrightarrow (\mathbb{Z}m)^\times$, $\sigma \mapsto a$ é um isomorfismo, além disso o polinômio minimal de ζ é*

$$P_\zeta(X) = \prod_{\substack{i=1 \\ (i,m)=1}}^{m} (X - \zeta^i).$$

[Veja [7], p. 190]

Proposição 4.2 *Se $L_1, L_2, \cdots, L_n$ são extensões ciclotômicas, então $L_1 L_2 \cdots L_n$ é uma extensão ciclotômica.*

Notação : Se G é um grupo ciclico de ordem m, notaremos G por $c(m)$.

Proposição 4.3 *Seja $m = p^r$, $r \in \mathbb{Z}^+$ e p um primo ímpar. Consideremos ζ uma raíz primitiva m-ésima da unidade e $L = \mathbb{Q}(\zeta)$, então $G(L/\mathbb{Q})$ é um grupo cíclico de ordem $\phi(m) = p^{r-1}(p-1)$.*
E se $r \geq 2$ e $m = 2^r$, $G(L/\mathbb{Q}) = c(2) \times c(2^{r-2})$, onde $c(2)$ é gerado por $\sigma \in G(L/\mathbb{Q})$, dado por $\sigma(\zeta) = \zeta^{-1}$ e $c(2^{r-2})$ é gerado por $\tau \in G(L/\mathbb{Q})$, dado por $\tau(\zeta) = \zeta^5$.

[Veja [7], p. 86 e p.88].

Proposição 4.4 *Seja ζ uma raíz primitiva m-ésima da unidade, então :*

$$\prod_{\substack{0 \leq i,j \leq m-1, \\ i \neq j}} (\zeta^i - \zeta^j) = (-1)^{m-1} m^m$$

Demonstração: Como ζ é uma raíz primitiva m-ésima da unidade, temos que $X^m - 1 = \prod_{i=0}^{m-1} (X - \zeta^i)$, portanto:

$$(-1)^{m-1} = \prod_{i=0}^{m-1} \zeta^i$$

Por outro lado, vale que:

$$mX^{m-1} = \sum_{j=0}^{m-1} \prod_{i=0,\ i \neq j}^{m-1} (X - \zeta^j).$$

Agora se fazemos $X = \zeta^j$ obtemos que, $m\zeta^{j(m-1)} = \sum_{j=0}^{m-1} \prod_{i=0,\ i \neq j}^{m-1} (\zeta^j - \zeta^i)$, assim tomando produtos da equação anterior para $j = 0, \cdots, m-1$. Temos que:

$$m^m \Big(\prod_{j=0}^{m-1} \zeta^j \Big)^{m-1} = \prod_{\substack{0 \leq i,j \leq m-1 \\ i \neq j}} (\zeta^j - \zeta^i).$$

Consequentemente, $\prod_{\substack{0 \leq i,j \leq m-1 \\ i \neq j}} (\zeta^i - \zeta^j) = (-1)^{m-1} m^m$. ■

Proposição 4.5 *Sejam ζ uma raíz primitiva m-ésima da unidade e $p \in \mathbb{Z}$ um primo, se p ramifica em $\mathbb{Q}(\zeta)$, então $p \mid m$.*

Demonstração: Sabemos que $\{1, \zeta, \cdots, \zeta^{\phi(m)-1}\}$ é uma base de $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$ e que $G(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\sigma_a \mid (m, a) = 1\}$, onde $\sigma_a(\zeta) = \zeta^a$, $(a, m) = 1$.
Seja P_ζ o polinômio minimal de ζ sobre $\mathbb{Q}$, então :

$d_{L|\mathbb{Q}}(1, \zeta, \cdots, \zeta^{\phi(m)-1}) = \triangle(P_\zeta) = \prod_{\substack{i<j \\ (i,m)=(j,m)=1}} (\sigma_j(\zeta) - \sigma_i(\zeta))^2$ o que é um subproduto do produto da proposição anterior.
Portanto $\triangle(P_\zeta) = d_{L|\mathbb{Q}}(1, \zeta, \cdots, \zeta^{\phi(m)-1}) \mid m^m$, seja agora um primo $p \in \mathbb{Z}$ que ramifica em $\mathbb{Q}(\zeta)$. Pelo corolario 3.9 temos que $\triangle(P_\zeta) \in p\mathbb{Z}$, assim $p \mid \triangle(f)$ e como $\triangle(P_\zeta) \mid m^m$, $p \mid m^m$ o que implica $p \mid m$. ■

Teorema 4.6 *Sejam $a \in Z^+$ e $m = p^a$, onde $p \in \mathbb{Z}$ é primo. Se ζ é uma raíz primitiva m-ésima da unidade e $\mathfrak{p}$ é um primo de $I_{\mathbb{Q}(\zeta)}$ acima de p, então :*

- $(1 - \zeta)^{\phi(m)} = (p)$ *em* $I_{\mathbb{Q}(\zeta)}$.
- $e(\mathfrak{p} \mid p) = \phi(m)$, $f(\mathfrak{p} \mid p) = 1$ *e* $r(\mathfrak{p} \mid p) = 1$.

Demonstração: Sabemos que $\langle\zeta\rangle = \{1, \zeta, \cdots, \zeta^{p^a-1}\}$, e, assim

$\langle\zeta^p\rangle = \{1, \zeta^p, \zeta^{2p}, \cdots, \zeta^{p(p^{a-1}-1)}\}$ que é o conjunto das raízes de $X^{\frac{m}{p}} - 1$.

Portanto as raízes de $\dfrac{X^m - 1}{X^{\frac{m}{p}} - 1}$ são as raízes primitivas m-ésimas de 1, isto é:

$$\frac{X^m - 1}{X^{\frac{m}{p}} - 1} = \prod_{\substack{0 \le b \le m \\ (b,m)=1}} (X - \zeta^b).$$

Usando a regra de L'Hospital, temos que:

$$p = \lim_{X \to 1} \frac{X^m - 1}{X^{\frac{m}{p}} - 1} = \lim_{X \to 1} \prod_{\substack{0 \le b \le m \\ (b,m)=1}} (X - \zeta^b) = \prod_{\substack{0 \le b \le m \\ (b,m)=1}} (1 - \zeta^b) = (1 - \zeta)^{\phi(m)} \prod_{\substack{0 \le b \le m \\ (b,m)=1}} \frac{1 - \zeta^b}{1 - \zeta}.$$

Vamos mostrar que se $(b, m) = 1$, $\dfrac{1 - \zeta^b}{1 - \zeta}$ é uma unidade em $I_{\mathbb{Q}(\zeta)}$.
De fato, sabemos que:

$$\frac{1 - \zeta^b}{1 - \zeta} = 1 + \zeta + \cdots + \zeta^{b-1} \in I_{\mathbb{Q}(\zeta)}.$$

