2 - Corpos quadráticos e ciclotômicos

Carina Alves
Antonio Aparecido de Andrade

ALVES, C., and ANDRADE, AA. Corpos quadráticos e ciclotômicos. In: *Reticulados via corpos ciclotômicos* [online]. São Paulo: Editora UNESP, 2014, pp. 70-105. ISBN 978-85-68334-39-3. Available from SciELO Books <http://books.scielo.org>.

2

Corpos quadráticos e ciclotômicos

2.1 Introdução

Neste capítulo apresentamos os conceitos de corpos quadráticos e corpos ciclotômicos, dando ênfase especialmente aos corpos ciclotômicos. Para isso usamos os resultados de Teoria Algébrica dos Números vistos no capítulo 1. Concluindo o capítulo apresentamos a decomposição de um ideal primo em uma extensão onde fizemos o uso do Teorema de Kummer.

Temos duas classes importantes dos corpos de números que são a classe dos corpos quadráticos e a classe dos corpos ciclotômicos. Nosso objetivo nas próximas seções é determinar o anel dos inteiros algébricos, base integral e discriminante dos corpos quadráticos e dos corpos ciclotômicos.

2.2 Corpos quadráticos

Nesta seção apresentamos os corpos quadráticos juntamente com a teoria necessária para caracterizar seu anel dos inteiros, base integral e discriminante.

Definição 2.2.1. *Uma extensão de corpos de grau 2 sobre o corpo* $\mathbb{Q}$ *é chamado um* **corpo quadrático**.

Proposição 2.2.1. *(*Ribeiro, 2013, p.13, Prop.2.2.1*) Todo corpo quadrático é da forma* $\mathbb{Q}(\sqrt{d})$, *sendo* d *um inteiro livre de quadrados.*

Demonstração: Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo quadrático, ou seja, um corpo de números de grau 2, e $f(X) = X^2+aX+b$, com $a, b \in \mathbb{Q}$, o polinômio minimal de $\theta \in \mathbb{K}$. Resolvendo a equação quadrática $\theta^2+a\theta+b = 0$ temos que $\theta = \dfrac{-a \pm \sqrt{a^2-4b}}{2}$ são as raízes de $f(X)$. Como $2\theta \pm a = \sqrt{a^2-4b}$ segue que $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{a^2-4b})$. Por outro lado, a^2-4b é um número racional que podemos escrever como $a^2-4b = \dfrac{u}{v} = \dfrac{uv}{v^2}$, com $u, v \in \mathbb{Z}$, $mdc(u, v) = 1$ e de forma que u e v não sejam quadrados perfeitos, pois caso contrário, teremos $\mathbb{Q}(\theta) = \mathbb{Q}$. Assim, $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{a^2-4b}) = \mathbb{Q}\left(\sqrt{\dfrac{u}{v}}\right) = \mathbb{Q}\left(\sqrt{\dfrac{uv}{v^2}}\right) = \mathbb{Q}(\sqrt{uv})$. Suponhamos que $uv = k^2d$, com $k, d \in \mathbb{Z}$, e d livre de quadrados. Logo, $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{uv}) = \mathbb{Q}(\sqrt{k^2d}) = \mathbb{Q}(\sqrt{d})$. ■

A Proposição 2.2.1 nos diz que todo corpo quadrático $\mathbb{K}$ é da forma $\mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados e $\{1, \sqrt{d}\}$ é uma base do espaço vetorial $\mathbb{Q}(\sqrt{d})$ sobre $\mathbb{Q}$.

Proposição 2.2.2. *(*Samuel, 1967, p.35*) Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, *com* d *um inteiro livre de quadrados, um corpo quadrático. Se um*

elemento $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ *é um inteiro algébrico, então* $2a$ *e* $a^2 - db^2$ *são números inteiros.*

Demonstração. Seja $\alpha \in \mathbb{K}$ um inteiro algébrico. Então existem $a_0, \cdots, a_{n-1} \in \mathbb{Z}$ tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Assim, considerando σ um automorfismo de $\mathbb{K}$ tal que $\sigma(\sqrt{d}) = -\sqrt{d}$, segue que, $\sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \cdots + a_1\sigma(\alpha) + a_0 = 0$, ou seja, $\sigma(\alpha)$ também é um inteiro algébrico de $\mathbb{K}$. Do Corolário 1.3.2, temos que $\alpha + \sigma(\alpha)$ e $\alpha\sigma(\alpha)$ também são inteiros algébricos de $\mathbb{K}$. Além disso, temos que se $\alpha = a + b\sqrt{d}$, com $a, b \in \mathbb{Q}$, então $\alpha + \sigma(\alpha) = 2a \in \mathbb{Q}$ e $\alpha\sigma(\alpha) = a^2 - db^2 \in \mathbb{Q}$. Como $\mathbb{Z}$ é integralmente fechado segue, da Proposição 1.3.4, que $2a$ e $a^2 - db^2$ são números inteiros. ■

Observação 2.2.1. *Se* $d > 0$, *a extensão* $\mathbb{Q}(\sqrt{d})$ *é dita real e se* $d < 0$, *a extensão* $\mathbb{Q}(\sqrt{d})$ *é dita imaginária.*

A seguir determinaremos o anel dos inteiros algébricos de um corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com d um inteiro livre de quadrados.

Teorema 2.2.1. *(*Stewart; Tall, 1987, p.67, Teo.3.2*) Se* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ *é um corpo quadrático com* $d \in \mathbb{Z}$ *livre de quadrados, então o anel dos inteiros algébricos* $\mathbb{A}_{\mathbb{K}}$ *de* $\mathbb{Q}(\sqrt{d})$ *é dado por:*

a) $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$ *se* $d \equiv 2$ *ou* $d \equiv 3 (mod\ 4)$ *e*

b) $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ *se* $d \equiv 1 (mod\ 4)$.

Demonstração: Seja $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, com $a, b \in \mathbb{Q}$, um inteiro algébrico sobre $\mathbb{Z}$. Se $b = 0$ então o polinômio minimal de α sobre $\mathbb{Q}$ é dado por $m(X) = X - a$, e como α é um inteiro algébrico sobre $\mathbb{Z}$, segue que $a \in \mathbb{Z}$. Se $b \neq 0$, então o polinômio minimal $m(X)$ de α sobre $\mathbb{Q}$ tem grau 2 e é obtido do seguinte modo:

$$\alpha = a + b\sqrt{d} \Longrightarrow \alpha - a = b\sqrt{d} \Longrightarrow (\alpha - a)^2 = b^2 d \Longrightarrow$$
$$\alpha^2 - 2a\alpha + a^2 = b^2 d \Longrightarrow \alpha^2 - 2a\alpha + (a^2 - b^2 d) = 0.$$

Logo $m(X) = X^2 - 2aX + a^2 - db^2$. Pela Proposição 2.2.2 temos que $2a,\ a^2 - db^2 \in \mathbb{Z}$. Assim, $(2a)^2 - d(2b)^2 \in \mathbb{Z}$ e daí $d(2b)^2 \in \mathbb{Z}$, pois $2a \in \mathbb{Z}$. Ainda temos que $2b \in \mathbb{Z}$, pois, caso contrário, no seu denominador existiria um fator primo p que apareceria na forma p^2 no denominador de $(2b)^2$ e como d é livre de quadrados teríamos que $d(2b)^2 \notin \mathbb{Z}$, o que é um absurdo. Logo, $2b \in \mathbb{Z}$. Assim, podemos escrever:

$$a = \frac{u}{2},\ b = \frac{v}{2},\quad com\, u,\ v \in \mathbb{Z}. \tag{2.1}$$

Além disso, temos que

$$(2a)^2 - d(2b)^2 \in 4\mathbb{Z}. \tag{2.2}$$

Substituindo a por $\frac{u}{2}$ e b por $\frac{v}{2}$, obtemos $u^2 - dv^2 \in 4\mathbb{Z}$.

a) Se $d \equiv 2$ ou $3(mod\ 4)$, temos que u e v são pares, pois se v fosse ímpar teríamos $v^2 \equiv 1(mod\ 4)$. Assim, como $u^2 - dv^2 \in 4\mathbb{Z}$ temos que $u^2 \equiv dv^2 \equiv d(mod\ 4)$, ou seja, $d \equiv 0(mod\ 4)$ ou $d \equiv 1(mod\ 4)$, o que é um absurdo. Portanto, concluímos que v é par, isto é, $v^2 \equiv 0(mod\ 4)$ e assim, $u^2 \equiv dv^2 \equiv 0(mod\ 4)$ o que implica que u é par. Logo, se $\alpha = a + b\sqrt{d} \in \mathbb{A}_{\mathbb{K}}$ temos que $\alpha \in \mathbb{Z}[\sqrt{d}]$ e assim, $\mathbb{A}_{\mathbb{K}} \subset \mathbb{Z}[\sqrt{d}]$. Por outro lado, tomando $\alpha \in \mathbb{Z}[\sqrt{d}]$, temos que α é raiz do polinômio $X^2 - 2aX + a^2 - db^2 \in \mathbb{Z}[X]$, pois pela Proposição 2.2.2, temos que $2a,\ a^2 - db^2 \in \mathbb{Z}$. Logo, $\mathbb{Z}[\sqrt{d}] \subset \mathbb{A}_{\mathbb{K}}$. Portanto, $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$.

b) Se $d \equiv 1(mod\ 4)$, temos que $u^2 - dv^2 \in 4\mathbb{Z}$, e que u e v são de mesma paridade, isto é, são ambos pares ou ímpares. Se u e v são pares então $a,\ b \in \mathbb{Z}$. Logo, $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Se u e v são ímpares, então $\alpha = a + b\sqrt{d} = u/2 + v/2\sqrt{d} = (u -$

$v)/2 + v((1+\sqrt{d})/2) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Portanto, $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, ou seja, $\mathbb{A}_{\mathbb{K}} \subset \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Por outro lado, se $\alpha = a + b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, com $a, b \in \mathbb{Z}$, temos que $2a + b \in \mathbb{Z}$ e $(a + b/2)^2 - d(b/2)^2 = a^2 + ab + (1-d)b^2/4 \in \mathbb{Z}$, pois $d \equiv 1(mod\ 4)$. Logo, $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subset \mathbb{A}_{\mathbb{K}}$, pois os coeficientes do polinômio minimal de α, $m(X) = X^2 - (2a + b)X + a^2 + ab + (1-d)b^2/4$ estão em $\mathbb{Z}$. Portanto, $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathbb{A}_{\mathbb{K}}$. ■

Exemplo 2.2.1. *Seja $\mathbb{K}$ o corpo quadrático $\mathbb{Q}(\sqrt{-1})$. O anel dos inteiros algébricos de $\mathbb{K}$ é dado por $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, onde $i = \sqrt{-1}$ pois $d = -1 \equiv 3(mod\ 4)$. O anel dos inteiros algébricos do corpo quadrático $\mathbb{Q}(\sqrt{-3})$é $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.*

Como os $\mathbb{Q}$-monomorfismos de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com $d \in \mathbb{Z}$ livre de quadrados, em $\mathbb{C}$ são σ_1 e σ_2, onde $\sigma_1(\sqrt{d}) = \sqrt{d}$ e $\sigma_2(\sqrt{d}) = -\sqrt{d}$, segue que o discriminante absoluto de um corpo quadrático é obtido do seguinte modo:

i) se $d \equiv 1(mod\ 4)$, então

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

ii) se $d \equiv 2$ ou $3(mod\ 4)$ então

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

Exemplo 2.2.2. *Dado* $\mathbb{K} = \mathbb{Q}(\sqrt{5})$, *tem-se* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, *isto é,* $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ *é uma base integral de* $\mathbb{A}_{\mathbb{K}}$ *e o discriminante absoluto de* $\mathbb{K}$ *é* 5. *Os monomorfismos de* $\mathbb{K}$ *em* $\mathbb{C}$ *são* σ_1 *a inclusão e* σ_2 *a conjugação complexa, isto é,* $\sigma_1(a+b\sqrt{5}) = a+b\sqrt{5}$ *e* $\sigma_2(a+b\sqrt{5}) = a-b\sqrt{5}$. *Logo,* $Tr_{\mathbb{K}/\mathbb{Q}}(a+b\sqrt{5}) = \sum_{i=1}^{2}\sigma_i(a+b\sqrt{5}) = 2a$ *e* $N_{\mathbb{K}/\mathbb{Q}}(a+b\sqrt{5}) = \prod_{i=1}^{2}\sigma_i(a+b\sqrt{5}) = a^2+b^2$.

Exemplo 2.2.3. *Dado* $\mathbb{K} = \mathbb{Q}(i)$ *então* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\sqrt{-1}]$, *isto é,* $\{1, \sqrt{-1}\}$ *é uma base integral para* $\mathbb{A}_{\mathbb{K}}$ *e o discriminante absoluto de* $\mathbb{K}$ *é* -4. *Os monomorfismos de* $\mathbb{K}$ *em* $\mathbb{C}$ *são* σ_1 *a inclusão e* σ_2 *a conjugação complexa, isto é,* $\sigma_1(a+b\sqrt{-1}) = a+b\sqrt{-1}$ *e* $\sigma_2(a+b\sqrt{-1}) = a-b\sqrt{-1}$. *Logo,* $Tr_{\mathbb{K}/\mathbb{Q}}(a+b\sqrt{-1}) = \sum_{i=1}^{2}\sigma_i(a+b\sqrt{-1}) = 2a$ *e* $N_{\mathbb{K}/\mathbb{Q}}(a+b\sqrt{-1}) = \prod_{i=1}^{2}\sigma_i(a+b\sqrt{-1}) = a^2+b^2$

2.3 Corpos ciclotômicos

Nesta seção apresentamos os corpos ciclotômicos. Esses corpos desempenham um papel fundamental na Teoria Algébrica dos Números, uma vez que é possível caracterizar o anel dos intei-

ros algébricos de um corpo ciclotômico e, consequentemente, seu discriminante.

