4 - Reticulados via corpos quadráticos e ciclotômicos

Carina Alves
Antonio Aparecido de Andrade

ALVES, C., and ANDRADE, AA. Reticulados via corpos quadráticos e ciclotômicos. In: *Reticulados via corpos ciclotômicos* [online]. São Paulo: Editora UNESP, 2014, pp. 135-169. ISBN 978-85-68334-39-3. Available from SciELO Books <http://books.scielo.org>.

4

Reticulados via corpos quadráticos e ciclotômicos

4.1 Introdução

Neste capítulo apresentamos aplicações dos resultados apresentados nos capítulos anteriores, mais precisamente, calculamos a densidade de centro dos reticulados obtidos via o homomorfismo canônico. Visto que a representação geométrica de um ideal é um reticulado, nosso maior desafio no cálculo da densidade de centro é minimizar uma forma quadrática, caracterizada em função do traço. No caso dos corpos quadráticos, caracterizamos a forma quadrática e calculamos a densidade de centro da realização geométrica do anel dos inteiros algébricos e de ideais principais. No caso dos corpos ciclotômicos, apresentamos um estudo da representação geométrica de ideais do anel de inteiros dos corpos ciclotômicos $\mathbb{Q}(\zeta_p)$, $\mathbb{Q}(\zeta_{p^r})$ e $\mathbb{Q}(\zeta_{pq})$, onde p e q são números primos distintos e r é um inteiro positivo não nulo, e seguindo esta

linha nos direcionamos ao estudo de reticulados obtidos via estes corpos.

Visto que, pelo Teorema de Kronecker-Weber, todo corpo de números abeliano está contido em um corpo ciclotômico $\mathbb{Q}(\zeta_n)$, para algum n, estudamos também reticulados via corpos abelianos o que equivale ao estudo da representação geométrica de ideais via subcorpos de corpos ciclotômicos.

4.2 Reticulados via corpos quadráticos

Nesta seção, apresentamos o cálculo da densidade de centro de reticulados de posto 2 no $\mathbb{R}^2$. Pela Proposição 2.2.1, temos que todo corpo quadrático tem a forma $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com d um número inteiro livre de quadrados e que seu anel de inteiros algébricos é $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$ se $d \equiv 2$ ou $3(mod\, 4)$, com $D_{\mathbb{K}} = 4d$ ou $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ se $d \equiv 1(mod\, 4)$ com $D_{\mathbb{K}} = d$.

De acordo com a Observação 3.5.1, temos que

$$\delta(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = \frac{\left(\frac{t_{\mathbb{A}_{\mathbb{K}}}}{4}\right)}{|D_{\mathbb{K}}|^{\frac{1}{2}}}. \tag{4.1}$$

A seguir exemplificamos o cálculo da densidade de centro de alguns reticulados via corpos quadráticos.

Exemplo 4.2.1. *Se* $\mathbb{K} = \mathbb{Q}(\sqrt{7})$ *então* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\sqrt{7}]$ *e* $D_{\mathbb{K}} = 28$. *Se* $\alpha = a + b\sqrt{7} \in \mathbb{A}_{\mathbb{K}}$, *temos que* $\alpha\overline{\alpha} = (a + b\sqrt{7})(a + b\sqrt{7}) = a^2 + 2ab\sqrt{7} + 7b^2$. *Assim,* $Tr(\alpha\overline{\alpha}) = Tr(a^2 + 2ab\sqrt{7} + 7b^2) = Tr(a^2) + Tr(2ab\sqrt{7}) + Tr(7b^2) = 2a^2 + 14b^2 = 2(a^2 + 7b^2)$, *e portanto temos que* $t_{\mathbb{A}_{\mathbb{K}}} = min\{Tr(\alpha\overline{\alpha}); \alpha \neq 0,\ \alpha \in \mathbb{A}_{\mathbb{K}}\} = 2$, *para* $a = 1$ *e* $b = 0$. *Assim,*

$$\delta(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = \frac{1}{2\sqrt{28}} \simeq 0,09449.$$

Exemplo 4.2.2. *Se* $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ *então* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ *e* $D_{\mathbb{K}} = 5$. *Se* $\alpha = a + b\sqrt{5} \in \mathbb{A}_{\mathbb{K}}$, *temos que* $\alpha\overline{\alpha} = (a + b\sqrt{5})(a + b\sqrt{5}) = a^2 + 2ab\sqrt{5} + 5b^2$. *Assim,* $Tr(\alpha\overline{\alpha}) = Tr(a^2 + 2ab\sqrt{5} + 5b^2) = Tr(a^2) + Tr(2ab\sqrt{5}) + Tr(5b^2) = 2a^2 + 10b^2 = 2(a^2 + 5b^2)$, *e daí* $t_{\mathbb{A}_{\mathbb{K}}} = 2$, *para* $a = 1$ *e* $b = 0$. *Portanto,*

$$\delta(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = \frac{1}{2\sqrt{5}} \simeq 0,2236.$$

Consideremos, agora ideais principais do anel dos inteiros algébricos, $\mathbb{A}_{\mathbb{K}}$, de um corpo quadrático $\mathbb{K}$. Seja $\mathfrak{a}$ um ideal não nulo de $\mathbb{A}_{\mathbb{K}}$, tal que $\mathfrak{a} = \gamma\mathbb{A}_{\mathbb{K}}$, onde $\gamma \in \mathbb{A}_{\mathbb{K}}$. Então, pela Proposição 3.5.2, temos que $\sigma_{\mathbb{K}}(\mathfrak{a})$ é um reticulado de posto 2 no $\mathbb{R}^2$ e sua densidade de centro, pela Observação 3.5.1, é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{\left(\frac{t_{\mathfrak{a}}}{4}\right)}{|D_{\mathbb{K}}|^{\frac{1}{2}}|N(\gamma)|}.$$

Exemplo 4.2.3. *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{11})$, $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\sqrt{11}]$ *e* $\mathfrak{a}$ *o ideal principal de* $\mathbb{A}_{\mathbb{K}}$, *gerado por* $\gamma = 1 + 2\sqrt{11}$. *Se* $\alpha \in \gamma\mathbb{A}_{\mathbb{K}}$, *então existem* $a, b \in \mathbb{Z}$ *tais que* $\alpha = (1 + 2\sqrt{11})(a + b\sqrt{11}) = (a + 22b) + (2a+b)\sqrt{11}$. *Assim* $\alpha\overline{\alpha} = (a+22b)^2+11(2a+b^2)+2(a+22b)(2a+b)\sqrt{11}$ *e* $Tr(\alpha\overline{\alpha}) = 2[(a + 22b)^2 + 11(2a + b)^2]$. *Logo* $t_{\mathfrak{a}} = 90$, *para* $a = 1$ *e* $b = 0$. *Como* $D_{\mathbb{K}} = 44$ *e* $N(< 1 + 2\sqrt{11} >) = |N(1 + 2\sqrt{11})| = |(1 + 2\sqrt{11})(1 - 2\sqrt{11})| = |1 - 2\sqrt{11} + 2\sqrt{11} - 44| = |-43| = 43$, *segue que*

$$\begin{aligned}\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) &= \frac{\frac{90}{4}}{\sqrt{44}\cdot 43} = \frac{\frac{90}{4}}{2\cdot\sqrt{11}\cdot 43} = \frac{\frac{90}{4}}{86\cdot\sqrt{11}} = \\ &= \frac{90}{4\cdot\sqrt{11}\cdot 86} = \frac{45}{2\cdot\sqrt{11}\cdot 86} = \frac{45}{172\cdot\sqrt{11}} \simeq 0,0788.\end{aligned}$$

Exemplo 4.2.4. *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{5})$, $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ *e* $\mathfrak{a}$ *o ideal principal de* $\mathbb{A}_{\mathbb{K}}$, *gerado por* $\gamma = 3-2\sqrt{5}$. *Se* $\alpha \in \gamma\mathbb{A}_{\mathbb{K}}$, *então existem* $a, b \in \mathbb{Z}$ *tais que* $\alpha = \left(3a - \frac{7}{2}b\right) + \sqrt{5}\left(-2a + \frac{1}{2}b\right)$. *Assim* $\alpha\overline{\alpha} = \left(3a - \frac{7}{2}b\right)^2 + 5\left(-2a + \frac{1}{2}b\right)^2 + 2\sqrt{5}\left(3a - \frac{7}{2}b\right)\left(-2a + \frac{1}{2}b\right)$ *e portanto,* $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha\overline{\alpha}) = 2\left[\left(3a - \frac{7}{2}b\right)^2 + 5\left(-2a + \frac{1}{2}b\right)^2\right]$. *Logo* $t_{\mathfrak{a}} = 27$, *para* $a = 0$ *e* $b = 1$. *Como* $D_{\mathbb{K}} = 5$ *e* $|N_{\mathbb{K}/\mathbb{Q}}(\gamma)| = 11$ *segue que*

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{27}{44\sqrt{5}} \simeq 0,2744.$$

Proposição 4.2.1. *(*Vicente, 2000, p.72*) Se* $\mathbb{K}$ *é um corpo quadrático totalmente imaginário e* $\mathfrak{a}$ *é um ideal principal do anel dos inteiros algébricos de* $\mathbb{K}$, *então os reticulados* $\sigma_{\mathbb{K}}(\mathfrak{a})$ *e* $\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})$ *tem a mesma densidade de centro.*

Demonstração. Sejam $\mathfrak{a} = \gamma\mathbb{A}_{\mathbb{K}}$ um ideal principal de $\mathbb{A}_{\mathbb{K}}$ e $x \in \mathfrak{a}$, onde $x = \gamma l$, com $l \in \mathbb{A}_{\mathbb{K}}$. Assim, $x\overline{x} = \gamma\overline{\gamma}l\overline{l}$ e $Tr_{\mathbb{K}/\mathbb{Q}}(\gamma\overline{\gamma}) = 2(\gamma\overline{\gamma}l\overline{l})$, pois $\gamma\overline{\gamma}l\overline{l} \in \mathbb{Q}$. Como

$$\frac{\sqrt{\frac{1}{2}Tr_{\mathbb{K}/\mathbb{Q}}(\gamma\overline{\gamma}l\overline{l})}}{2} = \sqrt{\gamma\overline{\gamma}}\cdot\frac{\sqrt{l\overline{l}}}{2},$$

segue que, $\rho(\sigma_{\mathbb{K}}(\gamma\mathbb{A}_{\mathbb{K}})) = |N(\gamma)|\rho(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}}))$ e sendo $\mathbb{K}$ um corpo qua-

drático totalmente imaginário segue que $r_2 = 1$. Portanto,

$$\begin{aligned}\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) &= \frac{2^{r_2}(\rho(\sigma_{\mathbb{K}}(\gamma\mathbb{A}_{\mathbb{K}})))^n}{|D_{\mathbb{K}}|^{\frac{1}{2}}|N(\gamma)|} = \frac{2(\rho(\sigma_{\mathbb{K}}(\gamma\mathbb{A}_{\mathbb{K}})))^2}{|D_{\mathbb{K}}|^{\frac{1}{2}}\dfrac{\rho(\sigma_{\mathbb{K}}(\gamma\mathbb{A}_{\mathbb{K}}))}{\rho(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}}))}} = \\ &= \frac{2(\rho(\sigma_{\mathbb{K}}(\gamma\mathbb{A}_{\mathbb{K}})))^2\rho(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}}))}{|D_{\mathbb{K}}|^{\frac{1}{2}}\rho(\sigma_{\mathbb{K}}(\gamma\mathbb{A}_{\mathbb{K}}))} = \\ &= \frac{2(\rho(\sigma_{\mathbb{K}}(\gamma\mathbb{A}_{\mathbb{K}})))\rho(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}}))}{|D_{\mathbb{K}}|^{\frac{1}{2}}} = \\ &= \frac{2\rho(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}}))^2}{|D_{\mathbb{K}}|^{\frac{1}{2}}} = \delta(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})).\end{aligned}$$

■

Exemplo 4.2.5. *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{-7})$, $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[w]$, $\alpha = a + bw \in \mathbb{A}_{\mathbb{K}}$, *com* $w = \dfrac{11+\sqrt{-7}}{2}$ *e* $\mathfrak{a} = \gamma\mathbb{A}_{\mathbb{K}}$ *um ideal principal de* $\mathbb{A}_{\mathbb{K}}$. *Então* $\alpha\overline{\alpha} = \left[a + b\left(\frac{11}{2} + \frac{\sqrt{-7}}{2}\right)\right]\left[a + b\left(\frac{11}{2} - \frac{\sqrt{-7}}{2}\right)\right] = a^2 + ab\left(\frac{11}{2} - \frac{\sqrt{-7}}{2}\right) + ab\left(\frac{11}{2} + \frac{\sqrt{-7}}{2}\right) + b^2\left(\frac{121}{4} + \frac{7}{4}\right) = a^2 + ab\overline{w} + ab\omega + 32b^2$. *Assim,* $Tr(\alpha\overline{\alpha}) = 2(a^2 + 11ab + 32b^2)$ *e deste modo* $t_{\mathbb{A}_{\mathbb{K}}} = 2$, *para* $a = 1$ *e* $b = 0$. *Visto que* $D_{\mathbb{K}} = -7$, *temos que a densidade de centro é* $\delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \delta(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = \dfrac{\frac{2}{4}}{\sqrt{7}} = \dfrac{\frac{1}{2}}{\sqrt{7}} = \dfrac{1}{2\sqrt{7}} \simeq 0,1889$.