Agora como $(b, m) = 1$, existe $a \in \mathbb{Z}$ tal que $ab \equiv 1 (mod\, m)$. Logo $\zeta^{ab} = \zeta$, portanto:

$$\frac{1-\zeta}{1-\zeta^b} = \frac{1-\zeta^{ab}}{1-\zeta^b} = 1 + \zeta^b + \cdots + \zeta^{b(a-1)} \in I_{\mathbb{Q}(\zeta)}.$$

Assim $\dfrac{1-\zeta^b}{1-\zeta} \in U(I_{\mathbb{Q}(\zeta)})$ e consequentemente $(1-\zeta)^{\phi(m)} = (p)$ em $I_{\mathbb{Q}(\zeta)}$.
Consideremos agora a decomposição de $(1-\zeta)$ em $I_{\mathbb{Q}(\zeta)}$ como produto de ideais primos, isto é:

$$(1-\zeta)I_{\mathbb{Q}(\zeta)} = \mathfrak{P}_1^{k_1} \cdots \mathfrak{P}_s^{k_s}.$$

Logo, $pI_{\mathbb{Q}(\zeta)} = (1-\zeta)^{\phi(m)} I_{\mathbb{Q}(\zeta)} = \mathfrak{P}_1^{\phi(m)k_1} \cdots \mathfrak{P}_s^{\phi(m)k_s}$. Como $\mathfrak{p}$ está acima de p, existe $j \in \{1, \cdots, s\}$ tal que $\mathfrak{p} = \mathfrak{P}_j$, assim $e(\mathfrak{p} \mid p) = \phi(m)k_j \geq \phi(m)$, portanto $e(\mathfrak{p} \mid p) = \phi(m)$ e como $e(\mathfrak{p} \mid p) f(\mathfrak{p} \mid p) r(\mathfrak{p} \mid p) = \phi(m)$, temos $f(\mathfrak{p} \mid p) = r(\mathfrak{p} \mid p) = 1$.
■

Corolário 4.7 *Sejam $m \in \mathbb{Z}$ e p um número primo, tal que p divide m então :*

- *Se $m = p^s m'$, com $(p, m') = 1$ e $p^s > 2$, então p ramifica em $\mathbb{Q}(\zeta)$.*
- *Se $m = 2m'$ com m' ímpar, temos que $\mathbb{Q}(\zeta) = \mathbb{Q}(\xi)$, sendo ξ uma raíz primitiva m'-ésima da unidade.*

Demonstração: Sejam $m = p^s m'$ com $(p, m') = 1$ e ξ uma raíz p^s-ésima da unidade, então $\mathbb{Q}(\xi) \subset \mathbb{Q}(\zeta)$.
Consideremos agora $\mathfrak{p}$ um ideal primo de $I_{\mathbb{Q}(\xi)}$ que está acima de p, pela proposição anterior $e(\mathfrak{p}|p) = \phi(p^s)$, se $p^s > 2$, então $e(\mathfrak{p}|p) > 1$, assim se $\mathfrak{P}$ é um ideal primo de $I_{\mathbb{Q}(\zeta)}$ que está acima de $\mathfrak{p}$, então $e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{p})e(\mathfrak{p}|p) > 1$, logo p ramifica em $\mathbb{Q}(\zeta)$.
Agora se $m = 2m'$ como m' é ímpar. Temos que:

$$\zeta = \exp \tfrac{2\pi i}{2m'} \quad \text{e} \quad -\xi = -\exp \tfrac{2\pi i}{m'} = \exp \pi i \exp \tfrac{2\pi i}{m'} = \exp \tfrac{(2+m')2\pi i}{2m'} = \zeta^{2+m'}$$

Portanto $\mathbb{Q}(\zeta) = \mathbb{Q}(\xi)$ se $(2m', 2+m') = 1$. Seja p primo tal que $p \mid 2m'$ e $p \mid 2+m'$, então p é impar e $p \mid m'$, portanto $p \mid (2 + m') - m'$, assim $p = 1$. ■

Teorema 4.8 *Seja ξ uma raíz primitiva p^n-ésima da unidade e $L = \mathbb{Q}(\xi)$, então ;*

$$d_{L|\mathbb{Q}}(1, \xi, \cdots, \xi^{\phi(p^n)-1}) = (-1)^{\frac{p(p-1)}{2}} p^{n\phi(p^n) - p^{n-1}}$$

Para a demonstração do teorema precisamos do seguinte resultado referente a discriminantes.

Proposição 4.9 *Seja L uma extensão de grau n de um corpo K e $\alpha \in L$ tal que $L = K(\alpha)$. Se f é o polinômio minimal de α sobre K então :*

$$d_{L|K}(1, \alpha, \cdots, \alpha^{n-1}) = (-1)^{\binom{n}{2}} N_{L|K}(f'(\alpha)).$$

Demonstração: Pela proposição 3.2 temos que:

$$d_{L|K}(1, \alpha, \cdots, \alpha^{n-1}) = \prod_{i<j}(\alpha_i - \alpha_j)^2 = \prod_{i<j}(\alpha_i - \alpha_j)\prod_{i<j}(\alpha_i - \alpha_j) =$$

$$(-1)^{\binom{n}{2}}\prod_{i\neq j}(\alpha_i - \alpha_j) = (-1)^{\binom{n}{2}}\prod_{i}\prod_{j\neq i}(\alpha_i - \alpha_j).$$

Agora se $f(X) = (X - \alpha_1)\cdots(X - \alpha_n)$, então $f'(X) = \sum_{k}\prod_{j\neq k}(X - \alpha_j)$, assim $f'(\alpha_i) = \prod_{j\neq i}(\alpha_i - \alpha_j)$, portanto $d_{L|K}(1, \alpha, \cdots, \alpha^{n-1}) = (-1)^{\binom{n}{2}}\prod_{i=1}^{n} f'(\alpha_i) =$

$$(-1)^{\binom{n}{2}}\prod_{i=1}^{n}\sigma_i f'(\alpha) = (-1)^{\binom{n}{2}} N_{L|K}(f'(\alpha)).$$ ■

Vamos agora demonstrar o teorema.

Demonstração: (Teorema 4.8)

$X^{p^n} - 1 = (X^{p^{n-1}} - 1)(X^{p^{n-1}(p-1)} + X^{p^{n-1}(p-2)} + \cdots + 1)$. Seja $W(x) = \dfrac{X^{p^n} - 1}{X^{p^{n-1}} - 1} \in \mathbb{Q}[X]$, então $W(x) = X^{p^{n-1}(p-1)} + X^{p^{n-1}(p-2)} + \cdots + 1$. Logo, $\partial W = p^{n-1}(p-1) = [L\colon \mathbb{Q}]$ e como $P_{\xi}(X) = \prod_{\substack{i=1,\\(i,\,p^n)=1}}^{n}(X - \xi^i)$ tem grau $\phi(p^n) = p^{n-1}(p-1)$, então W é o polinômio minimal de ξ.