Definição 2.3.1. *Seja $\mathbb{K}$ um corpo. Um elemento $\zeta \in \mathbb{K}$ é chamado uma raiz n-ésima da unidade se $\zeta^n = 1$, para $n \geq 1$, um inteiro.*

Segue da Definição 2.3.1 que as raízes n-ésimas da unidade são raízes do polinômio $x^n - 1$. Seja $U = \{\zeta^{r_1}, \cdots, \zeta^{r_n}\}$ o conjunto de todas as raízes distintas de $X^n - 1$ em $\mathbb{K}$. Como $(\zeta^i\zeta^j)^n = (\zeta^i)^n(\zeta^j)^n = (\zeta^n)^i(\zeta^n)^j = 1$ e $\left(\frac{\zeta^i}{\zeta^j}\right)^n = \frac{(\zeta^i)^n}{(\zeta^j)^n} = \frac{(\zeta^n)^i}{(\zeta^n)^j} = 1$, segue que o conjunto U é um grupo multiplicativo. Como todo grupo multiplicativo finito num corpo é cíclico então segue que U é um grupo cíclico. Assim, podemos representar as n raízes n-ésimas da unidade por $\zeta, \zeta^2, \cdots, \zeta^n = 1$, onde ζ é um gerador do grupo U. As raízes n-ésimas primitivas da unidade são os geradores do grupo U, isto é, os elementos ζ^k com $mdc(k, n) = 1$, para $k = 1, 2, \cdots, n$. O número das raízes n-ésimas primitivas da unidade é dado por

$$\phi(n) = \#\{0 < m < n : mdc(m, n) = 1, m \in \mathbb{Z}\},$$

onde ϕ é a função de Euler. Dado n um inteiro positivo, definimos ζ_n como sendo $e^{\frac{2\pi i}{n}}$ e o corpo $\mathbb{Q}(\zeta_n)$ é chamado o $n-$ésimo corpo ciclotômico.

Definição 2.3.2. *O polinômio $\varphi_n(X) = \prod_{j=1,\, mdc(j,n)=1}^{n} (X - \zeta_n^j)$ é chamado de $n-$ésimo polinômio ciclotômico.*

Lema 2.3.1. *(*Lang, 1972, p.206*) Se n é um inteiro positivo, então $X^n - 1 = \prod_{d|n} \varphi_d(X)$.*

Demonstração: Sendo $f(X) = X^n - 1$, temos que as raízes de $f(X)$ são $1, \omega, \omega^2, \cdots, \omega^{n-1}$. Logo $X^n - 1 = (X - 1)(X - \omega)\cdots(X - \omega^{n-1})$.

Analisando os períodos de cada raiz de f(X), e escrevendo todas as raízes de mesmo período como um polinômio da forma $\varphi_d(X) = \prod_{periodo\ \omega=d} (X-\omega)$, segue que $X^n - 1 = \prod_{d|n} \varphi_d(X)$. ■

Exemplo 2.3.1. *Considere o polinômio* $f(X) = X^6 - 1$. *Temos que as raízes de* $f(X)$ *são* ω, ω^2, ω^3, ω^4, ω^5, ω^6. *Deste modo,* ω, ω^2, ω^3, ω^4, *e* ω^5 *tem período* 6, 3, 2, 3 *e* 6, *respectivamente. Assim,* $\varphi_1(X) = (X-\omega^6) = (X-1)$, $\varphi_2(X) = (X-\omega^3)$, $\varphi_3(X) = (X-\omega^2)(X-\omega^4)$, $\varphi_6(X) = (X-\omega)(X-\omega^5)$. *Como os divisores de 6 são 1, 2, 3, 6, temos que* $X^6-1 = \prod_{d|6} \varphi_d(X)$, *ou seja,* $X^6-1 = \varphi_1(X)\varphi_2(X)\varphi_3(X)\varphi_6(X) = (X-1)(X-\omega^3)(X-\omega^2)(X-\omega^4)(X-\omega)(X-\omega^5)$.

Como consequência do Lema 2.3.1 temos que

$$\varphi_n(X) = \frac{X^n - 1}{\prod_{d|n,\, d<n} \varphi_d(X)}. \tag{2.3}$$

Assim $\varphi_1(X) = X-1$, $\varphi_2(X) = \dfrac{X^2-1}{\varphi_1(X)} = \dfrac{X^2-1}{X-1} = X+1$, $\varphi_3(X) = \dfrac{X^3-1}{\varphi_1(X)} = \dfrac{X^3-1}{X-1} = X^2+X+1$, $\varphi_4(X) = \dfrac{X^4-1}{\varphi_1(X)\varphi_2(X)} = \dfrac{(X^2-1)(X^2+1)}{(X-1)(X+1)} = X^2+1$. Quando $n = p$, onde p é um número primo, segue que

$$\varphi_p(X) = \frac{X^p-1}{\varphi_1(X)} = \frac{X^p-1}{X-1} = X^{p-1} + \cdots + X + 1. \tag{2.4}$$

que é chamado de **p-ésimo polinômio ciclotômico**. Quando $n = p^r$, onde r é um número inteiro maior que 1 e p é um número primo, de acordo com o Lema 2.3.1,

$$X^{p^r} - 1 = \varphi_1(X)\varphi_p(X)\varphi_{p^2}(X)\cdots\varphi_{p^{r-1}}(X)\varphi_{p^r}(X) \ \ e$$
$$X^{p^{r-1}} - 1 = \varphi_1(X)\varphi_p(X)\varphi_{p^2}(X)\cdots\varphi_{p^{r-1}}(X).$$

Logo $\varphi_{p^r}(X) = \dfrac{X^{p^r}-1}{X^{p^{r-1}}-1} = X^{(p-1)p^{r-1}} + X^{(p-2)p^{r-1}} + \cdots + X^{p^{r-1}} + 1$. Este polinômio é chamado de **p^r-ésimo polinômio ciclotômico**.

Teorema 2.3.1. *(*Lang, 1972, p.204, Teo.6*) Se ζ_n é uma raiz n-ésima primitiva da unidade, então $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.*

Demonstração. Seja $f(X)$ um polinômio mônico, irredutível e de menor grau de ζ_n sobre $\mathbb{Q}$. Logo $X^n - 1 = f(X)h(X)$, com $h(X) \in \mathbb{Q}[X]$. Pelo lema de Gauss segue que $f(X)$, $h(X) \in \mathbb{Z}[X]$. Seja p um número primo tal que $p \nmid n$. Assim, ζ_n^p é raiz n-ésima primitiva da unidade. Logo $(\zeta_n^p)^n - 1 = f(\zeta_n^p)h(\zeta_n^p)$, ou seja, $0 = f(\zeta_n^p)h(\zeta_n^p)$. Assim, se ζ_n^p não for raiz de $f(X)$, então ζ_n^p é raiz de $h(X)$, e portanto ζ_n é raiz de $h(X^p)$. Portanto, pelo modo como tomamos $f(X)$, segue que, $f(X) \mid h(X^p)$, ou seja, $h(X^p) = f(X)g(X)$, com $g(X) \in \mathbb{Z}[X]$ pelo lema de Gauss. Como consequência do pequeno Teorema de Fermat, $a^p \equiv a (mod\ p)$ e daí $h(X^p) \equiv h(X)^p (mod\ p)$. Assim, $f(X)g(X) \equiv h(X)^p (mod\ p)$, e portanto $h(X)^p \equiv f(X)g(X) (mod\ p)$. Logo, $\overline{h(\zeta_n)^p} = \overline{0}$, pois ζ_n é raiz de $f(X)$. E recursivamente chegamos que $\overline{h}(\zeta_n) = 0$. Portanto $\overline{f}$ e $\overline{h}$ tem uma raiz em comum. Assim $X^n - \overline{1} = \overline{f}(X)\overline{h}(X)$, e portanto $X^n - \overline{1}$ tem raízes múltiplas. Logo $nX^{n-1} = \overline{0}$ e assim, para qualquer $\alpha \in \mathbb{Z}_p$, $n\alpha^{n-1} = \overline{0}$. Como a característica de $\mathbb{Z}_p$ é p segue que $p|n$, o que contradiz o fato de termos suposto que $p \nmid n$. Portanto ζ_n^p é raiz de $f(X)$ $\forall$ $p \nmid n$ e $mdc(p, n) = 1$. Logo $\partial(f(X)) \geq \partial(\varphi_n(X))$, pois toda raiz de $\varphi_n(X)$ é raiz de $f(X)$, e como $f(X)|\varphi_n(X)$, segue que $\partial(\varphi_n(X)) \geq \partial(f(X))$. Portanto $\partial(f(X)) = \partial(\varphi_n(X)) = \phi(n)$. ∎

Observação 2.3.1. *Existe um único polinômio minimal $f(X)$ tal que $f(\zeta_n) = 0$. Pelo Teorema 2.3.1, $\partial(f(X)) = \partial(\varphi_n(X))$, e $\varphi_n(\zeta_n) = 0$. Assim $f(X) = \varphi_n(X)$, e assim $\varphi_n(X)$ é irredutível.*

Lema 2.3.2. *(*Lang, 1972, p.204*) Se* $mdc(m, n) = 1$, *então* $U_{mn} \cong U_m \times U_n$.

Demonstração. Seja a seguinte função:

$$\begin{aligned} \varphi : U_m \times U_n &\longrightarrow U_{mn} \\ (a, b) &\longmapsto ab \end{aligned}$$

i) φ esta bem definida, pois $(ab)^{mn} = (a^m)^n(b^n)^m = 1$

ii) φ é homomorfismo, pois $\forall (a, b), (c, d) \in U_m \times U_n$ temos que $\varphi((a, b) \cdot (c, d)) = \varphi(ac, bd) = (acbd) = (ab)(cd) = \varphi(a, b)\varphi(c, d)$.

iii) φ é injetora: Temos que provar que $Ker(\varphi) = \{(a, b) \in U_m \times U_n : \varphi(a, b) = 1\} = \{1\}$. Deste modo, temos que mostrar que para $\forall (a, b) \in U_m \times U_n$ tal que $\varphi(a, b) = ab = 1 \Longrightarrow a = b = 1$. Para isto, seja $a = \zeta_m^k$, $b = \zeta_n^l$, onde $0 \leq k \leq m-1$ e $0 \leq l \leq n-1$. Assim, $ab = 1 \iff \zeta_m^k\zeta_n^l = 1 \iff \zeta_m^k = \zeta_n^{-l} \iff \zeta_m^{nk} = \zeta_n^{-nl} \iff \zeta_m^{nk} = 1$. Logo, como ζ_m é uma raiz m-ésima primitiva da unidade, segue que $m|nk$, e como $mdc(m, n) = 1$ então $m|k$, e isto implica que $k = mx$. Analogamente $n|l$, e isto implica que $l = ny$. Deste modo, $\zeta_m^k = \zeta_m^{mx} = 1 = \zeta_n^{-ny} = \zeta_n^{-l}$, ou seja, $\zeta_m^k = \zeta_n^{-l} = 1$, e isto implica que $k = l = 0$, pois ζ_m e ζ_n são raízes m-ésima e n-ésima primitivas da unidade, respectivamente. Portanto $ab = 1 \iff a = b = 1$. Portanto $Ker(\varphi) = \{1\}$ e assim φ é injetora.

iv) φ é sobrejetora: Como $o(U_m \times U_n) = o(U_{mn})$ e φ é injetora, segue que φ é sobrejetora. Por *iii*) e *iv*), φ é bijetora. Portanto φ é isomorfismo. ■

Proposição 2.3.1. *(*Lang, 1972, p.205*) Temos que* $\zeta_m^k\zeta_n^l$, *para* $0 \leq k \leq m-1$ *e* $0 \leq l \leq n-1$, *é uma raiz* mn*-ésima primitiva da unidade se, e somente se,* ζ_m^k *é uma raiz* m*-ésima primitiva da unidade e* ζ_n^l *é uma raiz* n*-ésima primitiva da unidade.*

Demonstração. Se ζ_m^k não é uma raiz m-ésima primitiva da unidade, então temos que $mdc(k, m) = d > 1$. Assim, $(\zeta_m^k\zeta_n^l)^{\frac{mn}{d}} = ((\zeta_m^k\zeta_n^l)^{mn})^{\frac{1}{d}} = 1^{\frac{1}{d}} = 1$, o que é absurdo, pois $\frac{mn}{d} < mn$. Reciprocamente, se ζ_m^k é uma raiz m-ésima primitiva da unidade e ζ_n^l é uma raiz n-ésima primitiva da unidade, então $mdc(k, m) = mdc(l, n) = 1$. Assim,

$$(\zeta_m^k\zeta_n^l)^a = 1 \iff \zeta_m^{ka}\zeta_n^{la} = 1 \iff \zeta_m^{ka} = \zeta_n^{-la} \iff \zeta_m^{kan} = \zeta_n^{-lan} \iff$$
$$(\zeta_m^k)^{na} = (\zeta_n^n)^{-la} \iff (\zeta_m^k)^{na} = 1^{-la} \iff (\zeta_m^k)^{na} = 1 \iff m|na.$$

Como $mdc(m, n) = 1$ segue que $m|a$. De modo análogo, $n|a$. Ainda, usando o fato de que $mdc(m, n) = 1$ segue que $mn|a$. Assim temos que, $(\zeta_m^k\zeta_n^l)^{mn} = (\zeta_m^m)^{kn}(\zeta_n^n)^{lm} = 1$. Assim, mn é a menor potência tal que $(\zeta_m^k\zeta_n^l)^{mn} = 1$. Portanto $\zeta_m^k\zeta_n^l$ é uma raiz mn-ésima primitiva da unidade. ■

Corolário 2.3.1. *(*Lang, 1972, p.205*)* $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$.

Sejam p um número primo e ζ_p uma raiz p-ésima primitiva da unidade. Como em $\varphi_p(X)$ o coeficiente a_{p-2} do termo X^{p-2} é igual a 1, segue que

$$\begin{cases} Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1) = \left[\mathbb{Q}(\zeta_p) : \mathbb{Q}\right] \cdot 1 = p - 1, \text{ e} \\ Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^j) = -a_{p-2} = -1, \text{ para } j = 1, \cdots, p-1. \end{cases}$$

Consequentemente,

$$Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1-\zeta_p^j) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1) - Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^j) = p, \text{ para } j = 1, \cdots, p-1. \tag{2.5}$$

Os elementos $1 - \zeta_p^j$, para $j = 1, \cdots, p-1$, são todos os conjugados de $1 - \zeta_p^k$, para $k = 1, \cdots, p-1$. Assim, pela Definição 2.3.2, segue que $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1 - \zeta_p^k) = \varphi_p(1) = p$, para $k = 1, \cdots, p-1$.