4.3 Reticulados via corpos ciclotômicos

Nesta seção, apresentamos um estudo de como encontrar a maior densidade de centro para os reticulados obtidos via os corpos ciclotômicos $\mathbb{Q}(\zeta_p)$, $\mathbb{Q}(\zeta_{p^r})$ e $\mathbb{Q}(\zeta_{pq})$ onde p e q são números primos distintos e r é um inteiro positivo. Para isso, faremos uso das aplicações das formas quadráticas aos corpos ciclotômicos e desta forma calculamos a densidade de centro dos reticulados obtidos. Além disso, para alguns corpos ciclotômicos calculamos explicitamente a densidade de centro de algumas famílias de reticulados.

1 Reticulados via $\mathbb{Q}(\zeta_p)$.

Nesta seção apresentamos alguns resultados sobre os reticulados obtidos via os corpos ciclotômicos $\mathbb{Q}(\zeta_p)$, onde p é um número primo.

Sejam $\mathbb{K} = \mathbb{Q}(\zeta_p)$, $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$ o anel dos inteiros de $\mathbb{K}$ e $\alpha = \sum_{i=0}^{p-2} a_i\zeta_p^i \in \mathbb{Z}[\zeta_p]$. Como $\overline{\zeta_p} = \zeta_p^{-1}$ segue que $\overline{\alpha} = \sum_{i=0}^{p-2} a_i\zeta_p^{-i}$ e assim,

$$\begin{aligned}\alpha\overline{\alpha} &= \left(\sum_{i=0}^{p-2} a_i\zeta_p^i\right)\left(\sum_{i=0}^{p-2} a_i\zeta_p^{-i}\right) = (a_0^2 + \cdots + a_{p-2}^2) + \\ &+ (a_0a_1 + \cdots + a_{p-3}a_{p-2})(\zeta_p + \zeta_p^{-1}) + \cdots + \\ &+ (a_0a_{p-3} + a_1a_{p-2})(\zeta_p^{p-3} + \zeta_p^{-(p-3)}) + \\ &+ a_0a_{p-2}(\zeta_p^{p-2} + \zeta_p^{-(p-2)}).\end{aligned}$$

Por outro lado, fazendo $\alpha_i = \zeta_p^i + \zeta_p^{-i}$ e $A_i = a_0a_i + a_1a_{i+1} + \cdots + a_{p-2-i}a_{p-2}$, temos que $\alpha\overline{\alpha} = A_0 + A_1\alpha_1 + \cdots + A_{p-2}\alpha_{p-2}$. Como $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha_i) = -2$ segue que $Tr_{\mathbb{K}/\mathbb{Q}}(\alpha\overline{\alpha}) = (p-1)A_0 - 2(A_1 + A_2 + \cdots + A_{p-2}) = (p-1)A_0 - 2(a_0a_1 + \cdots + a_{p-3}a_{p-2} + a_0a_2 + \cdots + a_{p-4}a_{p-2} + \cdots + a_0a_{p-3} + a_1a_{p-2} + a_0a_{p-2})$. Assim,

$$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha\overline{\alpha}) = p\sum_{i=0}^{p-2} a_i^2 - \left[\sum_{i=0}^{p-2} a_i^2 + 2\sum_{0\le i<j\le p-2} a_ia_j\right]$$

e, portanto,

$$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha\overline{\alpha}) = p\sum_{i=0}^{p-2} a_i^2 - \left[\sum_{i=0}^{p-2} a_i\right]^2. \tag{4.2}$$

Fazendo algumas operações no segundo membro da Equação (4.2), temos que

$$Tr_{\mathbb{K}/\mathbb{Q}}(\alpha\overline{\alpha}) = \sum_{i=0}^{p-2} a_i^2 + \sum_{0\le i<j\le p-2} (a_i - a_j)^2, \tag{4.3}$$

que é a forma quadrática $Q_{p-1}(\underline{X})$ calculada em $(a_0, \cdots, a_{p-2})$.

Quando não houver possibilidade de confusão usaremos Q no lugar de Q_{p-1}.

Proposição 4.3.1. *(*Flores, 2000, p.41, Prop.3.1.1*) Sejam* $\mathfrak{p}$ *o ideal de* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$ *gerado por* $1-\zeta_p$, $\alpha \in \mathbb{Z}[\zeta_p]$ *e* $f(X) \in \mathbb{Z}[X]$ *tal que* $\alpha = f(\zeta_p)$. *Então*

$$\alpha \in \mathfrak{p} \Longleftrightarrow f(1) \equiv 0 (mod\ p).$$

Demonstração: Sendo o polinômio minimal de ζ_p sobre $\mathbb{Q}$ dado por

$$h(X) = \frac{X^p - 1}{X - 1},$$

temos que $\mathbb{A}_{\mathbb{K}} \simeq \dfrac{\mathbb{Z}[X]}{< h(X) >}$. Se $\overline{u(X)}$ representa a classe de equivalência, módulo $h(X)$, do polinômio $u(X)$ em $\mathbb{A}_{\mathbb{K}}$, segue que $\alpha \in \mathfrak{p}$ é equivalente à existência de $u(X) \in \mathbb{Z}[X]$ tal que $f(X) \equiv (1 - X)u(X)(mod\ h(X))$ e isto é equivalente à existência de $v(X) \in \mathbb{Z}[X]$ tal que $f(X) = (1 - X)u(X) + v(X)h(X)$. Como

$$h(X) = \frac{X^p - 1}{X - 1} \equiv \frac{(X-1)^p}{X-1} \equiv (X-1)^{p-1} (mod\ p\mathbb{Z}[X]),$$

segue que

$$f(X) \equiv (1 - X)u(X) + v(X)(X-1)^{p-1} (mod\ p\mathbb{Z}[X]).$$

Colocando $1 - X$ em evidência, encontramos $t(X) \in \mathbb{Z}[X]$ tal que

$$f(X) \equiv (1 - X)t(X) (mod\ p\mathbb{Z}[X]),$$

ou seja, existe $g(X) \in \mathbb{Z}[X]$ tal que

$$f(X) = (1 - X)t(X) + p.g(X),$$

e esta igualdade é equivalente à $f(1) \equiv 0 (mod\ p)$. ■

Proposição 4.3.2. *(*Flores, 1996, p.72, Prop.3.4.8*) Se $p > 2$ e $r = 1$ então $Q(\underline{x}) \geq 2p$, onde $x \in \mathfrak{p} = (1 - \zeta_p)\mathbb{A}_{\mathbb{K}}$ e $x \neq 0$. Além disso, $Q(\underline{x}) = 2p$ para $x = 1 - \zeta_p$.*

Demonstração: Seja $x = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$ um elemento de $\mathfrak{p}$ e suponhamos que $(a_0, \cdots, a_{p-2}) \in I_1 = \{(b_1, \cdots, b_n) \in \mathbb{Z}^n, |b_i| \leq 1\}$. Sejam r e s o número de $a_i's$ iguais a 1 e -1, respectivamente. Assim, o número de $a_i's$ nulos será $p - r - s - 1$. Como a forma quadrática $Q(X)$ é totalmente simétrica, segue que

$$\begin{aligned} Q(a_0, \cdots, a_{p-2}) &= Q(1, \cdots, 1, -1, \cdots, -1, 0, \cdots, 0) = \\ &= r + s + 4rs + r(p - 1 - r - s) + s(p - 1 - r - s) = \\ &= r + s + 4rs + rp - r - r^2 - rs + sp - s - sr - s^2 = \\ &= 2rs + rp + sp - r^2 - s^2 = -(r - s)^2 + p(r + s). \end{aligned}$$

Sabemos que quando $x \in \mathfrak{p}$, pela Proposição 4.3.1, $f(1) \equiv 0 (mod\ p)$, ou seja, sendo $f(x) = a_0 + a_1x + \cdots + a_{p-2}x^{p-2}$ segue que $f(1) = a_0 + \cdots + a_{p-2} = \sum_{i=0}^{p-2} a_i = r - s \equiv 0 (mod\ p)$, e consequentemente $r = s$, tendo em vista o intervalo de variação de r e s. Portanto $Q(\underline{x}) = 2pr$ e para $r = 1$ temos que $Q(\underline{x}) = 2p$ é o valor mínimo. Se $(b_0, \cdots, b_{p-2})$ é uma $(p-1)$-upla de $I_2 - I_1$, então pelo Teorema 1.9.1, tomando $a_1 = 2$ e $r = 1$ teremos que $y = \frac{2}{2} = 1$ e assim

$$Q(b_0, \cdots, b_{p-2}) \geq Q(2, 1, \cdots, 1) = 4 + p - 2 + p - 2 = 4 + 2p - 4 = 2p.$$

Pelo Teorema 1.9.2, se $(b_0, \cdots, b_{p-2}) \in I_d - I_{d-1}$, com $d > 1$, segue que

$$Q(b_0, \cdots, b_{p-2}) \geq 2p,$$

o que demonstra a primeira parte da demonstração. Para a segunda parte, se $x = 1 - \zeta_p \in \mathfrak{p}$, então

$$\begin{aligned} Q(\underline{x}) &= Q_{p-1}(1, -1, 0, \cdots, 0) = 1^2 + (-1)^2 + 4 + (p - 3).1 + \\ &+ (p - 3).1 = 6 + p - 3 + p - 3 = 2p - 6 + 6 = 2p, \end{aligned}$$

e isto conclui a demonstração. ■

Nosso objetivo agora é considerar ideais principais não nulos do anel dos inteiros algébricos, $\mathbb{A}_{\mathbb{K}}$, de $\mathbb{K} = \mathbb{Q}(\zeta_p)$ e calcular a densidade de centro da realização geométrica destes ideais. Deste modo, seja $\mathfrak{p} = \lambda\mathbb{A}_{\mathbb{K}}$ o ideal primo de $\mathbb{A}_{\mathbb{K}}$, com $\lambda = 1 - \zeta_p$. Se $\alpha \in \mathfrak{p}$, com $\alpha = \sum_{i=0}^{p-2} a_i\zeta_p^i$ temos que $\alpha \equiv \sum_{i=0}^{p-2} a_i (mod\ \mathfrak{p})$, uma vez que $\zeta_p \equiv 1 (mod\ \mathfrak{p})$. Assim, $\alpha \in \mathfrak{p}$ se, e somente se, $\sum_{i=0}^{p-2} a_i \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Como $1 - \zeta_p \in \mathfrak{p}$, pela Proposição 4.3.2, temos que $Q(1, -1, 0, \cdots, 0) = 2p$, e assim

$$t_{\mathfrak{p}} = min\{Tr_{\mathbb{K}/\mathbb{Q}}(\alpha\overline{\alpha}); \alpha \in \mathfrak{p},\ \alpha \neq 0\} = 2p.$$

Como $N(\mathfrak{p}) = N(\lambda) = p$ e $D_{\mathbb{K}} = \pm p^{p-2}$ segue que

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{p})) = \frac{\left(\frac{2p}{4}\right)^{\frac{p-1}{2}}}{p^{\frac{p-2}{2}}.p} = \frac{p^{\frac{p-1}{2}}}{2^{\frac{p-1}{2}}.p^{\frac{p}{2}}} = \frac{1}{p^{\frac{1}{2}}.2^{\frac{p-1}{2}}}, \tag{4.4}$$

e como $t_{\mathbb{A}_{\mathbb{K}}} = p - 1$ segue, da Proposição 1.9.1, que

$$\delta(\sigma_{\mathbb{K}}(\mathbb{A}_{\mathbb{K}})) = \frac{(p-1)^{\frac{p-1}{2}}}{2^{p-1}.p^{\frac{p-2}{2}}}. \tag{4.5}$$

Exemplo 4.3.1. *O quadro abaixo apresenta o valor aproximado da densidade de centro, $\delta(\sigma_{\mathbb{K}}(\mathfrak{p}))$, da realização geométrica do ideal principal $\mathfrak{p}$ de $\mathbb{Z}[\zeta_p]$ gerado por $1-\zeta_p$, onde p é um número primo:*

p	*dimensão*	*densidade de centro*
3	*2*	$\frac{1}{2\sqrt{3}} \approx 0,288675$
5	*4*	$\frac{1}{4\sqrt{5}} \approx 0,111803$
7	*6*	$\frac{1}{8\sqrt{7}} \approx 0,047245$
11	*10*	$\frac{1}{32\sqrt{11}} \approx 0,009422$
13	*12*	$\frac{1}{64\sqrt{13}} \approx 0,004333$
17	*16*	$\frac{1}{2^8\sqrt{17}} \approx 0,000947404$
19	*18*	$\frac{1}{2^9\sqrt{19}} \approx 0,000448077$
23	*22*	$\frac{1}{2^{11}\sqrt{23}} \approx 0,000101813$
29	*28*	$\frac{1}{2^{14}\sqrt{29}} \approx 0,000011333$
97	*96*	$\frac{1}{2^{48}\sqrt{97}} \approx 3,6072342 \cdot 10^{-16}$
6619	*6618*	$\frac{1}{2^{3309}\sqrt{6619}} \approx 9,57961725 \cdot 10^{-999}$

Tabela (4.3.1)

Observamos que a densidade de centro $0,288675$ *é a maior conhecida em dimensão 2 e corresponde a densidade de centro do reticulados conhecido na literatura* A_2, *(Conway; Sloane, 1999, p.15).*

Passamos agora ao cálculo da densidade de centro de $\sigma_{\mathbb{K}}(\mathfrak{p}^i)$, para $i \geq 1$. Assim, pelas condições para que um elemento de $\mathbb{A}_{\mathbb{K}}$ pertença ao ideal $\mathfrak{p}^i$, precisamos encontrar o mínimo que a forma quadrática assume nos elementos de $\mathfrak{p}^i$ para então calcular a densidade de centro de $\sigma_{\mathbb{K}}(\mathfrak{p}^i)$.