Logo pela proposição anterior temos que:

$$d_{L|\mathbb{Q}}(1, \xi, \cdots, \xi^{\phi(p^n)-1}) = (-1)^{\binom{\phi(p^n)}{2}} N_{L|K}(W'(\xi))$$

Agora como $W(X)(X^{p^{(n-1)}} - 1) = X^{p^n} - 1$, tem-se que:

$$W'(X)(X^{p^{(n-1)}} - 1) + p^{n-1}W(X)X^{p^{(n-1)}-1} = p^n X^{p^n-1}$$

Seja agora $\xi^{p^{(n-1)}} = \eta$, então η é uma raíz p-ésima da unidade e:

$$W'(\xi)(\eta-1)+p^{n-1}W(\xi)\xi^{p^{n-1}-1}=p^n\eta, \text{ logo } W'(\xi)=\frac{p^n\eta}{\eta-1}$$

Por outro lado notemos que:

$\binom{\phi(p^n)}{2}=\frac{p^{n-1}(p-1)(p^{n-1}(p-1)-1)}{2}=\frac{p(p-1)}{2}w$, onde $w=p^{n-2}(p^{n-1}(p-1)-1)$ é um número ímpar assim $(-1)^{\binom{\phi(p^n)}{2}}=(-1)^{\frac{p(p-1)}{2}}$.

Portanto, temos que:

$$d_{L|\mathbb{Q}}(1,\xi,\cdots,\xi^{\phi(p^n)-1})=(-1)^{\frac{p(p-1)}{2}}\prod_{\substack{j=1\\(j,p^n)=1}}^{p^n}\frac{p^n\eta^j}{\eta^j-1}=(-1)^{\frac{p(p-1)}{2}}\prod_{\substack{j=1,\\(j,p-1)=1}}^{p-1}\left(\frac{p^n\eta^j}{\eta^j-1}\right)^{p^{n-1}}$$

Mas $\prod_{j=1}^{p-1}\eta^j=1$, pois as η^j são raízes de $\phi_p(X)=\frac{X^p-1}{X-1}$ e como $\eta-1,\cdots,\eta^{p-1}-1$, são as raízes de $\psi_p(X)=\phi_p(X+1)=X^{p-1}\binom{p}{p-1}X^{p-2}+\cdots+\binom{p}{j}X^{j-1}+\cdots+\binom{p}{1}$, temos que, $\prod_{j=1}^{p-1}(\eta^j-1)=p$.

Assim $d_{L|\mathbb{Q}}(1,\xi,\cdots,\xi^{\phi(p^n)-1})=(-1)^{\frac{p(p-1)}{2}}\prod_{j=1}^{p-1}\frac{(p^n)^{p^{n-1}}}{p^{p^{n-1}}}=(-1)^{\frac{p(p-1)}{2}}\frac{p^{n(p^n-1)(p-1)}}{p^{p^{n-1}}}=(-1)^{\frac{p(p-1)}{2}}p^{n\phi(p^n)-p^{n-1}}$

4.2 Teorema de Kronecker-Weber

Vamos agora enunciar o teorema principal de nosso trabalho que dá uma caracterização de todas as extensões abelianas e finitas de $\mathbb{Q}$.

Teorema 4.10 Teorema de Kronecker-Weber

Se K uma extensão abeliana e finita de $\mathbb{Q}$, então K é uma extensão ciclotômica.

Lema 4.11 *Se o teorema de Kronecker-Weber se verifica para extensões cíclicas de ordem a potência de um primo, então se verifica para as extensões abelianas finitas.*

Demonstração: Seja K uma extensão abeliana de $\mathbb{Q}$, pelo teorema fundamental para grupos abelianos temos que $G = G(K\,|\,\mathbb{Q})$ é soma direta de n subgrupos cíclicos G_i onde cada um deles é de ordem $p_i^{m_i}$, sendo $p_i, m_i \in \mathbb{N}$ e p_i primo.

Consideremos agora K_i o corpo fixo de $\bigoplus_{j\neq i} G_j$, como $\bigoplus_{j\neq i} G_j \triangleleft G$, K_i é uma extensão de Galois de $\mathbb{Q}$. Por outro lado temos que:

$$G(K_i\,|\,\mathbb{Q}) \cong \frac{G(K\,|\,\mathbb{Q})}{G(K\,|\,K_i)} \cong \frac{\bigoplus G_j}{\bigoplus_{j\neq i} G_j} \cong G_i$$

Assim, temos que $G(K_i\,|\,\mathbb{Q})$ é cíclico de ordem $p_i^{m_i}$, e, portanto, K_i é ciclotômico. Vamos provar que K é o compositum dos K_i, pelo teorema fundamental da teoria de galois é suficiente provar que $\bigcap_{i=1}^{n} \hat{G}_i = (0)$ sendo $\hat{G}_i = \bigoplus_{j\neq i} G_j$.
Provaremos isto primeiramente para o caso sobre $n = 3$, para os casos $n = 1$ e $n = 2$ é trivial, nesse caso temos que $G = G_1 \oplus G_2 \oplus G_3$, assim $\hat{G}_1 = G_2 \oplus G_3$, $\hat{G}_2 = G_1 \oplus G_3$ e $\hat{G}_3 = G_1 \oplus G_2$, agora se $x \in \hat{G}_1 \oplus \hat{G}_2 \oplus \hat{G}_3$, existem $y_1, z_1 \in G_1$, $x_2, z_2 \in G_2$ e $x_3, y_3 \in G_3$ tais que:

$$x = x_1 + x_2,\;\; x = y_1 + y_3,\;\; x = z_1 + z_2$$

Igualando as duas ultimas equações temos que $z_1 + z_2 = y_1 + y_3$, portanto $z_1 - y_1 = y_3 - z_2$, assim $y_3 - z_2 = 0$ portanto $y_3 = z_2 = 0$, analogamente igualando as duas primeiras temos que $y_1 = x_2 = 0$, logo $x = 0$.
Vamos agora provar o caso geral. Se $G = \bigoplus_{i=1}^{n} G_i$ e $x \in \bigcap_{i=1}^{n} \hat{G}_i$, então em particular $x \in \hat{G}_1 \cap \hat{G}_2$, assim existem $y_i, z_i \in G_i$ tais que:

$$x = y_2 + y_3 + \cdots + y_n \;\text{ e }\; x = z_1 + z_3 + \cdots + z_n.$$

Logo $y_2 = z_1 + (z_3 - y_3) + \cdots + (z_n - y_n) \in G_2 \cap (G_1 + G_3 + \cdots + G_n) = (0)$. Assim $y_2 = 0$. Analogamente de $x \in \hat{G}_1 \cap \hat{G}_i$, podemos concluir $y_i = 0$, para qualquer $i \in \{2, \cdots, n\}$, logo $x = 0$; que era o que queriamos provar. Portanto, concluimos que K é o compositum dos K_i, assim temos que K é ciclotômica. ∎