Lema 2.3.3. *(*Simonato, 2000, p.18, Lema1.4.4*) Se* $\mathbb{A}_{\mathbb{K}}$ *é o anel dos inteiros algébricos de* $\mathbb{K} = \mathbb{Q}(\zeta_p)$ *então:*

i) $(1-\zeta_p)\mathbb{A}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}$.

ii) $Tr_{\mathbb{K}/\mathbb{Q}}((1-\zeta_p)y) \in p\mathbb{Z}$, $\forall\, y \in \mathbb{A}_{\mathbb{K}}$.

Demonstração: i) O p-ésimo polinômio ciclotômico de ζ_p é $\varphi_p(X) = X^{p-1} + \cdots + X + 1 = (X-\zeta_p)(X-\zeta_p^2)\cdots(X-\zeta_p^{p-1})$. Como $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1-\zeta_p^k) = (1-\zeta_p)(1-\zeta_p^2)\cdots(1-\zeta_p^{p-1}) = p$, segue que $\varphi_p(1) = (1-\zeta_p)(1-\zeta_p^2)\cdots(1-\zeta_p^{p-1}) = p$. Como $1-\zeta_p^j \in \mathbb{A}_{\mathbb{K}}$, para $j = 1, \cdots, p-1$, segue que $p \in (1-\zeta_p)\mathbb{A}_{\mathbb{K}}$. Portanto $p\mathbb{Z} \subset (1-\zeta_p)\mathbb{A}_{\mathbb{K}} \cap \mathbb{Z}$. Para mostrar a outra inclusão, vamos supor por absurdo que $p\mathbb{Z}$ está contido propriamente em $(1-\zeta_p)\mathbb{A}_{\mathbb{K}} \cap \mathbb{Z} \subset \mathbb{Z}$. Como $p\mathbb{Z}$ é um ideal maximal de $\mathbb{Z}$, então $(1-\zeta_p)\mathbb{A}_{\mathbb{K}} \cap \mathbb{Z} = \mathbb{Z}$. Como $1 \in \mathbb{Z}$ segue que $1 = (1-\zeta_p)a$, para algum $a \in \mathbb{A}_{\mathbb{K}}$. Logo $1-\zeta_p$ é inversível em $\mathbb{A}_{\mathbb{K}}$, e assim $1-\zeta_p^j$ são inversíveis em $\mathbb{A}_{\mathbb{K}}$, para $j = 2, \cdots, p-1$. Assim, $(1-\zeta_p)(1-\zeta_p^2)\cdots(1-\zeta_p^{p-1})$ é inversível em $\mathbb{A}_{\mathbb{K}} \cap \mathbb{Z}$, isto é, p é inversível em $\mathbb{A}_{\mathbb{K}} \cap \mathbb{Z}$, o que é um absurdo. Portanto $(1-\zeta_p)\mathbb{A}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}$.

ii) Cada conjugado $y_i(1-\zeta_p^i)$ de $y(1-\zeta_p)$ é um múltiplo de $1-\zeta_p^i$ em $\mathbb{A}_{\mathbb{K}}$, para $i = 1, 2, \cdots, p-1$. Como $1-\zeta_p^i = (1-\zeta_p)(1+\zeta_p+\cdots+\zeta_p^{i-1})$ segue que $1-\zeta_p^i$ é um múltiplo de $1-\zeta_p$ em $\mathbb{A}_{\mathbb{K}}$. Sendo o traço a soma dos conjugados, $Tr_{\mathbb{K}/\mathbb{Q}}(y(1-\zeta_p)) = y_1(1-\zeta_p) + y_2(1-\zeta_p^2) + \cdots + y_{p-1}(1-\zeta_p^{p-1}) = \alpha(1-\zeta_p)$, $\alpha \in \mathbb{A}_{\mathbb{K}}$. Portanto $Tr(y(1-\zeta_p)) \in \mathbb{A}_{\mathbb{K}}(1-\zeta_p)$. Como, pela Proposição 1.3.4, $\mathbb{Z}$ é integralmente fechado, segue pelo Corolário 1.5.1 que $Tr(y(1-\zeta_p)) \in \mathbb{Z}$. Assim, $Tr(y(1-\zeta_p)) \in \mathbb{A}_{\mathbb{K}}(1-\zeta_p) \cap \mathbb{Z} = p\mathbb{Z}$, onde a igualdade segue de (i).

■

Teorema 2.3.2. *(*Samuel, 1967, p.43, Teo.2*) O anel dos inteiros de* $\mathbb{K} = \mathbb{Q}(\zeta_p)$ *é* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$ *e* $\{1, \zeta_p, \cdots, \zeta_p^{p-2}\}$ *é uma base de* $\mathbb{Z}[\zeta_p]$ *como um* $\mathbb{Z}$*-módulo.*

Demonstração: Seja $\mathbb{A}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K} = \mathbb{Q}(\zeta_p)$. Como $\mathbb{Z}[\zeta_p] \subset \mathbb{A}_{\mathbb{K}}$, falta mostrar que $\mathbb{A}_{\mathbb{K}} \subset \mathbb{Z}[\zeta_p]$. Se $\alpha \in \mathbb{A}_{\mathbb{K}}$, então $\alpha \in \mathbb{Q}(\zeta_p)$, e assim podemos escrever

$$\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}, \tag{2.6}$$

com $a_i \in \mathbb{Q}$, para $i = 0, 1, \cdots, p-2$. Multiplicando por $1 - \zeta_p$ em ambos os membros temos que

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

Aplicando o traço nesta equação e usando a sua linearidade, obtemos que

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

pelo Lema 2.3.3. Como $Tr(\zeta_p^i - \zeta_p^{i+1}) = 0$, para $i = 1, 2, \cdots, p-2$, segue que $a_0 Tr(1-\zeta_p) = a_0 p \in p\mathbb{Z}$ e assim $a_0 \in \mathbb{Z}$. Como $\zeta_p^{-1} = \zeta_p^{p-1}$ segue que $\zeta_p^{-1} \in \mathbb{A}_{\mathbb{K}}$, e portanto pela Equação (2.6) segue que

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

Multiplicando ambos os membros por $1 - \zeta_p$ temos que

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

Logo

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

Mas $a_1 Tr(1-\zeta_p) = a_1 p \in p\mathbb{Z}$ e assim $a_1 \in \mathbb{Z}$. Continuando dessa forma, chegamos que $a_i \in \mathbb{Z}$, para todo $i = 0, 1, \cdots p-2$. Portanto $\mathbb{A}_{\mathbb{K}} \subseteq \mathbb{Z} + \mathbb{Z}\zeta_p + \cdots + \mathbb{Z}\zeta_p^{p-2}$, ou seja, $\mathbb{A}_{\mathbb{K}} \subseteq \mathbb{Z}[\zeta_p]$. Deste modo concluímos que $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$. Além disso, como $1, \zeta_p, \cdots, \zeta_p^{p-2}$ são

linearmente independentes sobre $\mathbb{Z}$, pois são sobre $\mathbb{Q}$ e como $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}+\mathbb{Z}\zeta_p+\cdots+\mathbb{Z}\zeta_p^{p-2}$ segue que $\{1, \zeta_p, \cdots, \zeta_p^{p-2}\}$ é uma base de $\mathbb{Z}[\zeta_p]$. ■

Proposição 2.3.2. *(*Simonato, 2000, p.19, Obs.1.4.6*) O discriminante absoluto de* $\mathbb{K} = \mathbb{Q}(\zeta_p)$ *sobre* $\mathbb{Q}$ *é dado por* $D_{\mathbb{K}} = D_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1, \zeta_p, \cdots, \zeta_p^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}$.

Demonstração: Sejam p um número primo e ζ_p uma raiz p-ésima da unidade. Vimos que $\{1, \zeta_p, \cdots, \zeta_p^{p-2}\}$ é uma base integral de $\mathbb{Z}[\zeta_p]$. Pela Proposição 1.6.4 temos que $D_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1, \zeta_p, \cdots, \zeta_p^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} N_{\mathbb{Q}(\zeta_p)/Q}(\varphi_p^{'}(\zeta_p))$, e deste modo vamos mostrar que $N_{\mathbb{Q}(\zeta_p)/Q}(\varphi_p^{'}(\zeta_p)) = p^{p-2}$. Como o p-ésimo polinômio ciclotômico é dado por $\varphi_p(X) = \dfrac{X^p - 1}{X - 1}$, segue que derivando ambos os lados temos que $\varphi_p^{'}(X) = \dfrac{(X-1)p\,X^{p-1} - (X^p - 1)}{(X-1)^2}$. Substituindo X por ζ_p temos que $\varphi_p^{'}(\zeta_p) = \dfrac{(\zeta_p - 1)p\,\zeta_p^{p-1} - (\zeta_p^p - 1)}{(\zeta_p - 1)^2}$. Como $\zeta_p^p = 1$, pois ζ_p é uma raiz p-ésima da unidade, temos que $\varphi_p^{'}(\zeta_p) = \dfrac{p\,\zeta_p^{-1}(\zeta_p - 1)}{(\zeta_p - 1)^2}$, ou seja, $\varphi_p^{'}(\zeta_p) = \dfrac{p}{(\zeta_p - 1)\zeta_p}$, e isto implica que $\varphi_p^{'}(\zeta_p) = \dfrac{-p}{(1 - \zeta_p)\zeta_p}$. Aplicando a norma e usando a sua linearidade obtemos que $N_{\mathbb{Q}(\zeta_p)/Q}(\varphi_p^{'}(\zeta_p)) = \dfrac{N_{\mathbb{Q}(\zeta_p)/Q}(-p)}{N_{\mathbb{Q}(\zeta_p)/Q}(1 - \zeta_p)N_{\mathbb{Q}(\zeta_p)/Q}(\zeta_p)} = \dfrac{(-p)^{p-1}}{p \cdot 1} = \dfrac{p^{p-1}}{p} = p^{p-2}$. Portanto $D_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1, \zeta_p, \cdots, \zeta_p^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}$. ■

Sejam p um número primo e $n \geq 1$ um inteiro. O Lema 2.3.3 estende naturalmente para o p^r-ésimo corpo ciclotômico, $\mathbb{Q}(\zeta_{p^r})$, ou seja, valem

$$\begin{cases} i)\ (1 - \zeta_{p^r})\mathbb{A}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z}. \\ ii)\ Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}((1 - \zeta_{p^r})y) \in p\mathbb{Z},\ \forall\, y \in \mathbb{A}_{\mathbb{K}}. \end{cases}$$

onde $\mathbb{A}_{\mathbb{K}}$ é o anel dos inteiros de $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$. Nosso objetivo agora é encontrar o anel dos inteiros algébricos, $\mathbb{A}_{\mathbb{K}}$, de $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$.

Lema 2.3.4. *(*Marcus, 1977, p.30, Lema.1*) Temos que* $\mathbb{Z}[1-\zeta_{p^r}] = \mathbb{Z}[\zeta_{p^r}]$ *e que*

$$D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1,\, 1-\zeta_{p^r}, \cdots, (1-\zeta_{p^r})^{\phi(p^r)-1}) = D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{\phi(p^r)-1}),$$

onde $p^r \geq 3$.

Demonstração. Por definição, $\mathbb{Z}[\alpha] = \left\{ \sum_i a_i \alpha^i \,:\, a_i \in \mathbb{Z} \right\}$. Logo, para qualquer $\alpha \in \mathbb{Z}[1-\zeta_{p^r}]$ temos que $\alpha = b_0 + b_1(1-\zeta_{p^r}) + b_2(1-\zeta_{p^r})^2 + \cdots + b_{(p-1)p^{r-1}-1}(1-\zeta_{p^r})^{(p-1)p^{r-1}-1} = (b_0 + b_1 + b_2 + \cdots + b_{(p-1)p^{r-1}-1}) + (-b_1 - 2b_2)\zeta_{p^r} + b_2\zeta_{p^r}^2 + \cdots$. Assim, temos que α é da forma $a_0 + a_1\zeta_{p^r} + a_2\zeta_{p^r}^2 + \cdots + a_{(p-1)p^{r-1}-1}\zeta_{p^r}^{(p-1)p^{r-1}-1}$, ou seja, $\alpha \in \mathbb{Z}[\zeta_{p^r}]$. Portanto $\mathbb{Z}[1-\zeta_{p^r}] \subset \mathbb{Z}[\zeta_{p^r}]$. Por outro lado, seja $\alpha \in \mathbb{Z}[\zeta_{p^r}]$. Assim, $\alpha = a_0 + a_1\zeta_{p^r} + a_2\zeta_{p^r}^2 + \cdots + a_{(p-1)p^{r-1}-1}\zeta_{p^r}^{(p-1)p^{r-1}-1}$. Observando que $\zeta_{p^r} = 1-(1-\zeta_{p^r})$, temos que

$$\begin{aligned}
\alpha &= a_0 + a_1(1-(1-\zeta_{p^r})) + \cdots + a_{(p-1)p^{r-1}-1}(1-(1-\zeta_{p^r}))^{(p-1)p^{r-1}-1} \\
&= a_0 + a_1 - a_1(1-\zeta_{p^r}) + a_2(1-2(1-\zeta_{p^r}) + (1-\zeta_{p^r})^2) + \cdots \\
&= a_0 + a_1 - a_1(1-\zeta_{p^r}) + a_2 - 2a_2(1-\zeta_{p^r}) + a_2(1-\zeta_{p^r})^2 + \cdots \\
&= (a_0 + \cdots + a_{(p-1)p^{r-1}-1}) + (-a_1 - 2a_2)(1-\zeta_{p^r}) + \cdots .
\end{aligned}$$

Dessa forma, chegamos que α é da forma $b_0 + b_1(1-\zeta_{p^r}) + b_2(1-\zeta_{p^r})^2 + \cdots + b_{(p-1)p^{r-1}-1}(1-\zeta_{p^r})^{(p-1)p^{r-1}-1}$, isto é, $\alpha \in \mathbb{Z}[1-\zeta_{p^r}]$. Assim $\mathbb{Z}[\zeta_{p^r}] \subset \mathbb{Z}[1-\zeta_{p^r}]$. Portanto, das duas inclusões concluímos que $\mathbb{Z}[\zeta_{p^r}] = \mathbb{Z}[1-\zeta_{p^r}]$. Para a segunda parte, como os conjugados de ζ_{p^r} são os elementos $\zeta_{p^r}^k$ tais que $k = 1, \cdots, p^r - 1$ e $mdc(k, p^r) = 1$, segue que os elementos $1-\zeta_{p^r}^k$ são os conjugados de $1-\zeta_{p^r}$. Como

$\det(\sigma_j(\zeta_{p^r}^i))$ é o determinante de uma matriz de Vandermonde,

$$\begin{aligned} D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{\phi(p^r)-1}) &= \prod_{t<k}(\zeta_{p^r}^k - \zeta_{p^r}^t)^2 \\ &= \prod_{t<k}((1-\zeta_{p^r}^k) - (1-\zeta_{p^r}^t))^2 \\ &= D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \cdots, (1-\zeta_{p^r})^{\phi(p^r)-1}). \end{aligned}$$

■

Lema 2.3.5. *(*Marcus, 1977, p.31, Lema 2*) Temos que* $\prod_k(1-\zeta_{p^r}^k) = p$, *onde o produto é tomado sobre todos os* k, *com* $1 \leq k \leq p^r$, *e tal que* $p \nmid k$.