Proposição 4.3.3. *(*Flores, 2000, p.48, Lema.3.2.5*) Sejam* $\mathbb{K} = \mathbb{Q}(\zeta_p)$ *e* $\mathfrak{p} = (1-\zeta_p)\mathbb{Z}[\zeta_p]$. *Se* $x \in \mathfrak{p}^i$, *com* $i = 1, \cdots, (p-1)/2$, *então* $Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) \geq 2.p.i.$ ■

Pela Proposição 4.3.3 e pelo fato da norma ser multiplicativa, temos que

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^i)) \geq \frac{\left(\frac{p.i}{2}\right)^{\frac{p-1}{2}}}{p^{\frac{p-2}{2}}.p^i} = \frac{p^{\frac{p-1}{2}}.\left(\frac{i}{2}\right)^{\frac{p-1}{2}}}{p^{\frac{p-2+2i}{2}}} = \frac{\left(\frac{i}{2}\right)^{\frac{p-1}{2}}}{p^{\frac{p-2+2i}{2}}.p^{\frac{1-p}{2}}} = \frac{\left(\frac{i}{2}\right)^{\frac{p-1}{2}}}{p^{i-\frac{1}{2}}}.$$

Esta expressão admite um limitante mínimo quando $i = \dfrac{p-1}{2\ln p}$. Deste modo, devemos tomar i como sendo um número inteiro próximo de $\dfrac{p-1}{2\ln p}$.

Exemplo 4.3.2. *O quadro abaixo apresenta o valor aproximado da densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathfrak{p}^i)$, $i \geq 1$, onde $\mathfrak{p}^i$ é o ideal principal de $\mathbb{Z}[\zeta_p]$ gerado por $(1-\zeta_p)^i$, onde p é um número primo.*

p	*dimensão*	$\dfrac{p-1}{2\ln p}$	i	$\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^i))$
3	*2*	*0,91*	*1*	*0,288675*
5	*4*	*1,24*	*1*	*0,111803*
7	*6*	*1,54*	*2*	*0,054*
11	*10*	*2,08*	*2*	*0,027*
13	*12*	*2,33*	*3*	*0,021*
17	*16*	*2,82*	*3*	*0,022*
19	*18*	*3,07*	*3*	*0,02443*
23	*22*	*3,5*	*4*	*0,0351*
97	*96*	*10,49*	*10*	*474491823048089,9652*
6619	*6618*	*376,178*	*376*	$3,0254 \cdot 10^{6090}$

Tabela (4.3.2)

Agora veremos uma família de reticulados A_n, para cada dimensão n, a partir de subcorpos de $\mathbb{Q}(\zeta_p)$. Para isto precisamos dos seguintes resultados:

Teorema 4.3.1. *(*Flores; Nóbrega, 1999, p.45, Teo.1*) Sejam p um número primo e $\mathbb{K}$ um subcorpo de $\mathbb{Q}(\zeta_{p^r})$, com $[\mathbb{K}:\mathbb{Q}] = up^j$ e tal que p não divide u. Então*

$$|D_{\mathbb{K}}| = p^{u\left((j+2)p^j - \frac{p^{j+1}-1}{p-1}\right)-1}.$$

Corolário 4.3.1. *(*Flores, 2000, p.22, Corol.2.1.18*) Se $\mathbb{K} \subset \mathbb{Q}(\zeta_p)$, então*

$$|D_{\mathbb{K}}| = p^{[\mathbb{K}:\mathbb{Q}]-1}.$$

Teorema 4.3.2. *(*Flores, 2000, p.50, Teo.3.3.1*) Sejam $\mathbb{L} = \mathbb{Q}(\zeta_p)$, $\mathbb{K}$ um subcorpo de $\mathbb{L}$ de grau $(p-1)/t$ sobre $\mathbb{Q}$, $\mathfrak{p} = (1-\zeta_p)\mathbb{Z}[\zeta_p]$ e $\mathfrak{p}_{\mathbb{K}} = \mathfrak{p} \cap \mathbb{K}$. Então*

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{p}_{\mathbb{K}}^i)) \geq \left(\frac{i}{2}\right)^{\frac{p-1}{2t}} p^{\frac{(1-2i)}{2}}. \tag{4.6}$$

Demonstração: Como $\mathfrak{p}_{\mathbb{K}}$ ramifica totalmente em $\mathbb{L}$, segue que $\mathfrak{p}_{\mathbb{K}}^i\mathbb{Z}[\zeta_p] = \mathfrak{p}^{t.i}$. Pela Proposição 4.3.3, temos que se $x \in \mathfrak{p}_{\mathbb{K}}^i$, para $i = 1, \cdots, (p-1)/2$, então $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \geq 2.p.t.i$. Assim, como $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = Tr_{\mathbb{K}/\mathbb{Q}}(Tr_{\mathbb{L}/\mathbb{K}}(x\overline{x})) = Tr_{\mathbb{K}/\mathbb{Q}}(t(x\overline{x})) = tTr_{\mathbb{K}/\mathbb{Q}}(x\overline{x})$, segue que $Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = \frac{1}{t}Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \geq \frac{1}{t}2.p.t.i = 2.p.i$. Assim, o raio de empacotamento satisfaz

$$\rho \geq \frac{\sqrt{c_{\mathbb{K}}2pi}}{2},$$

onde

$$c_{\mathbb{K}} = \begin{cases} 1, \text{ se } \mathbb{K} \text{ for real;} \\ \frac{1}{2}, \text{ caso contrário.} \end{cases}$$

Pelo Corolário 4.3.1, temos que o discriminante de $\mathbb{K}$ é

$$D_{\mathbb{K}} = \pm p^{\frac{p-1}{t}-1},$$

e como a norma de $\mathfrak{p}_{\mathbb{K}}^i$ é p^i, segue que, a densidade de centro satisfaz

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{p}_{\mathbb{K}}^{i})) = \frac{2^{r_2}\rho(\sigma_{\mathbb{K}}(\mathfrak{p}_{\mathbb{K}}^{i}))^n}{|D_{\mathbb{K}}|^{\frac{1}{2}}N(\mathfrak{p}_{\mathbb{K}}^{i})} \geq \frac{2^{r_2}.(\frac{\sqrt{c_{\mathbb{K}}2pi}}{2})^{\frac{p-1}{t}}}{p^{\frac{p-1-t}{2t}}.p^{i}} = \left(\frac{i}{2}\right)^{\frac{p-1}{2t}} p^{\frac{(1-2i)}{2}}. \quad \blacksquare$$

Usando o software Maple, Flores mostrou que quando p e t são fixados, o maior valor para o limitante inferior na Equação (4.6) é obtido quando i é igual ao inteiro mais próximo de $\dfrac{p-1}{2t\ln p}$.

Se $n \in \mathbb{N} - \{0\}$, então existem infinitos primos p tais que $p \equiv 1(mod\ n)$. Sejam

$$p_n = min\{p \mid p\ \acute{e}\ primo\ e\ p \equiv 1(mod\ n)\}$$

e i_0 o inteiro mais próximo de $\dfrac{p_n - 1}{2t\ln p_n}$, onde $t = \dfrac{p_n - 1}{n}$. Denotamos por A_n a representação geométrica do ideal $\mathfrak{p}_{\mathbb{K}}^{i_0} = \mathfrak{p}^{i_0} \cap \mathbb{K} \subseteq \mathbb{A}_{\mathbb{K}}$, isto é, $A_n = \sigma_{\mathbb{K}}(\mathfrak{p}_{\mathbb{K}}^{i_0})$ onde $\mathbb{K}$ é um subcorpo de $\mathbb{Q}(\zeta_{p_n})$ de grau n sobre $\mathbb{Q}$.

Exemplo 4.3.3. *Como exemplo, mostramos na Tabela 4.3.3, para alguns valores de n, a densidade de centro e o ganho fundamental de codificação, $\gamma_n = \dfrac{d_{E\,min}^2}{Vol(A_n)^{2/n}}$, onde $d_{E,\,min}$ é a distância mínima Euclidiana de A_n.*

n	p_n	$t = \frac{p_n-1}{n}$	$\frac{p_n-1}{2t\ln p_n}$	i_0	$\delta(A_n)$	γ_n
2	*3*	*1*	*0,9*	*1*	*0,288675*	*0.624*
3	*7*	*2*	*0,771*	*1*	*0,133631*	*0.193*
4	*5*	*1*	*1,243*	*1*	*0,111803*	*1.263*
5	*11*	*2*	*1,04*	*1*	*0,0533002*	*0.927*
6	*7*	*1*	*1,5417*	*2*	*0,053994924*	*1.795*
7	*29*	*4*	*1,0394*	*1*	*0,0164133*	*0.921*
8	*41*	*5*	*1,077*	*1*	*0,00976086*	*1.472*
9	*19*	*2*	*1,528*	*2*	*0,0120745*	*1.758*
10	*11*	*1*	*2,085*	*2*	*0,027410122*	*2.896*

Tabela (4.3.3)

Uma das diferenças entre esta família e as demais da literatura, é que as constelações desta família são obtidas para qualquer dimensão.

2 Reticulados via $\mathbb{Q}(\zeta_{p^r})$

Nesta seção apresentamos alguns resultados sobre reticulados obtidos via os corpos ciclotômicos $\mathbb{Q}(\zeta_{p^r})$, onde p é um número primo e $r \geq 1$, $r \in \mathbb{Z}$.

Sejam $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$ e $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_{p^r}]$ o anel dos inteiros de $\mathbb{K}$. Se $x = \sum_{i=0}^{m-1} a_i \zeta_{p^r}^i \in \mathbb{Z}[\zeta_{p^r}]$, onde $m = \varphi(p^r)$, existe uma única representação da forma

$$x = \sum_{j=0}^{t} x_j \zeta_{p^r}^j,$$

onde $t = p^{r-1} - 1$ e

$$x_j = \sum_{i=0,\, i \equiv j (mod\ p^{r-1})}^{m-1} a_i \zeta_{p^r}^i, \text{ para } j = 0, \cdots, t.$$

Observação 4.3.1. *Se* $x = a_0 + a_1\zeta_{p^r} + \cdots + a_{m-1}\zeta_{p^r}^{m-1} \in \mathbb{Z}[\zeta_{p^r}]$, *usamos a expressão*

$$x\overline{x} = A_0 + \sum_{i=1}^{m-1} A_i \alpha_i,$$

onde

$$\alpha_i = \zeta_{p^r}^i + \zeta_{p^r}^{-i} \text{ e } A_j = \sum_{i=0}^{m-(j+1)} a_i a_{j+i}, \text{ para } j = 0, \cdots, m-1.$$

Lema 4.3.1. *(*Flores, 2000, p.43, Teo.3.1.2*) Se p é um número primo e r é um número inteiro positivo, então*

$$Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^k) = \begin{cases} 0, \text{ se } mdc(k, p^r) < p^{r-1}; \\ -p^{r-1}, \text{ se } mdc(k, p^r) = p^{r-1}; \\ p^{r-1}(p-1), \text{ se } mdc(k, p^r) > p^{r-1}. \end{cases}$$