Lema 4.12 *Seja K uma extensão abeliana de $\mathbb{Q}$ de grau λ^m, com λ primo. Para a prova do teorema de Kronecker-Weber é suficiente provar que K é ciclotômica com a hipótese adicional de que todo primo $p \neq \lambda$ não ramifica em K.*

Demonstração: Sejam $\{p_1, \cdots, p_n\}$ os primos que ramificam em K e consideremos $p \neq \lambda$ um deles.
Seja agora $\mathfrak{P}$ um ideal primo de I_K que está acima de p, assim se $f = f(\mathfrak{P}|p)$, temos que $\frac{I_K}{\mathfrak{P}}$ tem p^f elementos e pelo corolário 2.25 sabemos que, para $j \geq 1$, $\frac{V_j}{V_{j+1}}$ é isomorfo a um subgrupo de $\left(\frac{I_K}{\mathfrak{P}}, +\right)$, então $\left|\frac{V_j}{V_{j+1}}\right|$ divide p^f, além disso, se $G = G(K\,|\,\mathbb{Q})$ temos:

$$\frac{G}{V_j} \cong \frac{\frac{G}{V_{j+1}}}{\frac{V_j}{V_{j+1}}}, \text{ assim } \left|\frac{V_j}{V_{j+1}}\right| = \frac{\left|\frac{G}{V_{j+1}}\right|}{\left|\frac{G}{V_j}\right|} = \lambda^{m'}.$$

Sendo $0 \leq m' \leq m$, mas λ e p são primos distintos, então $m' = 0$, portanto $\frac{V_j}{V_{j+1}}$ é trivial para $j \geq 1$, conseqüentemente $V_1 = V_2 = \cdots$, mas existe $n_0 \in \mathbb{N}$ tal que V_{n_0} é trivial, assim temos que V_j é trivial para todo $j \geq 1$. Logo pelo teorema 3.36, temos que $T_{\mathfrak{P}}$ é um grupo cíclico cuja ordem divide $p-1$ e como $|T_{\mathfrak{P}}| = \lambda^u$, com $0 \leq u \leq m$, temos que $p \equiv 1\,(mod \lambda^u)$.
Seja agora ξ uma raíz primitiva p-ésima da unidade, então pela proposição 4.1, $\mathbb{Q}(\xi)/\mathbb{Q}$ é uma extensão cíclica de ordem $p-1$, portanto existe um único subcorpo L de $\mathbb{Q}(\xi)$, tal que $L/\mathbb{Q}$ tem grau λ^u.

$$\begin{array}{ccc} \mathfrak{P}_1 & I_{\mathbb{Q}(\xi)} & \mathbb{Q}(\xi) \\ | & | & | \\ \mathfrak{P}_2 & I_L & L \\ | & | & | \\ p & \mathbb{Z} & \mathbb{Q} \end{array}$$

Pelo teorema 4.6 (com $a = 1$), sabemos que p é totalmente ramificado em $\mathbb{Q}(\xi)$, e, portanto, $r(\mathfrak{P}_1|p) = f(\mathfrak{P}_1|p) = 1$, logo $r(\mathfrak{P}_2|p) = f(\mathfrak{P}_2|p) = 1$. Assim, p é totalmente ramificado em L e para p' primo, $p' \neq p$ temos que p' não ramifica em L (pois ele não ramifica em $\mathbb{Q}(\xi)$).
Seja KL o compositum de K e L, como $[K : \mathbb{Q}] = \lambda^m$ e $[L : \mathbb{Q}] = \lambda^u$, temos que

$[KL : \mathbb{Q}] = \lambda^{m+v}$, sendo $v \leq u$.
Consideremos agora $\mathfrak{P}'$ ideal primo de I_{KL} que está acima de $\mathfrak{P}$, lembremos que $G_{\mathfrak{P}'} = \{\sigma \in G(KL/\mathbb{Q}) | \, \sigma(\mathfrak{P}') = \mathfrak{P}'\}$ e $T_{\mathfrak{P}'} = \{\sigma \in G_{\mathfrak{P}'} | \, \sigma(x) - x \in \mathfrak{P}', \, \forall x \in I_{KL}\}$.
Pelo teorema 2.28 temos que $G(KL/\mathbb{Q}) \cong G(K/\mathbb{Q}) \times_{G(L\cap K/\mathbb{Q})} G(L/\mathbb{Q})$ mediante a aplicacão
$\rho \mapsto (\rho_{\big|_K}, \rho_{\big|_L})$.

$$\begin{array}{ccc} \mathfrak{P}' & I_{KL} & KL \\ | & | & | \\ \mathfrak{P} & I_K & K \\ | & | & | \\ p & \mathbb{Z} & \mathbb{Q} \end{array}$$

Agora para $\rho \in \mathfrak{P}'$ e $x \in I_{K'}$ temos que $\rho_{\big|_K}(x) - x = \rho(x) - x \in \mathfrak{P}' \cap I_K = \mathfrak{P}$, portanto $\rho_{\big|_K} \in T_{\mathfrak{P}}$, assim $T_{\mathfrak{P}'} \subset T_{\mathfrak{P}} \times G(L/\mathbb{Q})$, agora $|T_{\mathfrak{P}'}| = e(\mathfrak{P}'|p) = e(\mathfrak{P}'|\mathfrak{P})e(\mathfrak{P}|p) \geq e(\mathfrak{P}|p) = |T_{\mathfrak{P}}| = \lambda^u$, por outro lado $[KL : \mathbb{Q}] = \lambda^{m+v}$ e $p \neq \lambda$, concluímos que os grupos de ramificação $V_i(\mathfrak{P}')$ são triviais e portanto $T_{\mathfrak{P}'}$ é cíclico, mas $|T_{\mathfrak{P}}| = |G(L/\mathbb{Q})| = \lambda^u$, assim temos que nenhum elemento de $T_{\mathfrak{P}} \times G(L/\mathbb{Q})$ tem ordem maior que λ^u, portanto $|T_{\mathfrak{P}'}| = \lambda^u$
Seja agora K' o corpo fixo de $T_{\mathfrak{P}'}$ e $\mathfrak{P}'' = \mathfrak{P}' \cap I_{K'}$, então $\mathfrak{P}''$ é um ideal primo de $I_{K'}$, logo, como consequencia dos corolarios 2.15 e 2.17, temos que $e(\mathfrak{P}''|p) = 1$, assim p não ramifica em K'

$$\begin{array}{ccc} \mathfrak{P}' & I_{KL} & KL \\ | & | & | \\ \mathfrak{P}'' & I_{K'} & K' \\ | & | & | \\ p & \mathbb{Z} & \mathbb{Q} \end{array}$$