Demonstração. Como $\varphi_{p^r}(X) = \dfrac{X^{p^r}-1}{X^{p^{r-1}}-1} = 1 + X^{p^{r-1}} + X^{2p^{r-1}} + \cdots + X^{(p-1)p^{r-1}}$, segue que todos os $\zeta_{p^r}^k$, onde $1 \leq k \leq p^r$ e tal que $p \nmid k$ são raízes de $\varphi_{p^r}(X)$ pois são raízes de $X^{p^r}-1$ mas não de $X^{p^{r-1}}-1$. Deste modo, $\varphi_{p^r}(X) = \prod_k(X-\zeta_{p^r}^k)$ e existem exatamente $\phi(p^r) = (p-1)p^{r-1}$ valores de k pois $\partial(\varphi_{p^r}(X)) = (p-1)p^{r-1}$. Tomando $X = 1$, temos que $\varphi_{p^r}(1) = \prod_k(1-\zeta_{p^r}^k) = 1 + 1^{p^{r-1}} + \cdots + 1^{(p-1)p^{r-1}} = p$.

■

Teorema 2.3.3. *(*Marcus, 1977, p.29, Teo.9*) Sejam* $\{\alpha_1, \cdots, \alpha_n\}$ *uma base de* $\mathbb{K}$ *sobre* $\mathbb{Q}$ *consistindo de inteiros algébricos e* $d = D_{\mathbb{K}/\mathbb{Q}}(\alpha_1, \cdots, \alpha_n)$. *Se* $\alpha \in \mathbb{A}_{\mathbb{K}}$, *então* α *pode ser expresso na forma* $\dfrac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d}$, *com* $m_j \in \mathbb{Z}$ *e* m_j^2 *divisível por* d, *para* $j = 1, 2, \cdots, n$.

Demonstração. Se $\alpha \in \mathbb{A}_{\mathbb{K}}$, então $\alpha \in \mathbb{K}$. Como $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, segue que

$$\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n,$$

com $x_j \in \mathbb{Q}$, para $j = 1, \cdots, n$. Sejam $\sigma_1, \cdots, \sigma_n$ os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Aplicando cada σ_i, para $i = 1, \cdots, n$, em α, obtemos um sistema de n equações dada por

$$\sigma_i(\alpha) = x_1\sigma_i(\alpha_1) + \cdots + x_n\sigma_i(\alpha_n),$$

para $i = 1, \cdots, n$. Resolvendo esse sistema pela regra de Cramer, obtemos que as n raízes são dadas por $x_j = \frac{\gamma_j}{\delta}$, onde $\delta = \det(\sigma_i(\alpha_j))$ e γ_j é obtido de δ trocando a j-ésima coluna por $\sigma_i(\alpha)$. Temos que os γ_j, para $j = 1, 2, \cdots, n$, e δ são inteiros algébricos pois são obtidos a partir dos $\alpha_i's$, que são, por hipótese, inteiros algébricos. Pela Proposição 1.6.3, temos que $\delta^2 = d$ e portanto $dx_j = d\frac{\gamma_j}{\delta} = \delta^2\frac{\gamma_j}{\delta} = \delta\gamma_j$ é um inteiro algébrico. Como $\mathbb{Z}$ é integralmente fechado segue que $dx_j \in \mathbb{Z}$, para $j = 1, 2, \cdots, n$. Seja $m_j = dx_j$, para $j = 1, 2, \cdots n$. Se mostrarmos que $\frac{m_j^2}{d} \in \mathbb{Z}$, teremos que m_j^2 é divisível por d. Mas, como $\frac{m_j^2}{d} \in \mathbb{Q}$ e como $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$ então é suficiente mostrarmos que $\frac{m_j^2}{d}$ é um inteiro algébrico. Como $m_j = dx_j = \delta\gamma_j$ segue que $m_j^2 = d^2x_j^2 = \delta^2\gamma_j^2 = d\gamma_j^2$. Logo $\frac{m_j^2}{d} = \gamma_j^2$ é um inteiro algébrico pois γ_j é um inteiro algébrico. Portanto $\frac{m_j^2}{d} \in \mathbb{Z}$ e assim m_j^2 é divisível por d. ■

Lema 2.3.6. *(*Marcus, 1977, p.31*) Se* $d = D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{n-1})$, *onde* $n = \phi(p^r)$, *então* $d = p^s$ *para algum* $s \in \mathbb{N}$.

Demonstração: Pela Equação (2.3) temos que

$$X^{p^r} - 1 = \varphi_{p^r}(X)g(X), \tag{2.7}$$

onde $g(X) = X^{p^{r-1}} - 1$ e $\varphi_{p^r}(X)$ é o polinômio irredutível de ζ_{p^r} sobre $\mathbb{Q}$. Derivando a Equação (2.7) temos que $p^r X^{p^r-1} = \varphi_{p^r}'(X)g(X) + \varphi_{p^r}(X)g'(X)$, e substituindo X por ζ_{p^r} obtemos que

$$p^r\zeta_{p^r}^{p^r-1} = \varphi_{p^r}^{'}(\zeta_{p^r})g(\zeta_{p^r}) + \varphi_{p^r}(\zeta_{p^r})g^{'}(\zeta_{p^r}).$$

Como $\varphi_{p^r}(\zeta_{p^r}) = 0$ segue que

$$p^r\zeta_{p^r}^{p^r-1} = \varphi_{p^r}^{'}(\zeta_{p^r})g(\zeta_{p^r}),$$

e isto é equivalente a

$$p^r\zeta_{p^r}^{p^r}\zeta_{p^r}^{-1} = \varphi_{p^r}^{'}(\zeta_{p^r})g(\zeta_{p^r}),$$

ou seja,

$$p^r = \zeta_{p^r}\varphi_{p^r}^{'}(\zeta_{p^r})g(\zeta_{p^r}).$$

Aplicando a função norma nesta última igualdade obtemos que

$$p^{nr} = N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\varphi_{p^r}^{'}(\zeta_{p^r}))N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}g(\zeta_{p^r})).$$

Pela Proposição 1.6.4, temos que

$$p^{nr} = \pm D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1,\cdots,\zeta_{p^r}^{n-1})N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}g(\zeta_{p^r})).$$

Logo, $d|p^{nr}$, ou seja, $d = p^s$, para algum inteiro s. ■

Teorema 2.3.4. *(*Marcus, 1977, p.30, Teo.10*) O anel $\mathbb{A}_{\mathbb{K}}$ dos inteiros algébricos de $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$ é $\mathbb{Z}[\zeta_{p^r}]$.*

Demonstração. Mostraremos que $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[1-\zeta_{p^r}]$, e assim o teorema segue pelo Lema 2.3.4. Suponhamos que $\mathbb{A}_{\mathbb{K}} \neq \mathbb{Z}[1-\zeta_{p^r}]$. Pelo Teorema 2.3.3, todo elemento $\alpha \in \mathbb{A}_{\mathbb{K}}$ pode ser expresso na forma

$$\alpha = \frac{m_1 + m_2(1-\zeta_{p^r}) + \cdots + m_n(1-\zeta_{p^r})^{n-1}}{d},$$

onde $n = \phi(p^r)$, e $m_i \in \mathbb{Z}$, para $i = 1, 2, \cdots, n$. Pelo Lema 2.3.6, temos que $d = p^s$, onde $s \in \mathbb{N}$. Logo, existe $\alpha \in \mathbb{A}_{\mathbb{K}}$ de modo que nem todos os m_j são divisíveis por p^s. Seja $i \leq n$ tal que m_i não seja divisível por p^s. Assim, temos que $m_i = p^s q + r$, onde $q, r \in \mathbb{Z}$ e $r < p^s$. Logo, podemos reescrever α da seguinte forma

$$\alpha = \frac{m_1 + m_2(1-\zeta_{p^r}) + \cdots + (p^s q + r)(1-\zeta_{p^r})^{i-1} + \cdots + m_n(1-\zeta_{p^r})^{n-1}}{p^s}.$$

Desse modo, $\mathbb{A}_{\mathbb{K}}$ contém um elemento da forma

$$\gamma = \frac{r(1-\zeta_{p^r})^{i-1} + m_{i+1}(1-\zeta_{p^r})^{i} + \cdots + m_n(1-\zeta_{p^r})^{n-1}}{p^s}.$$

Multiplicando ambos os lados por p^{s-1}, obtemos que

$$\gamma p^{s-1} = \frac{r(1-\zeta_{p^r})^{i-1} + m_{i+1}(1-\zeta_{p^r})^{i} + \cdots + m_n(1-\zeta_{p^r})^{n-1}}{p},$$

que podemos reescrever como

$$\beta = \frac{a_i(1-\zeta_{p^r})^{i-1} + a_{i+1}(1-\zeta_{p^r})^{i} + \cdots + a_n(1-\zeta_{p^r})^{n-1}}{p},$$

com $a_j \in \mathbb{Z}$ e a_i não divisível por p. Pelo Lema 2.3.5, temos que $p/(1-\zeta_{p^r})^n \in \mathbb{Z}[\zeta_{p^r}]$ pois $1-\zeta_{p^r}^k$ é divisível, em $\mathbb{Z}[\zeta_{p^r}]$, por $1-\zeta_{p^r}$. Então $p/(1-\zeta_{p^r})^i \in \mathbb{Z}[\zeta_{p^r}]$ e portanto temos que $\beta p/(1-\zeta_{p^r})^i \in \mathbb{A}_{\mathbb{K}}$. Subtraindo termos que estão em $\mathbb{A}_{\mathbb{K}}$, obtemos que $a_i/(1-\zeta_{p^r}) \in \mathbb{A}_{\mathbb{K}}$. Disto segue que $N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1-\zeta_{p^r}) \mid N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(a_i)$. Como $N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(a_i) = a_i^n$ e pelo Lema 2.3.5, temos que $N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1-\zeta_{p^r}) = p$. Assim $p \mid a_i^n$, o que é impossível pois a_i não é divisível por p. Portanto $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[1-\zeta_{p^r}] = \mathbb{Z}[\zeta_{p^r}]$. ∎

Observação 2.3.2. *Como o p^r-ésimo polinômio ciclotômico tem grau $(p-1)p^{r-1}$ e seu termo independente é igual a 1, obtemos pela seção 1.4, que*

$$N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^t) = (-1)^{(p-1)p^{r-1}}, \text{ onde } t = 0, \cdots, p^{r-1} \text{ e } mdc(t, p^r) = 1. \tag{2.8}$$

$$Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^t) = -a_{p-2} = -1, \text{ para } j = 1, \cdots, (p-1)p^{r-1} \tag{2.9}$$

$$Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1) = [\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = (p-1)p^{r-1}. \tag{2.10}$$

Proposição 2.3.3. *(*Simonato, 2000, p.22, Prop.1.4.9*) O discriminante absoluto de* $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$ *sobre* $\mathbb{Q}$ *é dado por* $D_{\mathbb{K}} = D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{\phi(p^r)-1}) = \pm p^{p^{r-1}\cdot(r(p-1)-1)}$.

Demonstração. Pela Proposição 1.6.4 temos que

$$D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{\phi(p^r)-1}) = \pm N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\varphi_{p^r}^{'}(\zeta_{p^r})).$$

Derivando ambos os membros de $\varphi_{p^r}(X) = \dfrac{X^{p^r}-1}{X^{p^{r-1}}-1}$, temos que

$$\varphi_{p^r}^{'}(X) = \frac{p^r X^{p^r-1}(X^{p^{r-1}}-1) - (X^{p^r}-1)p^{r-1}X^{p^{r-1}-1}}{(X^{p^{r-1}}-1)^2},$$

e substituindo X por ζ_{p^r} temos que

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

Como $\zeta_{p^r}^{p^r} = 1$ segue que

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

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

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

Da Equação (2.8) temos que $N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}) = \pm 1$. Também $N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(-p^r) = (-p^r)^{(p-1)p^{r-1}}$ e

$$\begin{aligned} N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1-\zeta_p) &= N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}(\zeta_p)}(1-\zeta_p)) \\ &= (N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1-\zeta_p))^{p^{r-1}} = p^{p^{r-1}}. \end{aligned}$$

Portanto $D_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1, \zeta_{p^r}, \cdots, \zeta_{p^r}^{\phi(p^r)-1}) = \dfrac{\pm p^{r(p-1)p^{r-1}}}{p^{p^{r-1}}} = \pm p^{p^{r-1}(r(p-1)-1)}$.

■

A seguir nosso objetivo é determinar o anel dos inteiros $\mathbb{A}_{\mathbb{K}}$ para qualquer corpo ciclotômico, $\mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n-ésima primitiva da unidade. Esta generalização seguirá de um resultado mais geral considerando os inteiros algébricos de um corpo composto $\mathbb{KL}$, onde $\mathbb{K}$ e $\mathbb{L}$ são corpos numéricos.