Demonstração: Temos que $(\zeta_{p^r})^{p^s} = e^{\frac{2\pi i p^s}{p^r}} = \zeta_{p^{r-s}}$, e que o polinômio minimal de ζ_{p^r} sobre $\mathbb{Q}$ é dado por

$$X^{(p-1)p^{r-1}} + X^{(p-2)p^{r-1}} + \cdots + X^{p^{r-1}} + 1.$$

Assim se $r \geq 1$ então $Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}) = 0$. Se $mdc(k, p^r) = 1$, então $\zeta_{p^r}^k$ é um conjugado de ζ_{p^r}, ou seja, $\zeta_{p^r}^k$ é raiz do mesmo polinômio minimal e deste modo tem o mesmo traço que ζ_{p^r}. Portanto $Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^k) = 0$. Se $mdc(k, p^r) > 1$, temos três casos a considerar:
1º caso: Se $mdc(k, p^r) = p^s < p^{r-1}$, onde $s \leq r-2$, temos que $p^s | k$ e assim $k = p^s k'$, com $k' \in \mathbb{Z}$. Logo, $\zeta_{p^r}^k = \zeta_{p^r}^{p^s k'} = \zeta_{p^{r-s}}^{k'}$, onde $mdc(p^{r-s}, k') = 1$, e assim

$$\begin{aligned} Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^k) &= Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^{r-s}}^{k'}) = Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^{r-s}}) = \\ &= Tr_{\mathbb{Q}(\zeta_{p^{r-s}})/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}(\zeta_{p^{r-s}})}(\zeta_{p^{r-s}})) = \\ &= p^s Tr_{\mathbb{Q}(\zeta_{p^{r-s}})/\mathbb{Q}}(\zeta_{p^{r-s}}) = p^s.0 = 0. \end{aligned}$$

2º caso: Se $mdc(k, p^r) = p^{r-1}$, temos que $p^{r-1} | k$ e assim $k = p^{r-1}k'$, com $k' \in \mathbb{Z}$. Logo, $\zeta_{p^r}^k = \zeta_{p^r}^{p^{r-1}k'} = \zeta_p^{k'}$, onde $mdc(p, k') = 1$. Como o polinômio minimal de ζ_p sobre $\mathbb{Q}$ é $X^{p-1} + X^{p-2} + \cdots + X + 1$, segue que $Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p) = -1$. Assim,

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

3º caso: Se $mdc(k, p^r) > p^{r-1}$, temos que $mdc(k, p^r) = p^r$ e assim $p^r | k$ o que implica que $k = p^r k'$, com $k' \in \mathbb{Z}$. Deste modo, $\zeta_{p^r}^k = \zeta_{p^r}^{p^r k'} = 1$. Portanto, $Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^k) = Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1) = (p-1)p^{r-1}$. ■

O próximo teorema nos fornece uma relação entre uma forma quadrática com o cálculo de distâncias dos reticulados $\sigma_{\mathbb{K}}(\mathbb{Z}[\zeta_{p^r}])$.

Teorema 4.3.3. *(*Flores, 1996, p.67, Teo.3.4.3*) Sejam p um número primo, r um número inteiro positivo, $n = \varphi(p^r)$ e $x = a_0 + a_1\zeta_{p^r} + \cdots + a_{n-1}\zeta_{p^r}^{n-1}$ um inteiro algébrico de $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$. Então*

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{p^{r-1}}{2}\widetilde{Q}_r(\underline{x}),$$

onde $\underline{x} = (a_0, a_1, \cdots, a_{n-1})$, $\widetilde{Q}_r(\underline{x}) = Q_{p-1}(\underline{x_0}) + \cdots + Q_{p-1}(\underline{x_t})$, com $t = p^{r-1} - 1$ e $\underline{x_k} = (a_k, a_{p^{r-1}+k}, \cdots, a_{(p-2)p^{r-1}+k})$.

Demonstração: Pelo Lema 3.5.3, temos que

$$|\sigma_{\mathbb{K}}(x)|^2 = \tfrac{1}{2}Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}).$$

Pelo Lema 4.3.1, temos que os elementos $\zeta_{p^r}^k$, com $mdc(k, p^r) < p^{r-1}$, tem traço nulo. Se $mdc(k, p^r) > p^{r-1}$ temos que $mdc(k, p^r) = p^r$. Assim, $k = 0$ ou $k \geq p^r > (p-1)p^{r-1}$, o que não ocorre pois $1 \leq k \leq n-1 = (p-1)p^{r-1} - 1$. Deste modo, podemos considerar apenas os índices k tais que $mdc(k, p^r) = p^{r-1}$. Tais k são: $p^{r-1}, 2p^{r-1}, \cdots, (p-2)p^{r-1}$. Tomando $x\overline{x}$ como na Observação 4.3.1 temos que

$$\begin{aligned}
|\sigma_{\mathbb{K}}(x)|^2 &= \frac{1}{2}Tr_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) = \frac{1}{2}\left(Tr_{\mathbb{K}/\mathbb{Q}}(A_0) + \sum_{i=1}^{n-1} Tr_{\mathbb{K}/\mathbb{Q}}(A_i\alpha_i)\right) \\
&= \frac{1}{2}((p-1)p^{r-1}A_0 + Tr_{\mathbb{K}/\mathbb{Q}}(A_1\alpha_1) + \cdots + Tr_{\mathbb{K}/\mathbb{Q}}(A_{n-1}\alpha_{n-1})) \\
&= \frac{1}{2}\left((p-1)p^{r-1}\sum_{i=0}^{n-1} a_i^2 + \cdots + A_{n-1}Tr_{\mathbb{K}/\mathbb{Q}}(\alpha_{n-1})\right) \\
&= \frac{(p-1)}{2}p^{r-1}\left(\sum_{i=0}^{n-1} a_i^2\right) - p^{r-1}\left(\sum_{j=1}^{p-2} A_{jp^{r-1}}\right) \\
&= \frac{p^{r-1}}{2}\left((p-1)\left(\sum_{i=0}^{n-1} a_i^2\right) - 2\sum_{j=1}^{p-2} A_{jp^{r-1}}\right).
\end{aligned}$$

Fazendo

$$(p-1)\left(\sum_{i=0}^{n-1} a_i^2\right) = (p-1)b_0 + \cdots + (p-1)b_t,$$

onde $t = p^{r-1} - 1$ e

$$\begin{cases} b_0 = a_0^2 + a_{p^{r-1}}^2 + \cdots + a_{(p-2)p^{r-1}}^2; \\ b_1 = a_1^2 + a_{p^{r-1}+1}^2 + \cdots + a_{(p-2)p^{r-1}+1}^2; \\ \vdots \\ b_t = a_t^2 + a_{p^{r-1}+t}^2 + \cdots + a_{(p-2)p^{r-1}+t}^2, \end{cases}$$

segue que

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{p^{r-1}}{2}\left((p-1)b_0 + \cdots + (p-1)b_t - 2\sum_{j=1}^{p-2} A_{jp^{r-1}}\right).$$

Temos que $\sum_{j=1}^{p-2} A_{jp^{r-1}} = \sum a_i a_j$, onde a última soma é tomada sobre todos os $a_i s$, para $i = 0, \cdots, n-1$, satisfazendo $i < j$ e $i \equiv j (mod\ p^{r-1})$, uma vez tomando $a_i a_j$ tal que $i < j$ e $i \equiv j (mod\ p^{r-1})$, temos que $p^{r-1} | (i-j)$ o que implica que existe $u \in \{1, \cdots, p-2\}$ tal que $i - j = up^{r-1}$, ou seja, $j = i + up^{r-1}$. Logo $a_i a_j = a_i a_{i+up^{r-1}}$. Como no primeiro somatório, um produto $a_i a_j$ aparece uma única vez, segue a igualdade. Podemos agora reescrever

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{p^{r-1}}{2}((p-1)b_0 - 2d_0 + \cdots + (p-1)b_t - 2d_t),$$

onde $d_k = \sum a_i a_j$, onde $i < j,\ j \equiv k (mod\ p^{r-1})$, e $k = 0, \cdots, t$. Assim

$$(p-1)b_k - 2d_k = Q_{p-1}(a_k, a_{k+p^{r-1}}, \cdots, a_{k+(p-2)p^{r-1}}),$$

para $k = 0, \cdots, t$, o que completa a demonstração. ■

Exemplo 4.3.4. *Sejam $p = 7, r = 1$ e $x = 1 - \zeta_7$ um elemento de $\mathbb{Z}[\zeta_7]$. Se $\underline{x} = (1, -1, 0, 0, 0, 0)$, então $|\sigma_{\mathbb{K}}(x)|^2 = \frac{1}{2}\widetilde{Q_6}(\underline{x}) =$*

$\frac{1}{2}Q_6(1,-1,0,0,0,$
$0) = \frac{1}{2}(1^2+(-1)^2+4.1^2+4.(-1)^2+2^2) = \frac{1}{2}(1+1+4+4+4) = \frac{14}{2} = 7,$
ou seja, $|\sigma_{\mathbb{K}}(x)| = \sqrt{7}$.

Exemplo 4.3.5. *Sejam* $p = 3, r = 2$ *e* $x = 1-\zeta_9$ *um elemento de* $\mathbb{Z}[\zeta_9]$. *Se* $\underline{x} = (1,-1,0,0,0,0)$, *então* $|\sigma_{\mathbb{K}}(x)|^2 = \frac{3}{2}\widetilde{Q_2}(\underline{x}) = \frac{3}{2}(Q_2(1,0)+Q_2(-1,0)+Q_2(0,0)) = \frac{3}{2}(2+2+0) = \frac{12}{2} = 6$, *ou seja,* $|\sigma(x)| = \sqrt{6}$.

Nosso objetivo agora é calcular a densidade de centro de alguns reticulados obtidos via os corpos ciclotômicos $\mathbb{Q}(\zeta_{p^r})$. Primeiramente calculamos a densidade de centro dos reticulados $\sigma(\mathfrak{p}^i)$, $i \geq 1$, onde $\mathfrak{p}$ é um ideal principal de $\mathbb{Z}[\zeta_{p^r}]$ gerado pelo elemento $1-\zeta_{p^r}$. Se $\mathbb{K}$ é um corpo ciclotômico, de grau n, então investigar os reticulados $\sigma_{\mathbb{K}}(\mathfrak{p})$, onde $\mathfrak{p} \subset \mathbb{A}_{\mathbb{K}}$ é um ideal, com densidade de centro máxima equivale a maximizar o quociente $\dfrac{\rho^n}{N(\mathfrak{p})}$, uma vez que a densidade de centro de $\sigma_{\mathbb{K}}(\mathfrak{p})$ é dada por $\dfrac{2^{r_2}\rho^n}{|D_{\mathbb{K}}|^{\frac{1}{2}}N(\mathfrak{p})}$ e os valores 2^{r_2} e $|D_{\mathbb{K}}|^{\frac{1}{2}}$ são determinados.

Proposição 4.3.4. *(*Flores, 1996, p.69, Prop.3.4.4*) Se* $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$ *e* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_{p^r}]$, *a densidade de centro dos reticulados* $\sigma_{\mathbb{K}}(\mathfrak{p}^j)$, *para* $j \in \mathbb{N}$, *é periódica, ou seja,*

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^n)) = \delta(\sigma_{\mathbb{K}}(\mathfrak{p}^{n+m})),$$

onde $m = \varphi(p^r)$ *e* $n \in \mathbb{N}$.

Demonstração: Pelo Exemplo 2.4.3, temos que $\mathfrak{p}^m = p\mathbb{A}_{\mathbb{K}}$, uma vez que p ramifica completamente. Logo, $\mathfrak{p}^{n+m} = \mathfrak{p}^n.\mathfrak{p}^m = p.\mathfrak{p}^n$, o que implica que $N(\mathfrak{p}^{n+m}) = p^{n+m}$. Como $\mathfrak{p}^{n+m} = p.(\mathfrak{p}^n)$ segue que $x \in \mathfrak{p}^{n+m}$ se, e somente se, $x = py$, onde $y \in \mathfrak{p}^n$. Assim

$$\begin{aligned}\widetilde{Q}_r(\underline{x}) &= \frac{2|\sigma(x)|^2}{p^{r-1}} = \frac{2|\sigma(py)|^2}{p^{r-1}} = \frac{2Tr_{\mathbb{K}/\mathbb{Q}}(py\overline{py})}{p^{r-1}} = \frac{2}{p^{r-1}}Tr_{\mathbb{K}/\mathbb{Q}}(p^2y\overline{y}) \\ &= \frac{2}{p^{r-1}}p^2Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) = p^2\frac{2}{p^{r-1}}Tr_{\mathbb{K}/\mathbb{Q}}(y\overline{y}) \\ &= p^2\frac{2}{p^{r-1}}|\sigma(y)|^2 = p^2\widetilde{Q}_r(\underline{y}),\end{aligned}$$

e

$$\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^n)) = min\left\{\frac{|\sigma(x)|}{2};\ x \in \mathfrak{p}^n\right\}$$

$$\begin{aligned}\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^{n+m})) &= min\left\{\frac{|\sigma(x)|}{2};\ x \in \mathfrak{p}^{n+m}\right\} = min\left\{\frac{|\sigma(x)|}{2};\ x \in p.\mathfrak{p}^n\right\} \\ &= p.\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^n)).\end{aligned}$$

Para a densidade de centro, temos que

$$\begin{aligned}\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^{n+m})) &= \frac{2^{r_2}(\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^{n+m})))^m}{|D_{\mathbb{K}}|^{\frac{1}{2}}.p^{n+m}} = \frac{2^{r_2}(p.\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^n)))^m}{|D_{\mathbb{K}}|^{\frac{1}{2}}.p^{n+m}} = \\ &= \frac{2^{r_2}p^m(\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^n)))^m}{|D_{\mathbb{K}}|^{\frac{1}{2}}.p^n.p^m} = \frac{2^{r_2}(\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^n)))^m}{|D_{\mathbb{K}}|^{\frac{1}{2}}.p^n} = \delta(\sigma_{\mathbb{K}}(\mathfrak{p}^n)).\blacksquare\end{aligned}$$

A próxima proposição é uma generalização da Proposição 4.3.1

Proposição 4.3.5. *(*Flores, 2000, p.41, Prop.3.1.1*) Sejam* $\mathfrak{p}$ *o ideal de* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_{p^r}]$ *gerado por* $1-\zeta_{p^r}$, $\alpha \in \mathbb{Z}[\zeta_{p^r}]$ *e* $f(X) \in \mathbb{Z}[X]$ *tal que* $\alpha = f(\zeta_{p^r})$. *Então*

$$\alpha \in \mathfrak{p}^{i+1} \Longleftrightarrow f(1) \equiv f'(1) \equiv \cdots \equiv f^{(i)}(1) \equiv 0 (mod\ p),$$

onde $f^{(i)}(X)$ *denota a i-ésima derivada formal de* f, $0 \leq i < m$, *e* $m = \varphi(p^r)$.