Consideremos agora $\mathfrak{P}'' \cap I_{K'\cap L}$ ideal primo não nulo de $K' \cap L$ acima de p, como p é totalmente ramificado em L temos que p é totalmente ramificado em $K' \cap L$, portanto $e(\mathfrak{P}'' \cap I_{K'\cap L}|p) = [K' \cap L : \mathbb{Q}]$, mas

$1 = e(\mathfrak{P}''|p) = e(\mathfrak{P}''|\mathfrak{P}'' \cap I_{K'\cap L})e(\mathfrak{P}'' \cap I_{K'\cap L}|p)$, assim $1 = [K' \cap L : \mathbb{Q}]$, portanto $K' \cap L = \mathbb{Q}$.
Sabemos que $[KL\colon \mathbb{Q}] = [KL\colon K'][K'\colon \mathbb{Q}]$, mas como K' é o corpo fixo de $T_{\mathfrak{P}'}$, temos que $[KL\colon K'] = |G(KL/K')| = |T_{\mathfrak{P}'}| = \lambda^u = [L\colon \mathbb{Q}]$, assim $[KL\colon \mathbb{Q}] = [L\colon \mathbb{Q}][K'\colon \mathbb{Q}]$.
Por outro lado, $[K'L\colon \mathbb{Q}] = [K'L\colon L][L\colon \mathbb{Q}]$ e como $G(K'L/L) \cong G(K'/K' \cap L) = G(K'/\mathbb{Q})$, temos que $[K'L\colon L] = [K'\colon \mathbb{Q}]$, assim $[K'L\colon \mathbb{Q}] = [KL\colon \mathbb{Q}]$, conseqüentemente $K'L = KL$, assim para provar que K é ciclotômica é suficiente provar que K' é ciclotômica.
Já sabemos que p não ramifica em K', além disso se q é um primo tal que $q \notin \{p_1, \cdots, p_n\}$, então q não ramifica em K', caso contrario q ramificaria em KL e para $\mathfrak{Q}$ primo de I_{KL} acima de q temos que $T_{\mathfrak{Q}|KL} < T_{\mathfrak{Q}|K} \times T_{\mathfrak{Q}|L}$, mas $q \neq p$, então q não ramifica em L além disso q não ramifica em K, portanto $T_{\mathfrak{Q}|K}$ e $T_{\mathfrak{Q}|L}$ são triviais logo $T_{\mathfrak{Q}|K} \times T_{\mathfrak{Q}|L}$ é trivial, conseqüentemente $e(\mathfrak{Q}\,|\,q) = |T_{\mathfrak{Q}|KL}| = 1$, assim q não ramifica em KL o que é uma contradição .
Assim, repetindo este proceso, eliminaremos finalmente os (finitos) primos $p \neq \lambda$ que ramificam em K. ■

Usando os dos últimos lemas, temos que para provar o teorema de Kronecker-Weber só precisamos considerar extenções cíclicas de $\mathbb{Q}$ de grau λ^m, sendo λ o único primo que ramifica.
Separaremos em dois casos, λ ímpar e $\lambda = 2$. Para o caso λ ímpar estudaremos primeiramente o conceito de Valorização .

Definição 4.1 *Seja D um domínio de Dedekind com um unico ideal primo $\mathfrak{R}$, então D é um DIP e se $\mathfrak{R} = (\pi)$ temos que para $\alpha \in D^*$ existe un unico $k \in \mathbb{N}$ tal que $\alpha = \pi^k u$, sendo u uma unidade em D, assim temos uma função $v\colon D^* \longrightarrow \mathbb{N}$, dada por $v(\alpha) = k$, v é chamada a valorização associada a $\mathfrak{R}$.*

Sejam $\alpha, \beta \in D^*$, temos:

1. Se $(\alpha) \subset (\beta)$, então $v(\alpha) \geq v(\beta)$.
2. $v(\alpha + \beta) \geq \min\{v(\alpha), v(\beta)\}$ e a igualdade se verifica quando $v(\alpha) \neq v(\beta)$.
3. $v(\alpha\beta) = v(\alpha) + v(\beta)$.

Lema 4.13 *Seja K uma extenção abeliana de $\mathbb{Q}$ de grau λ^m, sendo λ um primo ímpar o unico que ramifica, então $K/\mathbb{Q}$ é cíclica.*

Demonstração:

$$\begin{array}{ccc} \mathfrak{P} & I_K & K \\ | & | & | \\ \lambda & \mathbb{Z} & \mathbb{Q} \end{array}$$

Sejam $\mathfrak{P}$ ideal primo de I_K que está acima de λ e K^T o corpo fixo de $T_{\mathfrak{P}}$. Então λ não ramifica em K^T, e como por hipótese nenhum outro primo ramifica em K^T, temos pelo teorema de Minkowsky (Teorema 3.34) que $K^T = \mathbb{Q}$, logo
$T_{\mathfrak{P}} = G(K/\mathbb{Q})$, portanto λ é totalmente ramificado em K, assim $f(\mathfrak{P} \mid \lambda) = 1$, logo $\dfrac{I_K}{\mathfrak{P}}$ é um corpo com λ elementos.
Sabemos pelo teorema 3.36, que $\left|\dfrac{T_{\mathfrak{P}}}{V_1}\right|$ divide $\lambda - 1$, mas $T_{\mathfrak{P}}$ tem ordem λ^m, logo $\left|\dfrac{T_{\mathfrak{P}}}{V_1}\right| = \lambda^{m'}$, para $0 \leq m' \leq m$, assim $\lambda^{m'}$ divide $\lambda - 1$ o que acontece só quando $m' = 0$, assim temos que $T_{\mathfrak{P}} = V_1$, por outro lado $\dfrac{V_j}{V_{j+1}} \cong <\left(\dfrac{I_K}{\mathfrak{P}}, +\right)$, portanto $\dfrac{V_j}{V_{j+1}}$ é trivial ou é cíclico de ordem λ.