Se $\mathbb{K}$ e $\mathbb{L}$ são dois corpos numéricos, então o corpo composto $\mathbb{KL}$ (definido como o menor subcorpo de $\mathbb{C}$ contendo $\mathbb{K}$ e $\mathbb{L}$) consistem de todas as somas finitas

$$\alpha_1\beta_1 + \cdots + \alpha_r\beta_r, \text{ onde } \alpha_i \in \mathbb{K}, \text{ e } \beta_i \in \mathbb{L}, \text{ para } i = 1, 2, \cdots, r.$$

Se $\mathbb{A}_{\mathbb{K}}$, $\mathbb{A}_{\mathbb{L}}$ e $\mathbb{A}_{\mathbb{KL}}$ são os anéis dos inteiros algébricos de $\mathbb{K}$, $\mathbb{L}$ e $\mathbb{KL}$, respectivamente, então $\mathbb{A}_{\mathbb{KL}}$ contém o anel

$$\mathbb{A}_{\mathbb{K}}\mathbb{A}_{\mathbb{L}} = \{\alpha_1\beta_1 + \cdots + \alpha_r\beta_r : \alpha_i \in \mathbb{A}_{\mathbb{K}}, \beta_i \in \mathbb{A}_{\mathbb{L}}, \text{ para } i = 1, 2, \cdots, r\}.$$

Em geral, não temos uma igualdade. Entretanto, podemos mostrar que $\mathbb{A}_{\mathbb{KL}} = \mathbb{A}_{\mathbb{K}}\mathbb{A}_{\mathbb{L}}$ sob certas condições sobre os corpos ciclotômicos.

Sejam m e n os graus de $\mathbb{K}$ e $\mathbb{L}$, respectivamente, sobre $\mathbb{Q}$, e seja $d = mdc(d_1, d_2)$, onde d_1 e d_2 são o discriminante absoluto de $\mathbb{A}_{\mathbb{K}}$ e $\mathbb{A}_{\mathbb{L}}$, respectivamente.

Teorema 2.3.5. *(*Marcus, 1977, p.33, Teo.12*) Se* $[\mathbb{KL} : \mathbb{Q}] = mn$, *então* $\mathbb{A}_{\mathbb{KL}} \subset \frac{1}{d}\mathbb{A}_{\mathbb{K}}\mathbb{A}_{\mathbb{L}}$.

Demonstração. Sejam $\{\alpha_1, \cdots, \alpha_m\}$ uma base de $\mathbb{A}_{\mathbb{K}}$ sobre $\mathbb{Z}$ e $\{\beta_1, \cdots, \beta_n\}$ uma base de $\mathbb{A}_{\mathbb{L}}$ sobre $\mathbb{Z}$. Assim, temos que $\boldsymbol{B} = \{\alpha_i\beta_j,\ i = 1, \cdots, m;\ j = 1, \cdots, n\}$ é uma base de $\mathbb{A}_{\mathbb{K}}\mathbb{A}_{\mathbb{L}}$ sobre $\mathbb{Z}$ e também uma base de $\mathbb{KL}$ sobre $\mathbb{Q}$. Se $\alpha \in \mathbb{A}_{\mathbb{KL}}$, então α pode ser expresso na forma

$$\alpha = \sum_{i,j} \frac{m_{ij}}{r}\alpha_i\beta_j, \tag{2.11}$$

onde r e todos os m_{ij} estão em $\mathbb{Z}$, e que estes $mn+1$ inteiros não tem fatores comuns maiores que 1, ou seja, $mdc(r, mdc(m_{ij})) = 1$. Para mostrar o teorema, temos que mostrar que $r|d$ para qualquer α. Para isto, devemos mostrar que $r|d_1$ e $r|d_2$ pois assim, pela definição de máximo divisor comum, teremos que $r \mid d$. Temos que todo monomorfismo σ de $\mathbb{K}$ em $\mathbb{C}$ estende a um monomorfismo (que também denotamos por σ) de $\mathbb{KL}$ em $\mathbb{C}$, fixando $\mathbb{L}$. Portanto, para cada σ temos que

$$\sigma(\alpha) = \sum_{i,j} \frac{m_{ij}}{r} \sigma(\alpha_i)\beta_j.$$

Tomando $x_i = \sum_{j=1}^{n} \frac{m_{ij}}{r}\beta_j$, para cada $i = 1, \cdots, m$, obtemos m equações $\sum_{i=1}^{m} \sigma(\alpha_i)x_i = \sigma(\alpha)$ para cada σ. Agora, resolvendo este sistema pela regra de Cramer, obtemos que $x_i = \frac{\gamma_i}{\delta}$, onde δ é o determinante da matriz formado pelos coeficientes $\sigma(\alpha_i)$ e γ_i é obtido de δ trocando a i-ésima coluna por $\sigma(\alpha)$, para $i = 1, 2, \cdots, m$. Temos que δ e todos os γ_i são inteiros algébricos, pois todos os $\sigma(\alpha_i)$ e $\sigma(\alpha)$ são, e além disso $\delta^2 = d_1$. Se $e = d_1$, temos que $ex_i = \delta\gamma_i \in \mathbb{A}_{\mathbb{C}}$, onde $\mathbb{A}_{\mathbb{C}}$ é o anel dos inteiros algébricos de $\mathbb{C}$, e portanto $ex_i = \sum_{j=1}^{n} \frac{em_{ij}}{r}\beta_j \in \mathbb{A}_{\mathbb{C}} \cap \mathbb{L} = \mathbb{A}_{\mathbb{L}}$. Lembrando que $\{\beta_1, \cdots, \beta_n\}$ forma uma base integral para $\mathbb{A}_{\mathbb{L}}$, concluímos que os números racionais $\frac{em_{ij}}{r}$ devem ser inteiros, e deste modo r divide em_{ij}, para todo i e j. Como assumimos que r é relativamente primo com $mdc(m_{ij})$, segue que $r|e = d_1$. Analogamente, $r|d_2$. Portanto, $r \mid d$ e assim $d = kr$, com $k \in \mathbb{Z}$, ou seja, $r = \frac{d}{k}$. Substituindo na Equação (2.11) temos que $\alpha = \sum_{i,j} \frac{km_{ij}}{d}\alpha_i\beta_j = \frac{1}{d}\sum_{i,j} km_{ij}\alpha_i\beta_j$. Logo $\alpha \in \frac{1}{d}\mathbb{A}_{\mathbb{K}}\mathbb{A}_{\mathbb{L}}$. Portanto $\mathbb{A}_{\mathbb{KL}} \subset \frac{1}{d}\mathbb{A}_{\mathbb{K}}\mathbb{A}_{\mathbb{L}}$. ■

Corolário 2.3.2. *(*Marcus, 1977, p.34, Corol.1*) Se* $[\mathbb{KL} : \mathbb{Q}] = mn$ *e* $d = 1$, *então* $\mathbb{A}_{\mathbb{KL}} = \mathbb{A}_{\mathbb{K}}\mathbb{A}_{\mathbb{L}}$.

Demonstração. Como $\mathbb{A}_{\mathbb{K}}\mathbb{A}_{\mathbb{L}} \subset \mathbb{A}_{\mathbb{KL}}$ e como $d = 1$ segue, pelo Teorema 2.3.5, que $\mathbb{A}_{\mathbb{KL}} = \mathbb{A}_{\mathbb{K}}\mathbb{A}_{\mathbb{L}}$. ■

Teorema 2.3.6. *(*Marcus, 1977, p.34, Corol.2*) O anel dos inteiros de* $\mathbb{Q}(\zeta_n)$ *é* $R = \mathbb{Z}[\zeta_n]$.

Demonstração: O teorema já foi provado se n é primo ou se é uma potência de um primo. Agora, se n não é primo ou não é uma potência de um primo, então podemos escrever $n = n_1 n_2$, para inteiros relativamente primos n_1, n_2 maiores que 1. Vamos mostrar por indução que se o resultado também é válido para n_1 e n_2, então o resultado é válido para n. Assim, suponhamos por hipótese de indução que $R_1 = \mathbb{Z}[\zeta_{n_1}]$ e $R_2 = \mathbb{Z}[\zeta_{n_2}]$. Para aplicar o Corolário 2.3.2, temos que mostrar que

1)$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n_1})\mathbb{Q}(\zeta_{n_2})$ e como consequência $\mathbb{Z}[\zeta_n] = \mathbb{Z}[\zeta_{n_1}]\mathbb{Z}[\zeta_{n_2}]$.
2) $\phi(n) = \phi(n_1)\phi(n_2)$.
3) $d = 1$.

A parte (1) segue do Corolário 2.3.1 e a parte (2) segue do fato de n_1 e n_2 serem relativamente primos. Para a parte (3), temos da Proposição 1.6.4 que $D(1, \alpha, \cdots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N(f'(\alpha))$. Seja d_{n_1} e d_{n_2} o discriminante absoluto de $\mathbb{Z}[\zeta_{n_1}]$ e $\mathbb{Z}[\zeta_{n_2}]$, respectivamente. Como $f(X) = X^{n_1} - 1$, segue que $f'(X) = n_1 X^{n_1-1}$, e substituindo X por ζ_{n_1} segue que $f'(\zeta_{n_1}) = n_1 \zeta_{n_1}^{n_1-1} = \frac{n_1}{\zeta_{n_1}}$. Assim aplicando a função norma em ambos os lados e usando a sua linearidade temos que

$$N_{\mathbb{Q}(\zeta_{n_1})/\mathbb{Q}}(f'(\zeta_{n_1})) = \frac{N_{\mathbb{Q}(\zeta_{n_1})/\mathbb{Q}}(n_1)}{N_{\mathbb{Q}(\zeta_{n_1})/\mathbb{Q}}(\zeta_{n_1})} = \frac{n_1^{\phi(n_1)}}{\pm 1}.$$

Portanto $d_{n_1} = \pm n_1^{\phi(n_1)}$, e isto implica que

$$d_{n_1} | n_1^{\phi(n_1)}.$$

Analogamente,

$$d_{n_2} | n_2^{\phi(n_2)}.$$

Sendo $d = mdc(d_{n_1}, d_{n_2})$, temos que

$$\begin{cases} d | d_{n_1} \text{ e } d_{n_1} | n_1^{\phi(n_1)} \Longrightarrow d | n_1^{\phi(n_1)} \\ d | d_{n_2} \text{ e } d_{n_2} | n_2^{\phi(n_2)} \Longrightarrow d | n_2^{\phi(n_2)}. \end{cases}$$

Como $mdc(n_1^{\phi(n_1)}, n_2^{\phi(n_2)}) = 1$ segue que $d|1$, e portanto $d = 1$. Finalmente então concluímos que $R = R_1 R_2 = \mathbb{Z}[\zeta_{n_1}]\mathbb{Z}[\zeta_{n_2}] = \mathbb{Z}[\zeta_n]$. ■

Teorema 2.3.7. *(*Washington, 1982, p.11*) O discriminante absoluto de* $\mathbb{K} = \mathbb{Q}(\zeta_n)$ *sobre* $\mathbb{Q}$ *é dado por*

$$D_{\mathbb{K}} = D_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(1, \zeta_n, \cdots, \zeta_n^{\phi(n)-1}) = \pm \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$

Demonstração: Por (Ribenboim, 1972, p.217, prop.7O) temos que $D_{\mathbb{LM}} = D_{\mathbb{L}}^{[\mathbb{M}:\mathbb{Q}]} \cdot D_{\mathbb{M}}^{[\mathbb{L}:\mathbb{Q}]}$. Aplicando a função logaritmo em ambos os lados e usando as propriedades do logaritmo segue que $\log|D_{\mathbb{LM}}| = [\mathbb{M} : \mathbb{Q}] \log|D_{\mathbb{L}}| + [\mathbb{L} : \mathbb{Q}] \log|D_{\mathbb{M}}|$. Como toda extensão ciclotômica é Galoisiana, segue que $[\mathbb{LM} : \mathbb{Q}] = [\mathbb{L} : \mathbb{Q}][\mathbb{M} : \mathbb{Q}]$, e assim

$$\frac{\log|D_{\mathbb{LM}}|}{[\mathbb{LM} : \mathbb{Q}]} = \frac{\log|D_{\mathbb{L}}|}{[\mathbb{L} : \mathbb{Q}]} + \frac{\log|D_{\mathbb{M}}|}{[\mathbb{M} : \mathbb{Q}]}.$$

Portanto, se $n = \prod_i p_i^{a_i}$ temos que

$$\frac{\log|D_{\mathbb{K}}|}{[\mathbb{Q}(\zeta_n) : \mathbb{Q}]} = \frac{\log|D_{\mathbb{K}_1}|}{[\mathbb{Q}(\zeta_{p_1^{a_1}}) : \mathbb{Q}]} + \cdots + \frac{\log|D_{\mathbb{K}_r}|}{[\mathbb{Q}(\zeta_{p_r^{a_r}}) : \mathbb{Q}]} = \sum_{i=1}^{n} \frac{\log|D_{\mathbb{K}_i}|}{\phi(p_i^{a_i})},$$

onde $\mathbb{K}_i = \mathbb{Q}(\zeta_{p_i^{a_i}})$, $i = 1, 2, \cdots, r$. Assim, pela Proposição 2.3.3, temos que

$$\begin{aligned}
\frac{\log|D_{\mathbb{K}}|}{\phi(n)} &= \sum_{i=1}^{r} \frac{\log p_i^{p_i^{a_i-1}(a_i(p_i-1)-1)}}{p_i^{a_i-1}(p_i-1)} = \sum_{i=1}^{r} \frac{p_i^{a_i-1}(a_i(p_i-1)-1)}{p_i^{a_i-1}(p_i-1)} log p_i = \\
&= \sum_{i=1}^{r} \left(a_i - \frac{1}{p_i-1}\right) log p_i = \sum_{i=1}^{r} a_i log p_i - \sum_{i=1}^{r} \frac{log p_i}{p_i-1} = \\
&= \sum_{i=1}^{r} log p_i^{a_i} - \sum_{i=1}^{r} log p_i^{\frac{1}{p_i-1}} = \\
&= log\left(\prod_{i=1}^{r} p_i^{a_i}\right) - log\left(\prod_{i=1}^{r} p_i^{\frac{1}{p_i-1}}\right) = \\
&= log(n) - log\left(\prod_{i=1}^{r} p_i^{\frac{1}{p_i-1}}\right),
\end{aligned}$$

e consequentemente,

$$log|D_{\mathbb{K}}| = \phi(n)\left(log(n) - log\left(\prod_{i=1}^{r} p_i^{\frac{1}{p_i-1}}\right)\right) = log\left(\frac{n}{\prod_{i=1}^{r} p_i^{p_i-1}}\right)^{\phi(n)}.$$

Assim, $|D_{\mathbb{K}}| = \left(\frac{n}{\prod_{i=1}^{r} p_i^{p_i-1}}\right)^{\phi(n)}$ e portanto,

$$D_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(1, \zeta_n, \cdots, \zeta_n^{\phi(n)-1}) = (-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$

■

2.4 Decomposição de ideais primos em uma extensão

Nesta seção apresentamos a decomposição de um ideal primo em um extensão. Assim, dados $A \subset B$, anéis e $\mathfrak{a}$ um ideal de A, denotamos por $\mathfrak{a}B$ ao ideal de B formado pelos elementos da forma $\sum_{i=1}^{n} x_i y_i$, com $x_i \in \mathfrak{a}$ e $y_i \in B$. Além disso, consideramos $\mathbb{K} \subset \mathbb{L}$ corpos de números tais que $[\mathbb{L} : \mathbb{K}] = n$.