Demonstração: Sendo o polinômio minimal de ζ_{p^r} sobre $\mathbb{Q}$ dado por

$$h(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1},$$

temos que $\mathbb{A}_{\mathbb{K}} \simeq \dfrac{\mathbb{Z}[X]}{< h(X) >}$. Se $\overline{u(X)}$ representa a classe de equivalência, módulo $h(X)$, do polinômio $u(X)$ em $\mathbb{A}_{\mathbb{K}}$, segue que $\alpha \in \mathfrak{p}^{i+1}$ é equivalente à existência de $u(X) \in \mathbb{Z}[X]$ tal que $f(X) \equiv (1 - X)^{i+1}u(X)$
$(mod\ h(X))$ e isto é equivalente à existência de $v(X) \in \mathbb{Z}[X]$ tal que $f(X) = (1 - X)^{i+1}u(X) + v(X)h(X)$. Como

$$h(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} \equiv \frac{(X-1)^{p^r}}{(X-1)^{p^{r-1}}} \equiv (X-1)^{p^r - p^{r-1}} \equiv (X-1)^{(p-1)p^{r-1}} (mod\ p\mathbb{Z}[X]),$$

segue que

$$f(X) \equiv (1 - X)^{i+1}u(X) + v(X)(X-1)^{(p-1)p^{r-1}} (mod\ p\mathbb{Z}[X]).$$

Colocando $(1 - X)^{i+1}$ em evidência, encontramos $t(X) \in \mathbb{Z}[X]$ tal que

$$f(X) \equiv (1 - X)^{i+1}t(X) (mod\ p\mathbb{Z}[X]),$$

ou seja, existe $g(X) \in \mathbb{Z}[X]$ tal que

$$f(X) = (1 - X)^{i+1}t(X) + p.g(X),$$

e esta igualdade é equivalente à

$$f(1) \equiv f^{'}(1) \equiv \cdots \equiv f^{(i)}(1) \equiv 0 (mod\ p). \qquad \blacksquare$$

Proposição 4.3.6. *(*Flores, 1996, p.72, Prop.3.4.8*) Se* $r > 1$ *então* $\widetilde{Q}_r(\underline{x}) \geq 2(p-1)$, *para* $x \in \mathfrak{p} = (1 - \zeta_{p^r})\mathbb{A}_{\mathbb{K}}$ *e* $x \neq 0$. *Além disso,* $\widetilde{Q}_r(\underline{x}) = 2(p-1)$ *para* $x = 1 - \zeta_{p^r}$.

Demonstração: Se $x = a_0 + a_1\zeta_{p^r} + \cdots + a_{m-1}\zeta_{p^r}^{m-1} \in \mathbb{Z}[\zeta_{p^r}]$, onde $m = \varphi(p^r)$ e então podemos escrevê-lo de uma única maneira como $x = x_0 + x_1\zeta_{p^r} + \cdots + x_t\zeta_{p^r}^t$, onde $t = p^{r-1} - 1$ e

$$\begin{cases} x_0 = a_0 + a_{p^{r-1}}.\zeta_{p^r}^{p^{r-1}} + \cdots + a_{(p-2)p^{r-1}}.\zeta_{p^r}^{(p-2)p^{r-1}}; \\ x_1 = a_1 + a_{p^{r-1}+1}.\zeta_{p^r}^{p^{r-1}+1} + \cdots + a_{(p-2)p^{r-1}+1}.\zeta_{p^r}^{(p-2)p^{r-1}+1}; \\ \vdots \\ x_t = a_t + a_{p^{r-1}+t}.\zeta_{p^r}^{p^{r-1}+t} + \cdots + a_{(p-2)p^{r-1}+t}.\zeta_{p^r}^{(p-2)p^{r-1}+t}. \end{cases}$$

Assim pelo Teorema 4.3.3, temos que

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{p^{r-1}}{2}.\widetilde{Q}_r(\underline{x}) = \frac{p^{r-1}}{2}\left(Q(\underline{x_1}) + \cdots + Q(\underline{x_t})\right).$$

Se $x \in \mathfrak{p}$ e se existir um único x_j não nulo na decomposição acima, então $Q(\underline{x_j}) \geq 2p$, e portanto $\widetilde{Q}_r(\underline{x}) \geq 2p > 2(p-1)$. Visto que $p-1$ é o menor valor que $Q(\underline{a})$ assume, com $\underline{a} \in \mathbb{Z}^{p-1}$, segue que se o número dos $a_i's$ não nulos for maior que 1, então

$$\widetilde{Q}_r(\underline{x}) \geq 2(p-1).$$

Finalmente, temos que o elemento $x = 1 - \zeta_{p^r} \in \mathfrak{p}$ satisfaz $\widetilde{Q}_r(\underline{x}) = 2(p-1)$ e isto conclui a demonstração. ■

Lema 4.3.2. *(*Flores, 1996, p.75, Lema.3.4.11*) O elemento* $1-\zeta_{p^r}^{p^{r-2}}$ *pertence a* $\mathfrak{p}^{p^{r-2}}$.

Demonstração: Sendo $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_{p^r}]$, vimos que

$$p\mathbb{A}_{\mathbb{K}} = (1-\zeta_{p^r})^{(p-1)p^{r-1}}\mathbb{A}_{\mathbb{K}},$$

uma vez que p se ramifica totalmente em $\mathbb{A}_{\mathbb{K}}$. Sejam $c_i = \begin{pmatrix} p^{r-2} \\ i \end{pmatrix}$, com $0 \leq i \leq p^{r-2}$, os coeficientes do desenvolvimento binomial de $(1-\zeta_{p^r})^{p^{r-2}}$. Pela Proposição 1.9.3, para $i = 1, \cdots, p^{r-2}-1$, temos que $v_p(c_i) \geq 1$, ou seja, p é um divisor de $(1-\zeta_{p^r})^{p^{r-2}} - (1-\zeta_{p^r}^{p^{r-2}})$. Consequentemente,

$$1-\zeta_{p^r}^{p^{r-2}} \equiv (1-\zeta_{p^r})^{p^{r-2}} (mod\ \mathfrak{p}^{(p-1)p^{r-1}}),$$

o que implica que

$$1-\zeta_{p^r}^{p^{r-2}} \equiv (1-\zeta_{p^r})^{p^{r-2}} (mod\ \mathfrak{p}^{p^{r-2}}).$$

Como $\mathfrak{p}^{p^{r-2}} = p\mathbb{A}_{\mathbb{K}} = (1-\zeta_{p^r})^{p^{r-2}}\mathbb{A}_{\mathbb{K}}$ então $(1-\zeta_{p^r})^{p^{r-2}} \in \mathfrak{p}^{p^{r-2}}$. Assim $1-\zeta_{p^r}^{p^{r-2}} \equiv 0\, mod\ \mathfrak{p}^{p^{r-2}}$ e portanto $1-\zeta_{p^r}^{p^{r-2}} \in \mathfrak{p}^{p^{r-2}}$. ■

Teorema 4.3.4. *(Flores, p.47, Teo.3.2.3) Se $r > 2$ e $\mathfrak{p} = (1-\zeta_{p^r})\mathbb{A}_{\mathbb{K}}$ então a maior densidade de centro entre os reticulados $\sigma_{\mathbb{K}}(\mathfrak{p}^i)$, para $i = 1, \cdots, p^{r-2}$, ocorre com $i = 1$.*

Demonstração: Pelo Lema 4.3.2 temos que o elemento $x = 1-\zeta_{p^r}^{p^{r-2}}$ pertence a $\mathfrak{p}^{p^{r-2}}$ e além disso temos que $\widetilde{Q}_r(\underline{x}) = 2(p-1)$. Assim, para $i = 1, \cdots, p^{r-2}$, temos que

$$\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^i)) = \frac{\sqrt{(p-1)p^{r-1}}}{2},$$

e as densidades de centro são dadas por

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^i)) = \frac{((p-1)p^{r-1})^{n/2}}{2^{n/2}.|D_{\mathbb{K}}|^{\frac{1}{2}}.p^i},$$

onde $n = \varphi(p^r)$ e $|D_{\mathbb{K}}| = p^{p^{r-1}(pr-r-1)}$. Isto mostra que $\sigma_{\mathbb{K}}(\mathfrak{p})$ tem a maior densidade de centro dentre os reticulados considerados. ■

Exemplo 4.3.6. *O quadro abaixo apresenta o valor aproximado para a densidade de centro $\delta(\sigma_{\mathbb{K}}(\mathfrak{p}))$, onde $\mathfrak{p}$ é um ideal principal de $\mathbb{Z}[\zeta_{p^r}]$ gerado por $1-\zeta_{p^r}$, p é um número primo e $r > 2$.*

p	r	*dimensão*	*densidade de centro*
2	3	4	$\frac{1}{8} = 0,125$
2	4	8	$\frac{1}{32} = 0,03125$
3	3	18	$\frac{1}{3^{28}} \approx 4,37.10^{-14}$

O valor $0,125$ *obtido para a densidade de centro em dimensão 4 é o maior encontrado para esta dimensão, e corresponde a densidade de centro do reticulado conhecido na literatura* $\boldsymbol{D}_4$, *(Conway; Sloane, 1999, p.15).*

Teorema 4.3.5. *(Flores, p.47, Teo.3.2.4) Se* $r = 2$, $p > 2$ *e* $\mathfrak{p} = (1-\zeta_{p^r})\mathbb{A}_{\mathbb{K}}$ *então a maior densidade de centro entre os reticulados* $\sigma_{\mathbb{K}}(\mathfrak{p}^i)$, *para* $i = 1, \cdots, p$, *ocorre com* $i = 2$.

Demonstração: Mostramos que para $i = 2, \cdots, p$, o menor valor assumido por $\widetilde{Q_r}(\underline{x})$ para $x \in \mathfrak{p}^i$ é 2p. Consideramos primeiramente o caso $i = 2$ e sejam x um elemento de $\mathfrak{p}^2$ e os $x_i's$ como na Proposição 4.3.6. Se apenas um dos $x_i's$ não se anula, então, pela Proposição 4.3.2, temos que $\widetilde{Q_r}(\underline{x}) \geq 2p$, para $x \in \mathfrak{p}$. Para $\underline{a} \in \mathbb{Z}^{p-1}$ temos que o menor valor que $Q(\underline{a})$ assume é $p-1$. Assim, se o número dos $x_i's$ não nulos for maior do que 2, então $\widetilde{Q_r}(\underline{x}) \geq 3(p-1) \geq 2p$, uma vez que, $\widetilde{Q_r}(\underline{x}) = Q_{p-1}(\underline{x_0}) + \cdots + Q_{p-1}(\underline{x_t})$, com $t = p^{r-1} - 1$, e portanto $\widetilde{Q_r}(\underline{x}) = Q_{p-1}(a_0, a_{p^{r-1}}, \cdots, a_{(p-2)p^{r-1}}) + \cdots + Q_{p-1}(a_t, a_{p^{r-1}+t}, \cdots, a_{(p-2)p^{r-1}+t}) \geq p-1+p-1+p-1 = 3(p-1) \geq 2p$. Deste modo, falta considerar o caso em que apenas dois dos $x_i's$ não se anulam, digamos x_i e x_j. Mostraremos, primeiramente, que neste caso $\widetilde{Q_r}(\underline{x})$ não atinge o valor $2(p-1)$. Se isto ocorre, temos que $Q(\underline{x_i}) = Q(\underline{x_j}) = p-1$ e isto ocorre apenas nos casos seguintes:
1°*caso* : Se $\underline{x_i} = \pm e_l$ e $\underline{x_j} = \pm e_s$, podemos supor, sem perda de generalidade, que $\underline{x_i} = e_l$ e $\underline{x_j} = -e_s$. Logo existem $a, b \in \mathbb{N}$ tais que

$$x = \zeta_{p^r}^i x_i + \zeta_{p^r}^j x_j = \zeta_{p^r}^a - \zeta_{p^r}^b = f(\zeta_{p^r}),$$

onde $f(X) = X^a - X^b$. Como $x \in \mathfrak{p}^2$, segue que, pela Proposição 4.3.5, *que*

$$f'(1) \equiv a - b \equiv 0 (mod\ p).$$

Observe que $x = \zeta_{p^r}^a(1-\zeta_{p^r}^{b-a})$. Como estamos considerando apenas dois dos $x_i's$ não nulos, segue que $a - b \equiv 0(mod\ p)$ não ocorre, o que é uma contradição.