Sublema: *Se $m = 1$, isto é $[K : \mathbb{Q}] = \lambda$, então V_2 é trivial.*

Demonstração: Localizando respecto a λ podemos supor que I_K é um DIP. Consideremos π um gerador do ideal $\mathfrak{P}$ e $P_{\alpha|\mathbb{Q}}(X)$ o polinômio minimal de π sobre $\mathbb{Q}$, então $P_{\alpha|\mathbb{Q}}(X) \in \mathbb{Z}[X]$, sejam v a valuação associada a $\mathfrak{P}$ e j o menor inteiro positivo tal que V_{j+1} é trivial, vamos provar que $j = 1$.
Como V_j não é trivial temos que $|V_j| = \left|\dfrac{V_j}{V_{j+1}}\right| = \lambda = |G(K/\mathbb{Q})|$, assim
$V_j = G(K/\mathbb{Q})$, afirmamos que:

$$v(P'_{\alpha|\mathbb{Q}}(\pi)) = (j+1)(\lambda - 1)$$

De fato, temos que $P_{\alpha|\mathbb{Q}}(X) = X^\lambda + a_{\lambda-1}X^{\lambda-1} + \cdots + a_1X + a_0 = \prod_{i=1}^{n}(X - \sigma(\pi))$,

então $P'_{\alpha|\mathbb{Q}}(X) = \sum_{i=1}^{\lambda} \prod_{j\neq i}(X - \sigma_i(\pi))$, assim:

$$P'_{\alpha|\mathbb{Q}}(\pi) = \prod_{\substack{\sigma\in G(K/\mathbb{Q}) \\ \sigma\neq i_d}} (\pi - \sigma(\pi)) = \prod_{\sigma\in V_j - V_{j+1}} (\pi - \sigma(\pi))$$

Para $\sigma \in V_j$, temos que $\pi - \sigma(\pi) \in \mathfrak{P}^{j+1}$, portanto $v(\pi - \sigma(\pi)) = j+1$ e assim $v(P'_{\alpha|\mathbb{Q}}(\pi)) = (j+1)(\lambda-1)$.
Por outro lado $P'_{\alpha|\mathbb{Q}}(\pi) = \lambda\pi^{\lambda-1} + (\lambda-1)a_{\lambda-1}\pi^{\lambda-2} + \cdots + 2a_2\pi + a_1$, como λ é totalmente ramificado em K temos que $v(\lambda) = \lambda$ e sabemos que cada $a_i \in \mathbb{Z}$, assim temos que existe $m_i \in \mathbb{N}$ tal que $(a_i) \subset (\lambda^{m_i})$, portanto:

$$v(a_i) \equiv 0\,(mod\,\lambda)$$

E para $k \in \{0, \cdots, \lambda-1\}$ temos que:

$$v(a_{\lambda-k}(\lambda-k)\pi^{\lambda-(k+1)}) = v(a_{\lambda-k}) + v(\lambda-k) + v(\pi^{\lambda-(k+1)}) \equiv \lambda - (k+1)\,(mod\,\lambda\,)$$

Assim todos esses termos tem valorizações distintas, e, consequentemente:

$$v(P'_{\alpha|\mathbb{Q}}(\pi)) = \min\{v(\lambda\pi^{\lambda-1}), v((\lambda-1)a_{\lambda-1}\pi^{\lambda-2}), \cdots, v(2a_2\pi), v(a_1)\} \leq v(\lambda\pi^{\lambda-1}) = 2\lambda-1,$$

isto é:

$$v(P'_{\alpha|\mathbb{Q}}(\pi)) \leq 2\lambda - 1$$

Portanto, $2\lambda - 1 \geq (j+1)(\lambda-1)$, como λ é primo ímpar temos que o único inteiro $j \geq 1$ que satisfaz essa desigualdade é $j = 1$, portanto V_2 é trivial. ■

Voltando no caso $m > 1$, provaremos que $K/\mathbb{Q}$ é cíclica mostrando que V_2 é o único subgrupo de $G(K/\mathbb{Q}) = V_1$ de indice λ. Veja [10] pag. 176.
Seja H um subgrupo de V_1 de indice λ e K' seu corpo fixo, então :
$G' = G(K'/\mathbb{Q}) \cong \dfrac{G(K/\mathbb{Q})}{G(K/K')} = \dfrac{G(K/\mathbb{Q})}{H}$, assim :

$$G' \cong \frac{G(K/\mathbb{Q})}{H}$$

Agora, se $V'_j = V_j \cap G'$,e o j-esimo grupo de ramificação de K', então a aplicação $Res\colon G(K/\mathbb{Q}) \longrightarrow G(K'/\mathbb{Q})$, dada por $Res(\sigma) = \sigma_{\big|_{K'}}$, para todo $\sigma \in G(K/\mathbb{Q})$ é tal que $Res(\sigma) \in V'_j$ para todo $\sigma \in V_j$, como $[K' : \mathbb{Q}] = \lambda$. Pelo sublema temos que V'_2 é trivial, portanto $Res(V_2)$ é trivial, então para $\sigma \in V_2$ e $x \in K'$, temos $\sigma_{\big|_{K'}}(x) = \sigma(x) = x$, portanto σ fixa K', e assim $V_2 \subset H$.
Seja m o menor inteiro positivo talque V_m não é todo $G(K/\mathbb{Q})$. Temos que $m \geq 2$ e que $\dfrac{V_{m-1}}{V_m} = \dfrac{G}{V_m}$ tem ordem λ, logo aplicando o raciocínio anterior ao caso particular $H = V_m$, temos $V_m \supset V_2$, logo $V_2 = V_m$, portanto V_2 tem indice λ e $V_2 = H$. ■

Lema 4.14 *O teorema de Kronecker-Weber se verifica para extensões abelianas de $\mathbb{Q}$ de grau λ^m, sendo λ um primo ímpar.*

Demonstração: Pelo lema 4.12 y o teorema de Minkowsky podemos supor que λ é o único primo que ramifica em K, agora se ζ é uma raíz primitiva λ^{m+1}-ésima da unidade, então $\mathbb{Q}(\zeta)/\mathbb{Q}$ é cíclico de ordem $\phi(\lambda^{m+1}) = \lambda^m(\lambda - 1)$, portanto existe um unico subcorpo K' de $\mathbb{Q}(\zeta)$ tal que $K'/\mathbb{Q}$ tem grau λ^m e λ é o unico primo que ramifica em K'. Vamos provar que $K = K'$.
Suponhamos que $K \neq K'$, dado $\mathfrak{P}$ ideal primo de KK' temos que
$T_{\mathfrak{P}|KK'} < T_{\mathfrak{P}|K} \times T_{\mathfrak{P}|K'}$, segue-se que λ é o único primo que ramifica em KK', como $K/\mathbb{Q}$ e $K'/\mathbb{Q}$ são abelianas temos que $KK'/\mathbb{Q}$ é abeliana.
Por outro lado $[KK' : K'] = |G(KK'/K')| = |G(K/K \cap K')| = [K\colon K \cap K']$ que divide λ^m, assim $[KK'\colon K'] = \lambda^u$, com $0 \leq u \leq m$, no caso $u = 0$, teriamos $K \subset K'$ o que implica K é ciclotômica, logo podemos supor $1 \leq u \leq m$, portanto
$[KK'\colon \mathbb{Q}] = \lambda^{m+u} > \lambda^m$, assim pelo lema anterior $KK'/\mathbb{Q}$ é cíclico, mas
$G(KK'/\mathbb{Q}) < G(K/\mathbb{Q}) \times G(K'/\mathbb{Q})$, logo nenhum elemento de $G(KK'/\mathbb{Q})$ tem ordem maior que λ^m o que é uma contradição , desse modo $K = K'$. ■

Corolário 4.15 *Se $K/\mathbb{Q}$ é abeliana de grau λ^m sendo λ primo ímpar o único que ramifica em K e ζ é uma raíz primitiva λ^{m+1}-ésima da unidade, então K é o unico subcorpo de $\mathbb{Q}(\zeta)$ que tem grau λ^m sobre $\mathbb{Q}$.*

Temos que o teorema de Kronecker-Weber fica reduzido ao caso de extensões cíclicas de grau 2^m, com m um inteiro positivo.