Se $\mathfrak{p}$ é um ideal primo de B, consideremos a inclusão $i : A \longrightarrow B$, a projeção canônica $h : B \longrightarrow B/\mathfrak{p}$ e a composição $f = h \circ i$. O núcleo de f é $A \cap \mathfrak{p}$ e portanto $A/(A \cap \mathfrak{p}) \simeq f(A) \subset B/\mathfrak{p}$, e deste modo, $A/(A \cap \mathfrak{p})$ é um domínio, isto é, $A \cap \mathfrak{p}$ é um ideal primo de A.

Proposição 2.4.1. *(*Samuel, 1967, p.71, Prop.1*) Sejam $\mathfrak{p}$ um ideal primo não nulo de $\mathbb{A}_{\mathbb{K}}$ e $\mathfrak{p}\mathbb{A}_{\mathbb{L}} = \prod_{i=1}^{g} \mathfrak{b}_i^{e_i}$ a decomposição do ideal $\mathfrak{p}\mathbb{A}_{\mathbb{L}}$ em ideais primos de $\mathbb{A}_{\mathbb{L}}$. Então os $\mathfrak{b}_i$'s são os únicos ideais primos de $\mathbb{A}_{\mathbb{L}}$ cuja interseção com $\mathbb{A}_{\mathbb{K}}$ coincide com $\mathfrak{p}$ e nestas condições dizemos que $\mathfrak{b}_i$ é um ideal acima de $\mathfrak{p}$.*

Demonstração: Para cada $i = 1, \cdots, g$ temos que $\mathfrak{b}_i \supseteq \mathfrak{p}\mathbb{A}_{\mathbb{L}} \supseteq \mathfrak{p}$, e portanto $\mathfrak{b}_i \cap \mathbb{A}_{\mathbb{K}}$ é um ideal primo de $\mathbb{A}_{\mathbb{K}}$ que contém $\mathfrak{p}$. Sendo $\mathfrak{p}$ maximal resulta que $\mathfrak{p} = \mathfrak{b}_i \cap \mathbb{A}_{\mathbb{K}}$. Agora, se d é um ideal primo de $\mathbb{A}_{\mathbb{L}}$ tal que $d \cap \mathbb{A}_{\mathbb{K}} = \mathfrak{p}$, então $d = \mathfrak{p}\mathbb{A}_{\mathbb{L}} = \prod_{i=1}^{g} \mathfrak{b}_i^{e_i}$. Assim, $d \supseteq \mathfrak{b}_i$, para algum i. Como $\mathfrak{b}_i$ é maximal segue que $d = \mathfrak{b}_i$. ■

O anel $\mathbb{A}_{\mathbb{K}}/\mathfrak{p}$ pode ser considerado como um subanel de $\mathbb{A}_{\mathbb{L}}/\mathfrak{b}_i$ através do homomorfismo induzido acima. Além disso, $\mathbb{A}_{\mathbb{K}}/\mathfrak{p}$ e $\mathbb{A}_{\mathbb{L}}/\mathfrak{b}_i$ são corpos e $\mathbb{A}_{\mathbb{L}}/\mathfrak{b}_i$ é um espaço vetorial de dimensão finita sobre $\mathbb{A}_{\mathbb{K}}/\mathfrak{p}$, uma vez que $\mathbb{A}_{\mathbb{L}}$ e $\mathbb{A}_{\mathbb{L}}/\mathfrak{b}_i$ são finitamente gerados como

$\mathbb{A}_{\mathbb{K}}$-módulo e $\mathbb{A}_{\mathbb{K}}/\mathfrak{p}$-módulo, respectivamente. A dimensão $[\mathbb{A}_{\mathbb{L}}/\mathfrak{b}_i : \mathbb{A}_{\mathbb{K}}/\mathfrak{p}]$, denotada por f_i ou $f(\mathfrak{b}_i, \mathfrak{p})$ é denominada de **grau residual** de $\mathfrak{b}_i$ sobre $\mathbb{A}_{\mathbb{K}}$. O expoente e_i ou $e(\mathfrak{b}_i, \mathfrak{p})$ é denominado **índice de ramificação** de $\mathfrak{b}_i$ sobre $\mathbb{A}_{\mathbb{K}}$. Quando $e_i > 1$, para algum índice i, dizemos que $\mathfrak{p}$ se ramifica em $\mathbb{L}$.

As igualdades $\sum_{i=1}^{g} e_i f_i = [\mathbb{A}_{\mathbb{L}}/\mathfrak{p}\mathbb{A}_{\mathbb{L}} : \mathbb{A}/\mathfrak{p}] = n$ podem ser vistas em ([6], *p.*71, *Teo.*1) e este resultado é conhecido como **Igualdade Fundamental**.

A igualdade fundamental forma alguns tipos de decomposições de $\mathfrak{p}$. Diremos, então, que o ideal primo $\mathfrak{p}$ de $\mathbb{A}_{\mathbb{K}}$ é

(i) totalmente decomposto em $\mathbb{L}$, se $g = n$ e consequentemente, $e_i = f_i = 1$, $i = 1, \cdots, g$.

(ii) inerte em $\mathbb{L}$, se $g = 1$, $e_1 = 1$ e consequentemente $f_1 = n$.

(iii) totalmente ramificado em $\mathbb{L}$, se $g = 1$ e consequentemente $f_1 = 1$ e $e_1 = n$.

Teorema 2.4.1. *(*Lang, 1970, p.27, Prop.25*) (Kummer) Seja A um anel de Dedekind com corpo quociente $\mathbb{K}$. Seja $\mathbb{L}$ uma extensão finita separável de $\mathbb{K}$. Seja $\mathbb{A}_{\mathbb{L}}$ o fecho integral de A em $\mathbb{L}$ e assuma que $\mathbb{A}_{\mathbb{L}} = A[\alpha]$ para algum elemento α. Seja $f(X)$ o polinômio irredutível de α sobre $\mathbb{K}$. Seja $\mathfrak{p}$ um ideal primo de A. Seja $\overline{f}(X)$ a redução de $f(X)$ e $\mathfrak{p}$, e seja*

$$\overline{f}(X) = \overline{\mu}_1(X)^{e_1} \cdots \overline{\mu}_r(X)^{e_r}$$

a fatoração de $\overline{f}(X)$ em potências de fatores irredutíveis sobre $\overline{A} = A/\mathfrak{p}$, com coeficiente dominante 1. Então

$$\mathfrak{p}\mathbb{A}_{\mathbb{L}} = \mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_r^{e_r} \tag{2.12}$$

é a fatoração de $\mathfrak{p}$ em $\mathbb{A}_{\mathbb{L}}$, de modo e_i é o índice de ramificação de

$\mathfrak{B}_i$ *sobre* $\mathfrak{p}$, *e temos que*

$$\mathfrak{B}_i = \mathfrak{p}\mathbb{A}_{\mathbb{L}} + \mu_i(\alpha)\mathbb{A}_{\mathbb{L}}, \tag{2.13}$$

se $\mu_i(X) \in A[X]$ *é um polinômio com coeficiente dominante 1 cuja redução módulo* $\mathfrak{p}$ *é* $\overline{\mu}_i(X)$.

Demonstração: Sejam $\overline{\mu}(X)$ um fator irredutível de $\overline{f}(X)$, $\overline{\alpha}$ uma raiz de $\overline{\mu}(X)$, e $\mathfrak{B}$ o ideal primo de $\mathbb{A}_{\mathbb{L}}$ que é o kernel da função

$$A[\alpha] \longrightarrow \overline{A}[\overline{\alpha}].$$

Temos que $\mathfrak{p}\mathbb{A}_{\mathbb{L}} + \mu(\alpha)\mathbb{A}_{\mathbb{L}}$ está contido em $\mathfrak{B}$. Por outro lado, seja $g(\alpha) \in \mathfrak{B}$ onde $g(X) \in A[X]$. Então $\overline{g}(X) = \overline{\mu(X)h(X)}$ para algum $\overline{h}(X) \in \overline{A}[X]$, e portanto $g(X) - \mu(X)h(X)$, que é um polinômio com coeficientes em A, uma vez que tem coeficientes em $\mathfrak{p}$. Isto prova a inclusão contrária, provando (2.13). Para provar (2.12), seja $e_i^{'}$ o índice de ramificação de $\mathfrak{B}_i$, tal que

$$\mathfrak{p}\mathbb{A}_{\mathbb{L}} = \mathfrak{B}_1^{e_1^{'}} \cdots \mathfrak{B}_r^{e_r^{'}},$$

e seja d_i o grau de $\overline{\mu}_i$. Como $f(\alpha) = 0$, e como

$$f(X) - \mu_1(X)^{e_1} \cdots \mu_r(X)^{e_r} \in \mathfrak{p}A[X],$$

segue que

$$\mu_1(\alpha)^{e_1} \cdots \mu_r(\alpha)^{e_r} \in \mathfrak{p}\mathbb{A}_{\mathbb{L}}. \tag{2.14}$$

Por outro lado, temos que

$$\mathfrak{B}_i^{e_i} \subset \mathfrak{p}\mathbb{A}_{\mathbb{L}} + \mu_i(\alpha)^{e_i}\mathbb{A}_{\mathbb{L}},$$

consequentemente usando a Equação (2.14) temos que

$$\mathfrak{B}_1^{e_1} \cdots \mathfrak{B}_r^{e_r} \subset \mathfrak{p}\mathbb{A}_{\mathbb{L}} + \mu_1(\alpha)^{e_1} \cdots \mu_r(\alpha)^{e_r}\mathbb{A}_{\mathbb{L}} \subset \mathfrak{p}\mathbb{A}_{\mathbb{L}} = \mathfrak{B}_1^{e_1^{'}} \cdots \mathfrak{B}_r^{e_r^{'}}.$$

Isto prova que $e_i \geq e_i^{'}$ para todo i. Mas sabemos que

$$\sum e_i d_i = \partial f = [\mathbb{L} : \mathbb{K}] = \sum e_i^{'} d_i.$$

Assim $e_i = e_i^{'}$ para todo i, o que prova (2.12). ■

Teorema 2.4.2. *(*Samuel, 1967, p.74, Teo.1*) Se $\mathbb{K}$ é um corpo de números, então um ideal primo $p\mathbb{Z}$ de $\mathbb{Z}$ se ramifica em $\mathbb{K}$ se, e somente se, p divide $D_{\mathbb{K}}$.* ■

Decorre deste resultado que existe apenas um número finito de ideais primos de $\mathbb{Z}$ que se ramificam em $\mathbb{K}$.

Lema 2.4.1. *(*Marcus, 1977, p.78, Corol.*) Sejam ζ_m uma raiz m-ésima da unidade, $n = \varphi(m)$, p um número primo e $O_m(p)$ a ordem de p módulo m. Se p não divide m, então $p\mathbb{Z}[\zeta_m]$ se decompõe em $\frac{n}{O_m(p)}$ ideais primos distintos de $\mathbb{Z}[\zeta_m]$.* ■

Exemplo 2.4.1. *Se $\mathbb{K} = \mathbb{Q}(\sqrt{-17})$, então $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\sqrt{-17}]$ e $f(X) = X^2 + 17$ é o polinômio minimal de $\sqrt{-17}$ sobre $\mathbb{Q}$. Vamos obter a fatoração dos ideais $2\mathbb{A}_{\mathbb{K}}$, $3\mathbb{A}_{\mathbb{K}}$ e $5\mathbb{A}_{\mathbb{K}}$ em produto de ideais primos de $\mathbb{A}_{\mathbb{K}}$ usando o Lema de Kummer. Como*

$$X^2 + 17 \equiv (X+1)^2 (mod\ (\mathbb{Z}/2\mathbb{Z})[X]),$$

segue que

$$g = 1, \quad \overline{\mu_1}(X) = X + 1, \quad e_1 = 2 \quad e \quad f_1 = \partial \overline{\mu_1}(X) = 1$$
$$\mathfrak{p}_1 = 2\mathbb{A}_{\mathbb{K}} + (1 + \sqrt{-17})\mathbb{A}_{\mathbb{K}}.$$

Portanto, $2\mathbb{A}_{\mathbb{K}} = \mathfrak{p}_1^2$, onde $\mathfrak{p}_1$ é o ideal primo de $\mathbb{A}_{\mathbb{K}}$, com $N(\mathfrak{p}_1) = p^{f_1} = 2$. Pela Proposição 2.4.1 segue que $\mathfrak{p}_1$ é o único ideal de $\mathbb{A}_{\mathbb{K}}$ acima do ideal $2\mathbb{Z}$ e é totalmente ramificado em $\mathbb{K}$. Para o ideal $3\mathbb{A}_{\mathbb{K}}$ como

$$X^2 + 17 \equiv (X+1)(X-1) (mod\ (\mathbb{Z}/3\mathbb{Z})[X]),$$

Segue que:

$$g = 2,\ \overline{\mu_1}(X) = X + 1,\ \overline{\mu_2}(X) = X - 1,\ e_1 = e_2 = 1\, e\, f_1 = f_2 = 1.$$
$$\mathfrak{q}_1 = 3\mathbb{A}_{\mathbb{K}} + (1 + \sqrt{-17})\mathbb{A}_{\mathbb{K}} \quad e \quad \mathfrak{q}_2 = 3\mathbb{A}_{\mathbb{K}} + (1 - \sqrt{-17})\mathbb{A}_{\mathbb{K}}.$$

Portanto, $3\mathbb{A}_{\mathbb{K}} = \mathfrak{q}_1\mathfrak{q}_2$ *onde* $\mathfrak{q}_1$ *e* $\mathfrak{q}_2$ *são os únicos ideais primos de* $\mathbb{A}_{\mathbb{K}}$ *acima de* $3\mathbb{Z}$ *com norma 3 e o ideal* $3\mathbb{Z}$ *é totalmente decomposto em* $\mathbb{K}$. *Finalmente, para o ideal* $5\mathbb{A}_{\mathbb{K}}$, *temos que* $X^2 + 17 \equiv X^2 + 2(mod\ (\mathbb{Z}/5\mathbb{Z})[X])$ *e* $X^2 + 2$ *é irredutível sobre* $\mathbb{Z}/5\mathbb{Z}$. *Logo* $5\mathbb{A}_{\mathbb{K}}$ *é um ideal primo de* $\mathbb{A}_{\mathbb{K}}$ *com norma 25 e o ideal* $5\mathbb{Z}$ *é inerte em* $\mathbb{K}$.