$2^{\underline{o}}$ *caso* : Se $\underline{x_i} = (1, 1, \cdots, 1)$ e $\underline{x_j} = \pm e_s$, temos que se $x \in \mathfrak{p}$ então $\underline{x_j} = e_s$. Logo x é da forma

$$x = \zeta_{p^r}^i x_i + \zeta_{p^r}^j x_j = \zeta_{p^r}^i + \zeta_{p^r}^{p+i} + \cdots + \zeta_{p^r}^{(p-2)p+i} + \zeta_{p^r}^{j+s} = f(\zeta_{p^r}),$$

onde $f(X) = X^i + \cdots + X^{j+s}$. Se $x \in \mathfrak{p}^2$, pela Proposição 4.3.5, temos que

$$f'(1) \equiv i + \cdots + (p-2)p + i + j + s \equiv i - j \equiv 0(mod\ p),$$

o que não ocorre, pois $i, j \in \{0, \cdots, p-1\}$.

$3^{\underline{o}}$ *caso* : Se $\underline{x_i} = (1, 1, \cdots, 1)$ e $\underline{x_j} = \pm(-1, -1, \cdots, -1)$, temos que $\underline{x_j} = (-1, -1, \cdots, -1)$ e

$$x = \zeta_{p^r}^i x_i + \zeta_{p^r}^j x_j = \zeta_{p^r}^i + \zeta_{p^r}^{p+i} + \cdots + \zeta_{p^r}^{(p-2)p+i} - \zeta_{p^r}^j - \cdots - \zeta_{p^r}^{(p-2)p+j} = f(\zeta_{p^r}),$$

onde $f(X) = X^i + \cdots + X^{(p-2)p+i} - X^j + \cdots + X^{(p-2)p+j}$. Se $x \in \mathfrak{p}^2$, então

$$f'(1) \equiv i - j \equiv 0(mod\ p),$$

o que novamente não ocorre.

Mostramos, assim, que para $x \in \mathfrak{p}^2$ e dois $x_i's$ não nulos, o valor $2(p-1)$ não é atingido por $\widetilde{Q}_r(\underline{x})$. Mas, pelo Lema 1.9.2, o valor $2p-1$ também não é atingido e portanto para $x \in \mathfrak{p}^2$ temos que $\widetilde{Q}_r(x) \geq 2p$. Observe que o elemento $x = 1 - \zeta_{p^r}^p$ pertence a $\mathfrak{p}^i$, para $i = 1, \cdots, p$, e $\widetilde{Q}_r(\underline{x}) = 2p$. Como $|\sigma_{\mathbb{K}}(x)|^2 = \dfrac{p^{r-1}}{2}.\widetilde{Q}_r(\underline{x})$, segue que

$$|\sigma_{\mathbb{K}}(x)|^2 = \frac{p^{r-1}}{2}.2p = p^r,$$

o que implica que $\rho(\sigma_{\mathbb{K}}(\mathfrak{p}^i)) = \frac{1}{2} min\{|\sigma(x)|,\ x \neq 0,\ x \in \mathfrak{p}^i\} = \frac{\sqrt{p^r}}{2}$, para $i = 1, 2, \cdots, p$. Como o ideal de menor norma é $\mathfrak{p}^2$, segue que $\sigma_{\mathbb{K}}(\mathfrak{p}^2)$ tem a maior densidade de centro. Assim, para $i = 1, \cdots, p$, a maior densidade de centro é obtida em $\sigma_{\mathbb{K}}(\mathfrak{p})$ ou $\sigma_{\mathbb{K}}(\mathfrak{p}^2)$. Para $r = 2$, temos que

$$\frac{\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^2))}{\delta(\sigma_{\mathbb{K}}(\mathfrak{p}))} = \left(\frac{p}{p-1}\right)^{\frac{(p-1)p}{2}-1} > 1.$$

Logo, $\sigma_{\mathbb{K}}(\mathfrak{p}^2)$ é o mais denso dentre os reticulados considerados, e sua densidade de centro é dada por

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^2)) = \frac{p^{(p-1)p}}{2^{\frac{(p-1)p}{2}}.|D_{\mathbb{K}}|^{\frac{1}{2}}.p^2}.$$ ■

Exemplo 4.3.7. *Se* $\mathbb{A}_{\mathbb{K}} = \mathbb{Z}[\zeta_{3^2}]$ *e* $\mathfrak{p} = (1 - \zeta_{3^2})\mathbb{A}_{\mathbb{K}}$, *então*

$$\delta(\sigma_{\mathbb{K}}(\mathfrak{p}^2)) = \frac{1}{8\sqrt{3}} \approx 0,072168.$$

Note que $\mathbb{A}_{\mathbb{K}}$ *tem dimensão 6 e que o reticulado* $\sigma_{\mathbb{K}}((1-\zeta_{3^2})^2\mathbb{Z}[\zeta_{3^2}])$ *apresenta maior densidade de centro que o reticulado* $\sigma_{\mathbb{K}}((1 - \zeta_7)\mathbb{Z}[\zeta_7])$, *(Exemplo* 4.3.1*) e o reticulado* $\sigma_{\mathbb{K}}((1-\zeta_7)^2\mathbb{Z}[\zeta_7])$, *(Exemplo* 4.3.2*). Para esta dimensão temos que* $0,072168$ *é o maior valor conhecido para a densidade de centro e corresponde a densidade de centro do reticulado conhecido na literatura* E_6,*(Conway; Sloane, p.15).*

3 Reticulados via $\mathbb{Q}(\zeta_{pq})$

Nesta seção apresentamos alguns resultados sobre reticulados obtidos via os corpos ciclotômicos $\mathbb{Q}(\zeta_{pq})$, onde p e q são primos distintos.

Lema 4.3.3. *(Flores, p.64, Lema.3.5.1) Se p e q são números distintos então*

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^k) = \begin{cases} 1, & se\ mdc(k,pq)=1; \\ 1-p, & se\ mdc(k,pq)=p; \\ 1-q, & se\ mdc(k,pq)=q; \\ (1-p)(1-q), & se\ mdc(k,pq)=pq. \end{cases}$$

Demonstração: Suponhamos que $mdc(k,pq)=1$. Como $mdc(p,q)=1$, segue que existem inteiros r, s tais que que $pr+qs=1$. Deste modo,

$$\zeta_{pq}^k = \zeta_{pq}^{k(pr+qs)} = \zeta_{pq}^{kpr+kps} = \zeta_{pq}^{kpr}.\zeta_{pq}^{kqs} = \zeta_q^{kr}.\zeta_p^{ks},$$

onde $mdc(kr,q)=mdc(ks,p)=1$. Então

$$\begin{aligned} Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^k) &= Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_q^{kr}.\zeta_p^{ks}) \\ &= Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_p)}(\zeta_q^{kr}.\zeta_p^{ks})) \\ &= Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^{ks}Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_p)}(\zeta_q^{kr})) \\ &= Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^{ks}.Tr_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(\zeta_q^{kr})) \\ &= Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(-\zeta_p^{kr}) = 1. \end{aligned}$$

Se $mdc(k,pq)=p$, então existe $i\in\mathbb{Z}$, com $mdc(i,q)=1$, tal que

$$\zeta_{pq}^k = \zeta_{pq}^{pi} = \zeta_q^i.$$

Logo,

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^k) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_p)}(\zeta_q^i)) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(-1) = 1-p.$$

Se $mdc(k,pq)=q$, então existe $i\in\mathbb{Z}$, com $mdc(i,p)=1$, tal que

$$\zeta_{pq}^k = \zeta_{pq}^{qi} = \zeta_p^i.$$

Logo,

$$\begin{aligned} Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^k) &= Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_p)}(\zeta_p^i)) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^i(q-1)) = \\ &= (q-1)Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^i) = (q-1)(-1) = 1-q. \end{aligned}$$

Se $mdc(k, pq) = pq$, então existe $i \in \mathbb{Z}$, tal que $\zeta_{pq}^k = \zeta_{pq}^{pqi} = 1$. Logo,

$$\begin{aligned} Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^k) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_p)}(1)) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(q-1) = \\ (q-1)(p-1). \end{aligned}$$

■

Corolário 4.3.2. *(Flores, p.65, Corol.3.5.2) Se* $0 \leq i \leq pq$ *então*

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}((1-\zeta_{pq}^p-\zeta_{pq}^q+\zeta_{pq}^{p+q}).\zeta_{pq}^i) = \begin{cases} pq, \text{ se } i = 0 \text{ ou } i = pq-p-q; \\ -pq \text{ se } i = pq-p \text{ ou } i = pq-q; \\ 0, \text{ caso contrário.} \end{cases}$$

Demonstração: Se $mdc(i, pq) = 1$, então

$$(1-\zeta_{pq}^p-\zeta_{pq}^q+\zeta_{pq}^{p+q}).\zeta_{pq}^i = \zeta_{pq}^i-\zeta_{pq}^{p+i}-\zeta_{pq}^{q+i}+\zeta_{pq}^{p+q+i},$$

sendo que o expoente de cada parcela é primo com pq. Logo, o traço de cada uma dessas parcelas é 1. Assim

$$\begin{aligned} &Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}((1-\zeta_{pq}^p-\zeta_{pq}^q+\zeta_{pq}^{p+q}).\zeta_{pq}^i) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^i) - Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{p+i}) \\ &-Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{q+i}) + Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{p+q+i}) = 1-1-1+1 = 0. \end{aligned}$$

Para $i = 0$, aplicando o Lema 4.3.3 temos que

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}((1-\zeta_{pq}^p-\zeta_{pq}^q+\zeta_{pq}^{p+q})) = (p-1)(q-1)+p-1+q-1+1 = pq.$$

Para $i = pq-p$, temos que

$$\begin{aligned} &Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}((1-\zeta_{pq}^p-\zeta_{pq}^q+\zeta_{pq}^{p+q}).\zeta_{pq}^{pq-p}) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{pq-p}-1-\zeta_{pq}^{pq-p+q} \\ &-\zeta_{pq}^{q+pq}) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{p(q-1)}-1-\zeta_{pq}^{-p+q}+\zeta_{pq}^{q(1+p)}) = 1-p-(1-p) \\ &(1-q)-1+1-q = 1-p-pq+p+q-1-1+1-q = -pq. \end{aligned}$$

Analogamente para $i = pq - q$, temos que $Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}((1 - \zeta_{pq}^{p} - \zeta_{pq}^{q} + \zeta_{pq}^{p+q}).\zeta_{pq}^{pq-q}) = -pq$. Para $i = pq - p - q$ temos que

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}((1 - \zeta_{pq}^{p} - \zeta_{pq}^{q} + \zeta_{pq}^{p+q}).\zeta_{pq}^{pq-p-q}) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{pq-p-q} - \zeta_{pq}^{pq-q} - \zeta_{pq}^{pq-p} + \zeta_{pq}^{pq}) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{-p-q} - \zeta_{pq}^{q(p-1)} - \zeta_{pq}^{p(q-1)} + 1) = 1 - (1 - q) - (1 - p) + (1 - p)(1 - q) = pq,$$

e isto conclui a demonstração. ∎

Proposição 4.3.7. *(*Simonato, 2000, p.47, Prop.3.3.8*) Se p e q são números primos distintos, $n = \varphi(pq)$ e x é um elemento de $\mathbb{Z}[\zeta_{pq}]$, com $x = a_0 + a_1\zeta_{pq} + \cdots + a_{n-1}\zeta_{pq}^{n-1}$, então*

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(x\overline{x}) = (p-1)(q-1)A_0 + 2(1-p)\sum_{p|k} A_k + 2(1-q)\sum_{q|k} A_k + 2\sum_{p\nmid k,\, q\nmid k} A_k,$$

onde $A_k = \sum_{i=0}^{n-(k+1)} a_i a_{k+i}$, *para* $k = 0, 1, \cdots, n-1$.