Lema 4.16 *Toda extensão quadrática de $\mathbb{Q}$ é ciclotômica.*

Demonstração: Seja K uma extensão quadrática de $\mathbb{Q}$, então existe $m \in \mathbb{Z}$, livre de quadrados tal que $K = \mathbb{Q}(\sqrt{m})$, existem $p_1, \cdots, p_k$ primos distintos tais que $m = \pm p_1 \cdots p_k$, assim $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{\pm p_1 \cdots p_k}) \subset \mathbb{Q}(\sqrt{\pm p_1}) \cdots \mathbb{Q}(\sqrt{\pm p_k})$, logo só precisamos considerar o caso $K = \mathbb{Q}(\sqrt{\pm p})$, onde p é um número primo.
Se $p = 2$, seja ζ uma raíz primitiva 8-ésima da unidade, vamos provar que $\mathbb{Q}(\sqrt{\pm 2}) \subset \mathbb{Q}(\zeta)$.
De fato como $i^8 = 1$, temos que $i \in \mathbb{Q}(\zeta)$, também $\dfrac{\sqrt{2}}{2} + i\dfrac{\sqrt{2}}{2} \in \mathbb{Q}(\zeta)$ pois $\left(\dfrac{\sqrt{2}}{2} + i\dfrac{\sqrt{2}}{2}\right)^8 = i^4 = 1$, assim $\dfrac{1+i}{\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}} \in \mathbb{Q}(\zeta)$ e como $\left(\dfrac{1+i}{\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}}\right)^2 = 2$,
$\sqrt{2} \in \mathbb{Q}(\zeta)$, finalmente $\sqrt{-2} = i\sqrt{2} \in \mathbb{Q}(\zeta)$, portanto $\mathbb{Q}(\sqrt{\pm 2}) \subset \mathbb{Q}(\zeta)$.

Suponhamos agora que p é um primo ímpar. Consideremos ζ uma raíz primitiva p-ésima da unidade e $F(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$ o p-esimo polinômio ciclotômico, seu discriminante é $\triangle = \prod_{1\leq i,j\leq p-1} (\zeta^i - \zeta^j)^2$, que é um quadrado em $\mathbb{Q}(\zeta)$, da proposição 3.2 e do teorema 4.8, temos que $\triangle = d_{L|\mathbb{Q}}(1, \zeta, \cdots, \zeta^{p-1}) = \pm p^{p-2}$, portanto $\pm p^{p-2} = \triangle$, conseqüentemente:

$$\pm p = \frac{\triangle}{p^{p-3}}$$

Agora como $p-3$ é par, temos que p^{p-3} é um quadrado em $\mathbb{Q}(\zeta)$, portanto $\sqrt{\pm p} = i\sqrt{\frac{\triangle}{p^{p-3}}} \in \mathbb{Q}(\zeta, i)$, agora se ξ é uma raíz primitiva $4p$-ésima da unidade, assim temos que $\mathbb{Q}(\zeta, i) \subset \mathbb{Q}(\xi)$, já que $\zeta^{4p} = i^{4p} = 1$, portanto $\mathbb{Q}(\sqrt{\pm p}) \subset \mathbb{Q}(\xi)$, conseqüentemente $\mathbb{Q}(\sqrt{\pm p})$ é ciclotômica. ■

Lema 4.17 *Toda extensão cíclica K de $\mathbb{Q}$ de grau 2^m, sendo m um inteiro positivo, é ciclotômica.*

Antes de começar a prova do lema provaremos o seguinte resultado:

Sublema: *Se $K \subset \mathbb{R}$ é um corpo quadrático tal que 2 é o único primo que ramifica em K, então $K = \mathbb{Q}(\sqrt{2})$.*

Demonstração: Sabemos que existe $d \in \mathbb{Z}^+$ livre de quadrados tal que $K = \mathbb{Q}(\sqrt{d})$, por outro lado $I_K = \mathbb{Z}[\delta] = \mathbb{Z} + \delta\mathbb{Z}$, onde

$$\delta = \begin{cases} \sqrt{d}, \text{se } d \equiv 2 \text{ ou } 3 \ (mod\ 4) \\ \dfrac{1+\sqrt{d}}{2}, \text{se } d \equiv 1 \ (mod\ 4) \end{cases}$$

E para $p \in \mathbb{Z}$ primo temos que p ramifica em K se, e somente se, $p \mid d_K$.
Se $\delta = \sqrt{d}$, $P_\delta(X) = X^2 - d = (X + \sqrt{d})(X - \sqrt{d})$, assim

$$d_L = (2\delta)^2 = 4\delta^2$$

Se $\delta = \dfrac{1+\sqrt{d}}{2}$, então $P_\delta(X) = X^2 - X - \dfrac{d-1}{4} = \left(X - \dfrac{1+\sqrt{d}}{2}\right)\left(X - \dfrac{1-\sqrt{d}}{2}\right)$, portanto:

$$d_L = \left(\frac{1+\sqrt{d}}{2} - \frac{1-\sqrt{d}}{2}\right)^2 = d$$

Como 2 ramifica em K, temos que $2 \mid d_K$, logo se $d \equiv 1\,(mod\,4)$, temos que d é ímpar e $2 \mid d$, absurdo. Portanto $d \equiv 2$ ou $3\,(mod\,4)$, assim temos que 2 é o unico primo que divide $4d$, logo 2 é o unico primo que divide d, consequentemente $d = 2^n$, para algum n inteiro positivo e como d é livre de quadrados temos que $n = 1$. ■

Vamos em seguida começar a demonstração do lema fazendo indução sobre m.
Se $m = 1$, temos que K é quadrática e, portanto, ciclotômica.
Agora, para $m > 1$, podemos supor que 2 é o único primo que ramifica em K e que K está imerso em $\mathbb{C}$, se $\sigma \in Aut\,\mathbb{C}$ é a conjugação , então a restrição de σ a K é a identidade (no caso $K \subset \mathbb{R}$) ou um automorfismo de ordem 2.
Agora se E é o corpo fixo de σ restrito a K, temos que $[E\colon \mathbb{Q}] = \dfrac{|G(K/\mathbb{Q})|}{|G(K/E)|} \geq 2^{m-1}$, como $K/\mathbb{Q}$ é cíclica, existe um único K' subcorpo de E tal que $[K'\colon \mathbb{Q}] = 2$ e 2 é o único primo que ramifica em K', portanto $K' = \mathbb{Q}(\sqrt{2}\,)$.
Consideremos agora ζ uma raíz primitiva $4n$-ésima da unidade, onde $n = 2^m$ e $L = \mathbb{Q}(\zeta + \zeta^{-1})$, temos que $L \subset \mathbb{R}$, portanto $[\mathbb{Q}(\zeta) : L] \geq 2$ e como
$F(X) = X^2 - (\zeta + \zeta^{-1})X + 1 \in L[X]$ anula ζ, temos que $[\mathbb{Q}(\zeta) : L] = 2$.
Pela proposição 4.3 sabemos que $G(\mathbb{Q}(\zeta)/\mathbb{Q}) = c(2) \times c(2^m) \cong G(\mathbb{Q}(\zeta)/L) \times c(2^m)$, portanto:

$$G(L/\mathbb{Q}) \cong \frac{G(\mathbb{Q}(\zeta)/\mathbb{Q})}{G(\mathbb{Q}(\zeta)/L)} \cong c(2^m)$$