Exemplo 2.4.2. *Sejam* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_{15}]$ *o anel de inteiros algébricos de* $\mathbb{K} = \mathbb{Q}(\zeta_{15})$ *e* $f(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$ *o polinômio minimal de* ζ_{15} *sobre* $\mathbb{Q}$. *Vamos obter a fatoração de* $3\mathbb{A}_{\mathbb{K}}$. *Como*

$$f(X) \equiv (X^4 + X^3 + X^2 + X + 1)^2 (mod\ \mathbb{Z}/3\mathbb{Z})[X]),$$

segue que

$$g = 1,\ \overline{\mu_1}(X) = X^4 + X^3 + X^2 + X + 1,\ e_1 = 2\, e\, f_1 = \partial\overline{\mu_1}(X) = 4.$$
$$\mathfrak{p}_1 = 3\mathbb{A}_{\mathbb{K}} + (\zeta_{15}^4 + \zeta_{15}^3 + \zeta_{15}^2 + \zeta_{15} + 1)\mathbb{A}_{\mathbb{K}}.$$

Portanto, $3\mathbb{A}_{\mathbb{K}} = \mathfrak{p}_1^2$, *onde* $\mathfrak{p}_1$ *é o único ideal primo de* $\mathbb{A}_{\mathbb{K}}$ *acima de* $3\mathbb{Z}$ *com norma* 3^4. *Note que neste caso* $3\mathbb{Z}$ *se ramifica em* $\mathbb{K}$, *mas não é totalmente ramificado em* $\mathbb{K}$.

Tendo em vista o Lema 2.4.1 e considerando $\frac{n}{O_m(p)} > 1$, temos que a menor decomposição possível do ideal $p\mathbb{Z}[\zeta_m]$ em produto de ideais primos distintos de $\mathbb{Z}[\zeta_m]$ ocorre primeiramente em $m = 3$ e $p \equiv 1(mod\ 3)$, pois $p\mathbb{Z}[\zeta_3]$ se decompõe em 2 ideais primos distintos de $\mathbb{Z}[\zeta_3]$. Usando o Lema de Kummer vejamos, por exemplo, como se dá a fatoração do ideal $13\mathbb{Z}[\zeta_3]$. Note que $13 \equiv 1(mod\ 3)$ e o

polinômio minimal de ζ_3 sobre $\mathbb{Q}$ é $X^2 + X + 1$. Logo

$$X^2 + X + 1 \equiv (X + 4)(X + 10)(mod\ (\mathbb{Z}/13\mathbb{Z})[X]).$$
$$g = 2,\ \overline{\mu_1}(X) = X + 4,\ \overline{\mu_2}(X) = X + 10,\ e_1 = e_2 = 1,\ f_1 = f_2 = 1.$$

Assim, $13\mathbb{Z}[\zeta_3] = \mathfrak{p}_1\mathfrak{p}_2$, onde $\mathfrak{p}_1 = 13\mathbb{Z}[\zeta_3] + (\zeta_3 + 4)\mathbb{Z}[\zeta_3]$ *e* $\mathfrak{p}_2 = 13\mathbb{Z}[\zeta_3] + (\zeta_3 + 10)\mathbb{Z}[\zeta_3]$.

Agora, sejam $\mathbb{K} \subset \mathbb{L}$ corpos de números com $\mathbb{L}$ uma extensão Galoisiana de $\mathbb{K}$ de grau n. Veremos que em uma extensão Galoisiana a decomposição de um ideal em $\mathbb{A}_{\mathbb{L}}$, dado como no Teorema 2.4.1, assume certas características particulares. Seja G o grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$. Se G for um grupo abeliano diremos que $\mathbb{L}$ é uma extensão abeliana de $\mathbb{K}$.

Observação 2.4.1. *Seja $\mathbb{K}$ um corpo de números. Se $\mathbb{L} = \mathbb{K}(\zeta_m)$, então $\mathbb{L}$ é uma extensão galoisiana de $\mathbb{K}$ e o grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$ é isomorfo a um subgrupo de $(\mathbb{Z}/m\mathbb{Z})^*$.*

Decorre da Observação 2.4.1 que toda extensão ciclotômica de $\mathbb{K}$ é abeliana e, em particular, todo subcorpo de um corpo ciclotômico é uma extensão abeliana de $\mathbb{Q}$. Reciprocamente, se $\mathbb{K}$ é uma extensão abeliana de $\mathbb{Q}$, então existe um inteiro m tal que $\mathbb{K} \subset \mathbb{Q}(\zeta_m)$. Este resultado é conhecido como Teorema de Kronecker-Weber.

Lema 2.4.2. *(*Samuel, 1967, p.89, Lema 1*) Sejam A um anel e $\mathfrak{b}, \mathfrak{p}_1, \cdots, \mathfrak{p}_r$ ideais primos de A tais que $\mathfrak{b}$ não esteja contido em $\mathfrak{p}_i$, para $i = 1, \cdots, r$. Então existe b em $\mathfrak{b}$ tal que b não está em $\mathfrak{p}_i$, para todo $i = 1, \cdots, r$.*

Demonstração. Sem perda de generalidade, podemos considerar o caso em que $\mathfrak{p}_j$ não está contido em $\mathfrak{p}_i$, para $j \neq i$. Tomemos

elementos $x_{ij} \in \mathfrak{p}_j - \mathfrak{p}_i$ (para $j \neq i$, $1 \leq i \; e \; j \leq r$) e elementos $a_i \in \mathfrak{b} - \mathfrak{p}_i$. Se $b_i = a_i \prod_{j \neq i} x_{ij}$, então $b_i \in \mathfrak{b}$, $b_i \in A - \mathfrak{p}_i \, e \, b_i \in \mathfrak{p}_j$, para $j \neq i$. Colocando $b = b_1 + \cdots + b_r$, tem-se que $b \in \mathfrak{b}$ e $b \equiv b_i (mod \; \mathfrak{p}_i)$, isto é, $b \in \mathfrak{b} - \bigcup_{i=1}^{r} \mathfrak{p}_i$ é o elemento procurado. ■

Seja α um elemento de $\mathbb{A}_{\mathbb{L}}$. Aplicando $\sigma \in G$ na equação de dependência inteira de α sobre $\mathbb{A}_{\mathbb{K}}$ temos que $\sigma(\alpha) \in \mathbb{A}_{\mathbb{L}}$, ou seja, $\sigma(\mathbb{A}_{\mathbb{L}}) = \mathbb{A}_{\mathbb{L}}$ para todo $\sigma \in G$. Por outro lado, se $\mathfrak{p}$ é um ideal primo de $\mathbb{A}_{\mathbb{K}}$ e $\mathfrak{q}$ é um ideal primo de $\mathbb{A}_{\mathbb{L}}$ tal que $\mathfrak{q}$ contém $\mathfrak{p}\mathbb{A}_{\mathbb{L}}$ como na Proposição 2.4.1, ou seja, $\mathfrak{q} \cap \mathbb{A}_{\mathbb{K}} = \mathfrak{p}$, então $\sigma(\mathfrak{q}) \cap \mathbb{A}_{\mathbb{K}} = \mathfrak{p}$ para todo $\sigma \in G$, ou seja, $\sigma(\mathfrak{q})$ contém $\mathfrak{p}\mathbb{A}_{\mathbb{L}}$ e tem o mesmo expoente que $\mathfrak{q}$. Neste caso dizemos que $\mathfrak{q}$ e $\mathfrak{q}' = \sigma(\mathfrak{q})$ são ideais primos conjugados contidos em $\mathbb{A}_{\mathbb{L}}$.

Proposição 2.4.2. *(*Samuel, 1967, p.89, Prop.1*) Se $\mathfrak{p}$ é um ideal primo de $\mathbb{A}_{\mathbb{K}}$, então os ideais primos $\mathfrak{p}_i$ de $\mathbb{A}_{\mathbb{L}}$ acima de $\mathfrak{p}$ são dois a dois conjugados, têm o mesmo grau residual f e o mesmo índice de ramificação e. Portanto, $\mathfrak{p}\mathbb{A}_{\mathbb{L}} = \left(\prod_{i=1}^{g} \mathfrak{p}_i \right)^e$ e $n = efg$.*

Demonstração: Suponhamos, por absurdo, que existam ideais primos $\mathfrak{q}$ e $\mathfrak{q}'$ acima de $\mathfrak{p}$ tais que $\sigma(\mathfrak{q}) \neq \mathfrak{q}'$, para todo $\sigma \in G$. Como $\mathfrak{q}$ e $\mathfrak{q}'$ são ideais maximais, podemos supor que $\mathfrak{q}$ não esteja contido em $\sigma(\mathfrak{q}')$, para $\sigma \in G$. Pelo Lema 2.4.2, existe um elemento $\alpha \in \mathfrak{q} - \bigcup_{\sigma \in G} \sigma(\mathfrak{q}')$. Sendo α inteiro sobre $\mathbb{A}_{\mathbb{K}}$, segue que $\sigma(\alpha)$ também é inteiro sobre $\mathbb{A}_{\mathbb{K}}$, de onde $\prod_{\sigma \in G} \sigma(\alpha) = N_{\mathbb{L}/\mathbb{K}}(\alpha)$ é um elemento de $\mathfrak{q}$, e portanto um elemento de $\mathfrak{q} \cap \mathbb{A}_{\mathbb{K}}$.

Por outro lado, $\sigma(\alpha)$ não está em $\mathfrak{q}'$, pois caso contrário teríamos $\sigma^{-1}(\sigma(\alpha)) = \alpha \in \sigma^{-1}(\mathfrak{q}')$, contrariando a hipótese feita sobre α. Dessa forma, $N_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$ não pertence a $\mathfrak{q}'$ (pois $\mathfrak{q}'$ é ideal

primo) e assim $\mathfrak{p}$ não está contido em $\mathfrak{q}$, o que é um absurdo. ■

Exemplo 2.4.3. *Se p é um número primo e $\mathbb{A}_{\mathbb{K}}$ é o anel dos inteiros algébricos de $\mathbb{K} = \mathbb{Q}(\zeta_p)$, então o ideal $p\mathbb{A}_{\mathbb{K}}$ é da forma $p\mathbb{A}_{\mathbb{K}} = (1-\zeta_p)^{p-1}\mathbb{A}_{\mathbb{K}}$. De fato: Se $1 \leq k, j \leq p-1$, então existe um inteiro t, onde $1 \leq t \leq p-1$ tal que $j \equiv kt(mod\ p)$. Assim,*

$$1-\zeta_p^j = 1-(\zeta_p^k)^t = (1-\zeta_p^k)(1+\zeta_p^k+\cdots+(\zeta_p^k)^{t-1}),$$

e portanto, $(1-\zeta_p^k)|(1-\zeta_p^j)$. Analogamente $(1-\zeta_p^j)|(1-\zeta_p^k)$. Assim $1-\zeta_p^j$ e $1-\zeta_p^k$ são associados em $\mathbb{A}_{\mathbb{K}}$. Como $p = \prod_{j=1}^{p-1}(1-\zeta_p^j)$, segue que existe um elemento inversível β em $\mathbb{A}_{\mathbb{K}}$ tal que $p = (1-\zeta_p)^{p-1}.\beta$. Assim, $p\mathbb{A}_{\mathbb{K}} = (1-\zeta_p)^{p-1}\mathbb{A}_{\mathbb{K}}$ e $(1-\zeta_p)\mathbb{A}_{\mathbb{K}}$ é um ideal primo de $\mathbb{A}_{\mathbb{K}}$ e da igualdade fundamental, segue que o grau residual de $(1-\zeta_p)\mathbb{A}_{\mathbb{K}}$ sobre $\mathbb{Z}$ é 1.