Demonstração: Pela Observação 4.3.1 e da linearidade da função traço temos que

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(x\overline{x}) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(A_0) + \sum_{k=1}^{n-1} A_k Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\alpha_k),$$

onde $\alpha_k = \zeta_{pq}^{k} + \zeta_{pq}^{-k}$. Pelo Lema 4.3.3 temos que

$$\begin{aligned} Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(x\overline{x}) &= A_0(p-1)(q-1) + A_1 Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{1} + \zeta_{pq}^{-1}) + \cdots + \\ &+ A_{n-1} Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^{n-1} + \zeta_{pq}^{-n+1}) = (p-1)(q-1)A_0 + \\ &+ 2(1-p)\sum_{p|k} A_k + 2(1-q)\sum_{q|k} A_k + 2\sum_{p\nmid k,\, q\nmid k} A_k, \end{aligned}$$

e isto conclui a demonstração. ∎

Exemplo 4.3.8. *Se $p = 3$, $q = 7$ e $x = 1 + \zeta_{21}^{3} + \zeta_{21}^{6} + \zeta_{21}^{9}$ é um elemento de $\mathbb{Z}[\zeta_{21}]$, então $\underline{x} = (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$ e os A_{k}'s*

são dados por $A_0 = 4$, $A_3 = 3$, $A_6 = 2$, $A_9 = 1$ *e* $A_1 = A_2 = A_4 = A_5 = A_7 = A_8 = A_{10} = A_{11} = 0$. *Logo,* $Tr_{\mathbb{Q}(\zeta_{21})\mathbb{Q}}(x\overline{x}) = 48-24 = 24$ *e portanto* $|\sigma_{\mathbb{K}}(x)| = \sqrt{12}$. *Agora, se* $x = 1-\zeta_{21}^3$ *em* $\mathbb{Z}[\zeta_{21}]$ *então* $\underline{x} = (1,0,0,-1,0,0,0,0,0,0,0,0)$, *e os* $A_{k}'s$ *são dados por* $A_0 = 2$, $A_3 = -1$ *e* $A_1 = A_2 = A_4 = A_5 = A_6 = A_7 = A_8 = A_9 = A_{10} = A_{11} = 0$. *Logo,* $Tr_{\mathbb{Q}(\zeta_{21})/\mathbb{Q}}(x\overline{x}) = 24+4 = 28$ *e portanto* $|\sigma_{\mathbb{K}}(x)| = \sqrt{14}$.

Se $\mathbb{A}_{\mathbb{L}} = \mathbb{Z}[\zeta_{pq}]$, pela Seção 2.4, temos que se p e q são números primos distintos tais que $O_q(p) \equiv O_p(q) \equiv 1(mod\ 2)$ então

$$p\mathbb{A}_{\mathbb{L}} = (\mathfrak{p}_1 \cdots \mathfrak{p}_r\overline{\mathfrak{p}_1 \cdots \mathfrak{p}_r})^{p-1} \quad \text{e} \quad q\mathbb{A}_{\mathbb{L}} = (\mathfrak{q}_1 \cdots \mathfrak{q}_s\overline{\mathfrak{q}_1 \cdots \mathfrak{q}_s})^{q-1}. \quad (4.7)$$

Tomando o ideal $\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{q}_1 \cdots \mathfrak{q}_s$ temos que x pertence a $\mathfrak{p}$ se, e somente se, $x\overline{x}$ pertence a $(1-\zeta_{pq}^p)(1-\zeta_{pq}^q)\mathbb{A}_{\mathbb{L}}$. De fato, se x pertence a $\mathfrak{p}$, então $x\overline{x}$ é um elemento de $(1-\zeta_{pq}^p)(1-\zeta_{pq}^q)\mathbb{A}_{\mathbb{L}}$, uma vez que $p\mathbb{A}_{\mathbb{L}} = (\mathfrak{p}_1 \cdots \mathfrak{p}_r\overline{\mathfrak{p}_1 \cdots \mathfrak{p}_r})^{p-1} = (1-\zeta_{pq}^p)^{p-1}\mathbb{A}_{\mathbb{L}} = ((1-\zeta_{pq}^p)\mathbb{A}_{\mathbb{L}})^{p-1}$. Por outro lado, se x não é um elemento de $\mathfrak{p}$, então pelo menos um dos $\mathfrak{p}_{i}'s$ ou $\mathfrak{q}_{i}'s$ não aparecerá na fatoração do ideal $x\mathbb{A}_{\mathbb{L}}$ e portanto na fatoração de $x\overline{x}\mathbb{A}_{\mathbb{L}}$ não aparecerão todos os fatores de $(1-\zeta_{pq}^p)(1-\zeta_{pq}^q)\mathbb{A}_{\mathbb{L}}$, contradizendo a hipótese. Visto que o corpo $\mathbb{L} = \mathbb{Q}(\zeta_{pq})$ é totalmente complexo, segue que a densidade de centro do reticulado $\sigma_{\mathbb{L}}(\mathfrak{p})$, é dada por

$$\delta(\sigma_{\mathbb{L}}(\mathfrak{p})) = \frac{2^{\frac{n}{2}}\rho^n}{|D_{\mathbb{L}}|^{\frac{1}{2}}N(\mathfrak{p})},$$

onde $n = [\mathbb{L} : \mathbb{Q}]$ e

$$\rho = \rho(\sigma_{\mathbb{L}}(\mathfrak{p})) = \frac{1}{2}min\left\{\sqrt{\frac{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x})}{2}} \ : \ x \in \mathfrak{p},\ x \neq 0\right\}.$$

Exemplo 4.3.9. *Veremos a construção algébrica de* K_{12} *via a representação geométrica de um ideal primo acima de* $7\mathbb{A}_{\mathbb{L}}$ *em* $\mathbb{A}_{\mathbb{L}} = \mathbb{Z}[\zeta_{21}]$ *com* $\mathbb{L} = \mathbb{Q}(\zeta_{21})$. *Seja* $f(X)$ *o polinômio minimal de*

ζ_{21} *sobre* $\mathbb{Q}$. *Vamos fatorar os ideais* $3\mathbb{A}_{\mathbb{L}}$ *e* $7\mathbb{A}_{\mathbb{L}}$ *em um produto de ideais primos utilizando o Lema de Kummer. Temos que* $f(X) = X^{12} - X^{11} + X^9 - X^8 + X^6 - X^4 + X^3 - X + 1$, *e portanto* $f(X) \equiv (X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)^2 (mod\ (\mathbb{Z}/3\mathbb{Z})[X])$. *Assim*

$$g = 1,\ \overline{\mu_1}(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1,\ e_1 = 2\, e\, f_1 = 6.$$
$$\mathfrak{p}_1 = 3\mathbb{A}_{\mathbb{L}} + (\zeta_{21}^6 + \zeta_{21}^5 + \zeta_{21}^4 + \zeta_{21}^3 + \zeta_{21}^2 + 1)\mathbb{A}_{\mathbb{L}}.$$

Portanto, $3\mathbb{A}_{\mathbb{L}} = \mathfrak{p}_1^2$ *com* $N(\mathfrak{p}_1) = 3^6$. *Note que o ideal* $3\mathbb{A}_{\mathbb{L}}$ *não se fatora conforme a Equação (4.7), o que já era possível concluir pois* $O_7(3) = 6 \equiv 0(mod\ 2)$ *ou simplesmente observando que* $card(D_{\mathbb{L}}(3)) = e_1 f_1 = 12$. *Portanto* $D_{\mathbb{L}}(3) = G$, *onde* G *é o grupo de Galois de* $\mathbb{L}$ *sobre* $\mathbb{Q}$. *Para o caso* $7\mathbb{A}_{\mathbb{L}}$, *temos que*

$$f(X) \equiv (X+3)^6 (X+5)^6 (mod\ (\mathbb{Z}/7\mathbb{Z})[X])$$

Assim

$$g = 2,\ \overline{\mu_1}(X) = X + 3,\ \overline{\mu_2}(X) = X + 5,\ e_1 = e_2 = 6\, e\, f_1 = f_2 = 1.$$
$$\mathfrak{q}_1 = 7\mathbb{A}_{\mathbb{L}} + (\zeta_{21} + 3)\mathbb{A}_{\mathbb{L}} \quad e \quad \mathfrak{q}_2 = 7\mathbb{A}_{\mathbb{L}} + (\zeta_{21} + 5)\mathbb{A}_{\mathbb{L}}.$$

Portanto, $7\mathbb{A}_{\mathbb{L}} = (\mathfrak{q}_1\mathfrak{q}_2)^6$, *onde* $\mathfrak{q}_1$ *e* $\mathfrak{q}_2$ *são ideais com norma 7 e* $\mathfrak{q}_2 = \overline{\mathfrak{q}_1}$. *Observamos que* $O_3(7) = 1 \equiv 1(mod\ 2)$ *e que* $\overline{\sigma} = \sigma_{20}$ *não pertence a* $D_{\mathbb{L}}(7) = \{\sigma_1, \sigma_4, \sigma_{10}, \sigma_{13}, \sigma_{16}, \sigma_{19}\}$. *Dado que o discriminante absoluto de* $\mathbb{L}$ *é* $3^6 7^{10}$ *(Teorema* 2.3.7*), segue que a densidade de centro de* $\sigma_{\mathbb{L}}(\mathfrak{q}_1)$ *é dada por* $\delta(\sigma_{\mathbb{L}}(\mathfrak{q}_1)) = \dfrac{2^6 \rho^{12}}{3^3 7^6}$. *Calculamos então o raio de empacotamento*

$$\rho = \rho(\sigma_{\mathbb{L}}(\mathfrak{q}_1)) = \tfrac{1}{2} min\left\{ \sqrt{\tfrac{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x})}{2}} \ :\ x \in \mathfrak{q}_1,\ x \neq 0 \right\}.$$

Temos que $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x})$ *é par, ou seja,* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = 2l$, $l \in \mathbb{Z}$ *e para* x *em* $\mathfrak{q}_1$ *temos que* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \in 7\mathbb{Z}$, *o que implica que* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x})$ *é múltiplo de 14. Como* $mdc(p, q) = 1$, *segue que para* x *em* $\mathfrak{q}_1$, $x = \alpha_0 + \alpha_1\zeta_3$ *com* $\alpha_0, \alpha_1 \in \mathbb{Z}[\zeta_7]$, *segue que*

$$Tr_{\mathbb{L}/\mathbb{Q}(\zeta_7)}(x\overline{x}) = \alpha_0\overline{\alpha_0} + \alpha_1\overline{\alpha_1} + (\alpha_0 - \alpha_1)(\overline{\alpha_0 - \alpha_1}).$$

Aplicando o traço novamente temos:

$$Tr_{\mathbb{Q}(\zeta_7)/\mathbb{Q}}(Tr_{\mathbb{L}/\mathbb{Q}(\zeta_7)}(x\overline{x})) =$$
$$Tr_{\mathbb{Q}(\zeta_7)/\mathbb{Q}}(\alpha_0\overline{\alpha_0}) + Tr_{\mathbb{Q}(\zeta_7)/\mathbb{Q}}(\alpha_1\overline{\alpha_1}) + Tr_{\mathbb{Q}(\zeta_7)/\mathbb{Q}}[(\alpha_0 - \alpha_1)(\overline{\alpha_0 - \alpha_1})].$$

Temos duas possibilidades para $x = \alpha_0 + \alpha_1\zeta_3$.
1^o *caso* : *Se* $\alpha_0 = \alpha_1$, *então* $x = \alpha_0(1+\zeta_3) \in \mathfrak{q}_1$. *Como* $1+\zeta_3$ *não pertence ao ideal primo* $\mathfrak{q}_1$, *segue que* $\alpha_0 \in \mathfrak{q}_1$. *Logo,* $Tr_{\mathbb{Q}(\zeta_7)/\mathbb{Q}}(\alpha_0\overline{\alpha_0}) \geq 14$. *Portanto*

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \geq 2Tr_{\mathbb{Q}(\zeta_7)/\mathbb{Q}}(\alpha_0\overline{\alpha_0}) \geq 28.$$

2^o *caso* : *Se* $\alpha_0 \neq \alpha_1$, *para* $y = \sum_{i=0}^{5} a_i\zeta_7^i \in \mathbb{Z}[\zeta_7]$, *segue do Teorema 4.3.3, que* $Tr_{\mathbb{Q}(\zeta_7)/\mathbb{Q}}(y\overline{y})$ *é uma forma quadrática* $Q_6(a_0, a_1, a_2, a_3, a_4, a_5)$ *cujo valor mínimo é 6, (Proposição 1.9.1). Então*

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \geq 6 + 6 + 6 = 18 \quad e \quad Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \equiv 0 (mod\ 14),$$

e portanto $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \geq 28$. *Vamos caracterizar um elemento de* $\mathfrak{q}_1$. *Em* $\mathfrak{q}_1$ *temos que* $\zeta_{21} \equiv -3 (mod\ \mathfrak{q}_1)$ *e então para* x *em* $\mathfrak{q}_1$ *temos que*

$$x = \sum_{i=0}^{11} a_i\zeta_{21}^i \equiv \sum_{i=0}^{11} a_i(-3)^i (mod\ \mathfrak{q}_1).$$

Como $\mathfrak{q}_1 \cap \mathbb{Z} = 7\mathbb{Z}$, *segue que*

$$x \in \mathfrak{q}_1 \Longleftrightarrow \sum_{i=0}^{11} a_i(-3)^i \equiv 0 (mod\ 7).$$