Assim $L/\mathbb{Q}$ é cíclica de ordem $n = 2^m$ e 2 é o único primo que ramifica em L, portanto o único subcorpo quadrático de L é $\mathbb{Q}(\sqrt{2}\,)$, logo $L \cap K \supset \mathbb{Q}(\sqrt{2}\,)$ e assim $[L \cap K : \mathbb{Q}] \geq 2$.
Conseqüentemente, $[KL\colon \mathbb{Q}] = [KL\colon L][L\colon \mathbb{Q}] = [K\colon K \cap L][L\colon \mathbb{Q}] = 2^r 2^m = 2^{r+m}$, para algum $r \in \mathbb{Z}$, tal que $0 \leq r < m$, em particular $[KL\colon \mathbb{Q}] < n^2$.
Agora se $\Gamma = G(KL/\mathbb{Q})$, temos que $\Gamma \cong G \times_S H$, onde $S = G(L \cap K/\mathbb{Q})$,
$H = G(L/\mathbb{Q})$ e $G = G(K/\mathbb{Q})$.
Vamos provar que existem geradores σ e τ de G e H respectivamente, tais que $\sigma|_{L\cap K} = \tau|_{L\cap K}$.
De fato, como σ gera G, temos que $\sigma|_{L\cap K}$ gera S e como $L/L \cap K$ é de Galois existe $\tau \in H$, tal que $\tau|_{L\cap K} = \sigma|_{L\cap K}$, vamos provar que τ gera H.
Se μ gera H, existe $d \in \mathbb{Z}$ tal que $\tau = \mu^d$, logo $\sigma|_{L\cap K} = \tau|_{L\cap K} = \mu^d|_{L\cap K}$, portanto

$\mu^d|_{L\cap K}$ gera S, sabemos que $|S| = 2^{n'}$, $n' \leq n$, então $(d, 2^{n'}) = 1$, logo $(d, 2) = 1$, assim $(d, |H|) = (d, 2^n) = 1$, logo $\tau = \mu^d$ gera H e também $(\sigma, \tau) \in \Gamma$.
Voltando ao lema, consideremos Δ o subgrupo de Γ de ordem $n = 2^m$ gerado por (σ, τ) e F o corpo fixo de Δ, então F é um subcorpo de KL e portanto 2 é o único primo que ramifica em F, além disso:

$$[F : \mathbb{Q}] = \frac{|G(KL/\mathbb{Q})|}{|G(KL/F)|} = \frac{2^{r+m}}{2^m} = 2^r$$

Vamos provar agora que $F/\mathbb{Q}$ é cíclica.
Sabemos que:

$$G(F/\mathbb{Q}) \cong \frac{G(KL/\mathbb{Q})}{\Delta} \hookrightarrow \frac{< \sigma > \times < \tau >}{\Delta}$$

Então , será suficiente provar que $\dfrac{< \sigma > \times < \tau >}{\Delta}$ é um grupo cíclico; mas dado $(\sigma^a, \tau^b) \in < \sigma > \times < \tau >$, temos que $(\sigma^a, \tau^b)(\sigma^p, id_l) \in \Delta$ se, e somente se, $p + a = b$, isto é $p = b - a$, assim:

$$(\sigma, id_l)\Delta \text{ gera } \frac{< \sigma > \times < \tau >}{\Delta}.$$

Logo, pela hipótese de indução , F é ciclotômico e como $F \subset KL$ temos que $FL \subset KL$, vamos provar agora que $FL = KL$.
Para isso, consideremos a aplicação $Res: \Delta \subset G(KL/\mathbb{Q}) \longrightarrow G(L/\mathbb{Q})$, tal que $Res(\sigma^m, \tau^m) = \tau^m|_L$, então se $\tau^m|_L$ é a identidade temos que, $o(\tau) = o(\sigma)|\, m$ (onde $o(x)$ é a ordem do x), portanto $(\sigma^m, \tau^m) = (id_K, id_L)$, assim Res é injetora, mas $|\Delta| = n = |G(L/\mathbb{Q})|$, logo Res é isomorfismo.
Assim, dado $x \in F \cap L$ e $\tau_1 \in G(L/\mathbb{Q})$, existe $(\sigma_2, \tau_2) \in \Delta$ tal que $\tau_2|_L = \tau_1$, logo $\tau_1(x) = \tau_2(x) = x$, portanto τ_1 fixa $F \cap L$, conseqüentemente $F \cap L = \mathbb{Q}$ e obtemos que $G(FL/F) \cong G(L/L \cap F) = G(L/\mathbb{Q})$, logo $[FL : F] = n = [KL : F]$, assim $FL = KL$ o que implica que K é ciclotômica. ■

Bibliografia

[1] M. J Greenberg, An elementary proof of the Kronecker-Weber Theorem, American Mathematical Monthly, Vol. 81, No. 6 (Jun. - Jul., 1974), pp. 601-607.

[2] O. Endler, teoria dos números algébricos, Segunda edição , Projeto euclides, Rio de Janeiro, IMPA, 2006.

[3] S. Lang, Algebraic Number Theory, Second Edition, Springer-Verlag, New-York, 1970.

[4] I.Stewart and W.Tall, Algebraic Number Theory and Fermat's Last Theorem, Third Edition, AK-Peters, Naticks-Massachusets, 2002.

[5] O. Zariski and P.Samuel, Commutative Algebra, Vol I, Spriger-Verlag, New-York, 1979.

[6] L. Goldstein, Analytic Number Theory, Prentice-Hall,New Jersey, 1971.

[7] P. Martin, Introdução á Teoria dos Grupos e á Teoria de Galois, Publicações IME-USP.

[8] E. Weiss, Algebraic Number Theory, McGraw-Hill, New York, 1963.

[9] W. Narkiewics, Elementary and Analytic theory of algebraic numbers, PWN-Polish Scientific Publishers, 1974.

[10] M.Hall, Jr.,The Theory of Groups, Macmillan, New York,1959.