Exemplo 2.4.4. *De modo análogo ao Exemplo* 2.4.3*, temos que se p é um número primo, r um número maior que 1 e $\mathbb{A}_{\mathbb{K}}$ o anel dos inteiros algébricos de $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$ então $p\mathbb{A}_{\mathbb{K}} = (1-\zeta_{p^r})^{(p-1)p^{r-1}}\mathbb{A}_{\mathbb{K}}$. Em síntese podemos classificar o ideal primo $p\mathbb{Z}$ como totalmente ramificado em $\mathbb{Q}(\zeta_{p^r})$, com $r \geq 1$.*

Definição 2.4.1. *Seja $\mathfrak{p}$ um ideal primo de $\mathbb{A}_{\mathbb{K}}$. Para cada ideal primo $\mathfrak{q}$ de $\mathbb{A}_{\mathbb{L}}$ satisfazendo $\mathfrak{q} \cap \mathbb{A}_{\mathbb{K}} = \mathfrak{p}$, os conjuntos*

$$D(\mathfrak{q},\mathfrak{p}) = \{\sigma \in G : \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

e

$$E(\mathfrak{q},\mathfrak{p}) = \{\sigma \in G : \sigma(x) \equiv x(mod\ \mathfrak{q}),\ para\ todo\ x \in \mathbb{A}_{\mathbb{L}}\}$$

são subgrupos de G, chamados de **grupo de decomposição** *e* **grupo de inércia** *de $\mathfrak{q}$ com relação a $\mathfrak{p}$, respectivamente.*

Quando $\mathbb{L}$ é uma extensão abeliana de $\mathbb{K}$, os grupos $D(\mathfrak{q}_i, \mathfrak{p})$, para $i = 1, \cdots, g$, onde os $\mathfrak{q}_i's$ são os ideais de $\mathbb{A}_{\mathbb{L}}$ acima de $\mathfrak{p}$, são todos iguais, dependendo somente do ideal $\mathfrak{p}$ de $\mathbb{A}_{\mathbb{K}}$. O mesmo acontece com os grupos $E(\mathfrak{q}_i, \mathfrak{p})$, para $i = 1, \cdots, g$. Em não havendo possibilidade de confusão denotamos tais grupos simplesmente por $D(\mathfrak{p})$ e $E(\mathfrak{p})$.

Se g denota o número de conjugados de $\mathfrak{q}$, então

$$card(G)card(D(\mathfrak{p}))^{-1} = g \text{ ou } card(D(\mathfrak{p})) = \frac{n}{g} = ef$$

Cada $\sigma \in D(\mathfrak{p})$ induz um automorfismo $\widetilde{\sigma}$ de $\mathbb{A}_{\mathbb{L}/\mathfrak{q}}$ tal que $\widetilde{\sigma}(x + \mathfrak{q}) = \sigma(x) + \mathfrak{q}$ (uma vez que o homomorfismo $x \longrightarrow \sigma(x) + \mathfrak{q}$ de $\mathbb{A}_{\mathbb{L}}$ em $\mathbb{A}_{\mathbb{L}}/\mathfrak{q}$ é sobrejetivo e tem núcleo $\mathfrak{q}$). Como $\mathbb{A}_{\mathbb{L}}/\mathfrak{q}$ é uma extensão Galoisiana de grau f de $\mathbb{A}_{\mathbb{K}}/\mathfrak{p}$ ([6], *p.*90, *Prop.*2) e $\widetilde{\sigma}$ fixa o subcorpo $\mathbb{A}_{\mathbb{K}}/\mathfrak{p}$, pois σ fixa $\mathbb{K} \supset \mathbb{A}_{\mathbb{K}}$, concluímos que $\widetilde{\sigma} \in \widetilde{G}$, onde $\widetilde{G}$ denota o grupo de Galois de $\mathbb{A}_{\mathbb{L}}/\mathfrak{q}$ sobre $\mathbb{A}_{\mathbb{K}}/\mathfrak{p}$ e tal grupo é cíclico de ordem f. Além disso, temos que $\sigma \longrightarrow \widetilde{\sigma}$ é um homomorfismo sobrejetor de $D(\mathfrak{p})$ em $\widetilde{G}$ com núcleo $E(\mathfrak{p})$. Com isso, temos a seguinte proposição.

Proposição 2.4.3. *(*Marcus, 1977, p.99*)* $E(\mathfrak{p})$ *é um subgrupo normal de* $D(\mathfrak{p})$ *e* $D(\mathfrak{p})/E(\mathfrak{p}) \longrightarrow \widetilde{G}$ *é um isomorfismo de grupos.*

Como consequência da Proposição 2.4.3 temos que

$$card(\widetilde{G}) = card(D(\mathfrak{p}))card(E(\mathfrak{p}))^{-1}, \text{ ou seja, } card(E(\mathfrak{p})) = e.$$

Exemplo 2.4.5. *Sejam* $\mathbb{K} = \mathbb{Q}(\zeta_{20})$, $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_{20}]$ *e* $f(X) = X^8 - X^6 + X^4 - X^2 + 1$ *o polinômio minimal de* ζ_{20} *sobre* $\mathbb{Q}$. *A decomposição do ideal* $5\mathbb{A}_{\mathbb{K}}$ *em ideais primos de* $\mathbb{A}_{\mathbb{K}}$ *satisfaz:*

$$f(X) \equiv (X+3)^4(X+2)^4 (mod\ (\mathbb{Z}/5\mathbb{Z})[X]).$$

$$g = 2,\ \overline{\mu_1}(X) = X + 3,\ \overline{\mu_2}(X) = X + 2,\ e_1 = e_2 = 4\, e\, f_1 = f_2 = 1.$$

$$\mathfrak{p}_1 = 5\mathbb{A}_{\mathbb{K}} + (\zeta_{20} + 3)\mathbb{A}_{\mathbb{K}} \quad e \quad \mathfrak{p}_2 = 5\mathbb{A}_{\mathbb{K}} + (\zeta_{20} + 2)\mathbb{A}_{\mathbb{K}}.$$

Portanto, $5\mathbb{A}_{\mathbb{K}} = (\mathfrak{p}_1\mathfrak{p}_2)^4$. *O grupo* G *dos automorfismos de* $\mathbb{K}$ *sobre* $\mathbb{Q}$ *é dado por* $G = \{\sigma_i : mdc(i, 20) = 1$ *de forma que* $\sigma_i(\zeta_{20}) = \zeta_{20}^i\} = \{\sigma_1, \sigma_3, \sigma_7, \sigma_9, \sigma_{11}, \sigma_{13}, \sigma_{17}, \sigma_{19}\}$. *Além disso, temos que* $\mathfrak{p}_1$ *e* $\mathfrak{p}_2$ *são conjugados, uma vez que* $\sigma_3(\mathfrak{p}_1) = \mathfrak{p}_2$ *e* $\sigma_3(\mathfrak{p}_2) = \mathfrak{p}_1$. *Logo,* $\mathfrak{p}_1$ *e* $\mathfrak{p}_2$ *são ideais primos conjugados que têm o mesmo índice de ramificação (e=4) e o mesmo grau residual (f=1), conforme a Proposição* 2.4.2. *Visto que* $\mathbb{K}$ *é uma extensão abeliana de* $\mathbb{Q}$, *o grupo de decomposição* $D(5\mathbb{Z})$, *é dado por:*

$$D(5\mathbb{Z}) = \{\sigma \in G : \sigma(\mathfrak{p}_1) = \mathfrak{p}_1\} = \{\sigma_1, \sigma_9, \sigma_{13}, \sigma_{17}\}.$$

Da mesma forma, o grupo de inércia $E(5\mathbb{Z})$ *é dado por:*

$$E(5\mathbb{Z}) = \{\sigma \in G : \sigma(x) \equiv x(mod\ \mathfrak{p}_1), \text{ para todo } x \in \mathbb{A}_{\mathbb{K}}\} = \{\sigma \in D : \sigma(\zeta_{20}) \equiv \zeta_{20}(mod\ \mathfrak{p}_1)\}.$$

Como $card(E(5\mathbb{Z})) = 4$ *e como* $E(5\mathbb{Z})$ *é um subgrupo de* $D(5\mathbb{Z})$ *segue que* $E(5\mathbb{Z}) = D(5\mathbb{Z})$.

Quando tratamos de ideais no anel dos inteiros algébricos do corpo de números $\mathbb{L} = \mathbb{Q}(\zeta_{pq})$ com p e q números primos distintos, a fatoração dos ideais $p\mathbb{A}_{\mathbb{K}}$ ou $q\mathbb{A}_{\mathbb{K}}$ em produto de ideais primos de $\mathbb{A}_{\mathbb{K}}$ assume algumas particularidades interessantes que serão essenciais no próximo capítulo. Sejam $D_{\mathbb{L}}(p)$ o grupo de decomposição de um ideal de $\mathbb{A}_{\mathbb{L}}$ acima de $p\mathbb{Z}$ e $D_{\mathbb{K}}(p)$ o grupo de decomposição de um ideal de $A_{\mathbb{K}}$ acima de $p\mathbb{Z}$ em $\mathbb{K} = \mathbb{Q}(\zeta_q)$.

Observação 2.4.2. *Sejam* $\mathbb{A}_{\mathbb{L}}$ *o anel dos inteiros algébricos de* $\mathbb{L} = \mathbb{Q}(\zeta_{pq})$, $\overline{\sigma}$ *a conjugação complexa de* $\mathbb{Q}(\zeta_{pq})$ *e* $p\mathbb{A}_{\mathbb{L}} = (\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_g)^e$ *como na Proposição* 2.4.2. *Se* $\overline{\sigma}$ *não pertence ao grupo* $D_{\mathbb{L}}(p)$, *então para cada* $i = 1, \cdots, g$, *existe um único índice* k, $k \neq i$, *tal que* $\overline{\sigma}(\mathfrak{p}_i) = \overline{\mathfrak{p}_i} = \mathfrak{p}_k$ *(note que* $\overline{\sigma}(\overline{\mathfrak{p}_i}) = \mathfrak{p}_i$). *Aplicando* $\overline{\sigma}$ *no ideal* $p\mathbb{A}_{\mathbb{L}}$ *temos que*

$$p\mathbb{A}_{\mathbb{L}} = (\overline{\mathfrak{p}_1}\,\overline{\mathfrak{p}_2}\cdots\overline{\mathfrak{p}_g})^e.$$

Podemos supor $\overline{\mathfrak{p}_g} = \mathfrak{p}_1$, $\overline{\mathfrak{p}_{g-1}} = \mathfrak{p}_2, \cdots$ *e assim sucessivamente. Reordenando os ideais de maneira conveniente, obtemos que*

$$p\mathbb{A}_{\mathbb{L}} = (\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_{g/2}\overline{\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_{g/2}})^e.$$

Para saber em que situações teremos a fatoração acima, precisamos caracterizar quando $\overline{\sigma}$ pertence ao grupo de decomposição.

Proposição 2.4.4. *(*Flores, 2000, p.69, Teo.3.5.4*) Com as notações acima, temos que* $\overline{\sigma}$ *pertence a* $D_{\mathbb{L}}(p)$ *se, e somente se,* $\overline{\sigma}$ *pertence a* $D_{\mathbb{K}}(p)$.

Demonstração: Seja $\sigma_s \in D_{\mathbb{K}}(p)$ dado por $\sigma_s(\zeta_q) = \zeta_q^s$. Para cada $\sigma_s \in D_{\mathbb{K}}(p)$, existem $p-1$ automorfismos $\sigma_{s,i}$ de $D_{\mathbb{L}}(p)$ tais que $\sigma_{s,i}(x) = \sigma_s(x)$ para qualquer $x \in \mathbb{Q}(\zeta_q)$. Consideremos u e v tais que $pu + qv = 1$. Como cada $\sigma_{s,i}$ é definido por seu valor em ζ_{pq}, temos:

$$\sigma_{s,i}(\zeta_{pq}) = \sigma_{s,i}(\zeta_{pq}^{pu+qv}) = \sigma_{s,i}(\zeta_{pq}^{pu})\sigma_{s,i}(\zeta_{pq}^{qv}) = \sigma_{s,i}(\zeta_q^u)\sigma_{s,i}(\zeta_p^v) = \zeta_q^{us}\zeta_p^{vi} = \zeta_{pq}^{pus+qvi}.$$

Deste modo, $\overline{\sigma} \in D_{\mathbb{L}}(p)$ se, e somente se, existirem s, i tais que $pus + qvi \equiv -1(mod\ pq)$ e isto é o mesmo que

$$\begin{cases} pus + qvi \equiv -1(mod\ p) \\ pus + qvi \equiv -1(mod\ q). \end{cases}$$

A primeira condição vale sempre pois s pode assumir qualquer valor não nulo módulo p e a segunda condição equivale a $\overline{\sigma} \in D_{\mathbb{K}}(p)$, e isso conclui a demonstração. ■

Corolário 2.4.1. *(*Flores, 2000, p.70, Corol.3.5.5*) A conjugação complexa* $\overline{\sigma}$ *pertence a* $D_{\mathbb{L}}(p)$ *se, e somente se,* $O_q(p) \equiv 0(mod\ 2)$.

Demonstração: Pelo Lema 2.4.1 e pela Proposição 2.4.2 temos que o número g de conjugados de um ideal primo $\mathfrak{q}$ em $\mathbb{Q}(\zeta_q)$, acima de $p\mathbb{Z}$ é $\dfrac{q-1}{O_q(p)}$. Temos que $card(D(\mathfrak{p})) = \dfrac{n}{g}$ e assim, $g = \dfrac{n}{card(D(\mathfrak{p}))}$. Comparando com $g = \dfrac{q-1}{O_q(p)}$, temos que $card(D_{\mathbb{K}}(p)) = O_q(p)$, e assim 2 divide $O_q(p)$. Portanto $O_q(p) \equiv 0(mod\ 2)$. Reciprocamente, suponhamos que $O_q(p) \equiv 0(mod\ 2)$. Como o grupo $D_{\mathbb{K}}(p)$ é cíclico de ordem par, decorre que $\{-1, 1\}$ é o único subgrupo de ordem 2 deste grupo. ■

Exemplo 2.4.6. *Sejam* $\mathbb{L} = \mathbb{Q}(\zeta_{15})$, $p = 3$ *e* $q = 5$. *Como* $O_5(3) = 4$, *pelo Corolário* 2.4.1, *segue que* $\overline{\sigma}$ *está em* $D_{\mathbb{L}}(3)$ *e, portanto, o ideal* $3\mathbb{A}_{\mathbb{L}}$ *não se decompõe segundo a Observação* 2.4.2. *Visto que* $O_3(5) = 2$, *o mesmo ocorre com o ideal* $5\mathbb{A}_{\mathbb{L}}$.

Exemplo 2.4.7. *Sejam* $\mathbb{L} = \mathbb{Q}(\zeta_{57})$, $p = 19$ *e* $q = 3$. *Como* $O_3(19) = 1$, *segue pelo Corolário* 2.4.1, *que* $\overline{\sigma}$ *não pertence a* $D_{\mathbb{L}}(19)$. *Portanto o ideal* $19\mathbb{A}_{\mathbb{L}}$ *se decompõe segundo a Observação* 2.4.2.