O elemento $x = 1-\zeta_{21}^3 \in \mathbb{A}_{\mathbb{L}}$. *Como* $\underline{x} = (1, 0, 0, -1, 0, 0, 0, 0, 0, 0, 0, 0)$, *segue que* $\sum_{i=0}^{11} a_i(-3)^i = 1 - (-3)^3 = 28 \equiv 0 (mod\ 7)$ *e portanto* x *pertence a* $\mathfrak{q}_1$. *Pelo Exemplo* 4.3.8, *temos que* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = 28$. *Logo o menor valor de* $\{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) : x \in \mathfrak{q}_1, x \neq 0\}$ *é de fato 28. Portanto,* $\rho = \frac{\sqrt{14}}{2} = \sqrt{\frac{7}{2}}$, *e a densidade de centro é dada por:*

$$\delta(\sigma_{\mathbb{L}}(\mathfrak{q}_1)) = \frac{2^6\left(\sqrt{\frac{7}{2}}\right)^{12}}{3^3.7^6} = \frac{1}{3^3} \approx 0,037037.$$

Para esta dimensão temos que esta é a maior densidade de centro já obtida, e corresponde a densidade de centro do reticulado conhecido na literatura $\boldsymbol{K}_{12}$, *(Conway; Sloane, 1999, p.15).*

Exemplo 4.3.10. *Veremos a construção do reticulado* Λ_{24}. *Dados* $\mathbb{A}_{\mathbb{L}} = \mathbb{Z}[\zeta_{39}]$ *o anel dos inteiros algébricos de* $\mathbb{L} = \mathbb{Q}(\zeta_{39})$ *e* $f(X)$ *o polinômio minimal de* ζ_{39} *sobre* $\mathbb{Q}$, *vejamos as fatorações dos ideais* $3\mathbb{A}_{\mathbb{L}}$ *e* $13\mathbb{A}_{\mathbb{L}}$ *como um produto de ideais primos de* $\mathbb{A}_{\mathbb{L}}$. *Como*

$$\begin{aligned} f(X) \quad &= X^{24} - X^{23} + X^{21} - X^{20} + X^{18} - X^{17} + X^{15} - X^{14} + \\ &+ X^{12} - X^{10} + X^9 - X^7 + X^6 - X^4 + X^3 - X + 1, \end{aligned}$$

segue que

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

Assim

$$\begin{aligned} &g = 4, \qquad e_1 = e_2 = e_3 = e_4 = 2, \qquad f_1 = f_2 = f_3 = f_4 = 3 \\ &\overline{\mu_1}(X) = X^3 + 2X + 2, \qquad \overline{\mu_2}(X) = X^3 + X^2 + X + 2, \\ &\overline{\mu_3}(X) = X^3 + 2X^2 + 2X + 2, \qquad \overline{\mu_4}(X) = X^3 + X^2 + 2, \end{aligned}$$

Logo,

$$\begin{aligned} \mathfrak{p}_1 &= 3\mathbb{A}_{\mathbb{L}} + (\zeta_{39}^3 + 2\zeta_{39} + 2)\mathbb{A}_{\mathbb{L}} \\ \mathfrak{p}_2 &= 3\mathbb{A}_{\mathbb{L}} + (\zeta_{39}^3 + \zeta_{39}^2 + \zeta_{39} + 2)\mathbb{A}_{\mathbb{L}} \\ \mathfrak{p}_3 &= 3\mathbb{A}_{\mathbb{L}} + (\zeta_{39}^3 + 2\zeta_{39}^2 + 2\zeta_{39} + 2)\mathbb{A}_{\mathbb{L}} \\ \mathfrak{p}_4 &= 3\mathbb{A}_{\mathbb{L}} + (\zeta_{39}^3 + \zeta_{39}^2 + 2)\mathbb{A}_{\mathbb{L}} \end{aligned}$$

Portanto $3\mathbb{A}_{\mathbb{L}} = (\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4)^2$, *com* $N(\mathfrak{p}_i) = 3^3$, *para* $i = 1, 2, 3, 4$. *Como* $O_{13}(3) = 3 \equiv 1 (mod\ 2)$, *segue que* $\overline{\sigma} = \sigma_{38} \notin D_{\mathbb{L}}(3) = \{\sigma_1, \sigma_{14}, \sigma_{16}, \sigma_{22}, \sigma_{29}, \sigma_{35}\}$. *Neste caso, temos que* $\mathfrak{p}_4 = \overline{\mathfrak{p}_1}$ *e* $\mathfrak{p}_3 = \overline{\mathfrak{p}_2}$. *Para o ideal* $13\mathbb{A}_{\mathbb{L}}$ *temos que*

$$f(X) \equiv (X+4)^{12}(X+10)^{12}(mod\ (\mathbb{Z}/13\mathbb{Z})[X]).$$

$$g = 2, \quad \overline{\mu_1} = X+4, \quad \overline{\mu_2} = X+10, \quad e_1 = e_2 = 12, \quad f_1 = f_2 = 1.$$

$$\mathfrak{q}_1 = 13\mathbb{A}_{\mathbb{L}} + (\zeta_{39}+4)\mathbb{A}_{\mathbb{L}} \quad e \quad \mathfrak{q}_2 = 13\mathbb{A}_{\mathbb{L}} + (\zeta_{39}+10)\mathbb{A}_{\mathbb{L}}.$$

Logo, $13\mathbb{A}_{\mathbb{L}} = (\mathfrak{q}_1\mathfrak{q}_2)^{12}$, *onde* $\mathfrak{q}_1$ *e* $\mathfrak{q}_2$ *são ideais primos com norma 13. Observe novamente que* $\overline{\sigma} \notin D_{\mathbb{L}}(13) = \{\sigma_1, \sigma_4, \sigma_7, \sigma_{10}, \sigma_{16}, \sigma_{19}, \sigma_{22}, \sigma_{25}, \sigma_{28}, \sigma_{31}, \sigma_{34}, \sigma_{37}\}$, *pois* $O_3(13) = 1 \equiv 1(mod\ 2)$. *Neste caso, temos que* $\mathfrak{q}_2 = \overline{\mathfrak{q}_1}$. *Considerando o ideal* $\mathfrak{p} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{q}_1$, *vamos calcular a densidade de centro de* $\sigma_{\mathbb{L}}(\mathfrak{p})$. *Como* $D_{\mathbb{L}} = 3^{12}13^{22}$ *e* $N(\mathfrak{p}) = N(\mathfrak{p}_1)N(\mathfrak{p}_2)N(\mathfrak{q}_1) = 3^6.13$, *segue que*

$$\delta(\sigma_{\mathbb{L}}(\mathfrak{p})) = \frac{2^{12}\rho^{24}}{3^{12}13^{12}}.$$

Precisamos agora determinar

$$\rho = \rho(\sigma_{\mathbb{L}}(\mathfrak{p})) = \frac{1}{2} min\left\{ \sqrt{\frac{Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x})}{2}} \ : \ x \in \mathfrak{p},\ x \neq 0 \right\}.$$

Veremos agora que se $x \in \mathfrak{p}$, *então* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \geq 4.39$. *Visto que* $mdc(p,q) = 1$, *para* $x \in \mathfrak{p}$, *podemos escrever* $x = \alpha_0 + \alpha_1\zeta_3$, *com* $\alpha_0, \alpha_1 \in \mathbb{Z}[\zeta_{13}]$. *Temos também que se* x *pertence a* $\mathfrak{p}$, *então* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \equiv 0(mod\ 2.39)$. *Pelo Exemplo* 4.3.9, *temos que*

$$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) =$$
$$Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(\alpha_0\overline{\alpha}_0) + Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(\alpha_1\overline{\alpha}_1) + Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}[(\alpha_0-\alpha_1)(\overline{\alpha_0-\alpha_1})].$$

Nesta soma, para que o valor 2.39 *seja atingido, as únicas possibilidades são, a menos de ordem,* $Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(\alpha_0\overline{\alpha}_0) = 12$, $Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(\alpha_1\overline{\alpha}_1) = 30$ *e* $Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}[(\alpha_0-\alpha_1)(\overline{\alpha_0-\alpha_1})] = 36$. *As possibilidades para* α_0 *e* α_1 *são:*

$$\alpha_0 = \pm\zeta_{13}^{i_0}, \ i_0 = 0, \cdots, 12;$$
$$\alpha_1 = \pm(\zeta_{13}^{i_1} + \zeta_{13}^{i_2} + \zeta_{13}^{i_3}),$$

onde i_1, i_2, i_3, *são dois a dois distintos. Sejam* $\alpha_0 = -\zeta_{13}^{i_0}$ *e* $\alpha_1 = \zeta_{13}^{i_1} + \zeta_{13}^{i_2} + \zeta_{13}^{i_3}$. *Se* $i_0 \neq i_k$, *com* $k = 1, 2, 3$, *então* $Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}[(\alpha_0 - \alpha_1)(\overline{\alpha_0 - \alpha_1})] = 36$. *Sendo* x *um elemento de* $\mathfrak{p}$, *segue que*

$$Tr_{\mathbb{L}/\mathbb{Q}(\zeta_{13})}(x\overline{x}) = 3(\alpha_0\overline{\alpha}_0 + \alpha_1\overline{\alpha}_1) - (\alpha_0 + \alpha_1)\overline{(\alpha_0 + \alpha_1)} \in 3\mathbb{Z}[\zeta_{13}],$$

e portanto, se $y = (\alpha_0+\alpha_1)\overline{(\alpha_0 + \alpha_1)}$. *Assim* $y \equiv 0 (mod\ 3\mathbb{Z}[\zeta_{13}])$. *Seja* $\gamma : \mathbb{Z}[\zeta_{13}] \longrightarrow \mathbb{Z}$ *o homomorfismo de anéis dado por* $\gamma\left(\sum_{i=0}^{11} a_i\zeta_{13}^i\right) = \sum_{i=0}^{11} a_i$. *Como* y *está em* $3\mathbb{Z}[\zeta_{13}]$ *segue que* $\gamma(y) \equiv 0 (mod\ 3)$. *Reescrevendo* y *substituindo* α_0 *e* α_1 *pelos valores fixados acima temos que*

$$y = (-\zeta_{13}^{i_0} + \zeta_{13}^{i_1} + \zeta_{13}^{i_2} + \zeta_{13}^{i_3})(-\zeta_{13}^{-i_0} + \zeta_{13}^{-i_1} + \zeta_{13}^{-i_2} + \zeta_{13}^{-i_3}) = 4 - A + B \equiv 0 (mod\ 3\mathbb{Z}[\zeta_{13}]),$$

onde $A = \sum_{s=1}^{3}(\zeta_{13}^{i_0-i_s} + \zeta_{13}^{i_s-i_0})$ *e* $B = \sum_{r,s=1}^{3} \zeta_{13}^{i_r-i_s}$. *Sendo* n_A *o número de expoentes tais que* $i_0 - i_s = -1$ *ou* $i_s - i_0 = -1$ *e* n_B *o número de expoentes tais que* $i_r - i_s = -1$, *segue que as possibilidades para* n_A *são* 0 *ou* 1, *uma vez que* i_1, i_2, i_3 *são dois a dois distintos. Por outro lado, para* n_B *as possibilidades são* 0, 1 *ou* 2. *Observe que* $\gamma(\zeta_{13}^{-1}) = \gamma(-1 - \zeta_{13} - \cdots - \zeta_{13}^{11}) = -12 \equiv 0 (mod\ 3)$. *Assim,*

$$\gamma(A) = 6 - n_A \text{ e } \gamma(B) = 6 - n_B.$$

Logo, $\gamma(y) = 4 - \gamma(A) + \gamma(B) \equiv 1 + n_A - n_B \equiv 0 (mod\ 3\mathbb{Z}[\zeta_{13}])$ *e as únicas soluções possíveis são*

$$n_A = 0 \text{ e } n_B = 1$$

ou

$$n_A = 1 \text{ e } n_B = 2.$$

Suponhamos $n_A = 0$ *e* $n_B = 1$. *Dado* $0 < a \leq 11$, *por hipótese, o coeficiente de* ζ_{13}^a *é múltiplo de 3. Temos*

$$B = \zeta_{13}^{-1} + \sum_{r,s=1}^{3} \zeta_{13}^{i_r - i_s}, \text{ com } i_r - i_s \neq -1.$$

Se existem r *e* s *tais que* $i_r - i_s = a$, *então o coeficiente de* ζ_{13}^a *na equação acima é nulo, pois* $\zeta_{13}^{-1} = -1 - \zeta_{13} - \cdots - \zeta_{13}^{11}$. *Assim,* ζ_{13}^a *aparece também com coeficiente nulo na expansão de* A *na base integral* $\{1, \cdots, \zeta_{13}^{11}\}$. *Se não existem* r *e* s *tais que* $i_r - i_s = a$, *novamente* ζ_{13}^a *aparece com coeficiente nulo na decomposição de* y. *Deste modo, a única possibilidade portanto é* $a = 0$ *e* $y = 3$. *Então como*

$$Tr_{\mathbb{L}/\mathbb{Q}(\zeta_{13})}(x\overline{x}) = 3(\alpha_0\overline{\alpha}_0 + \alpha_1\overline{\alpha}_1) - (\alpha_0 + \alpha_1)(\overline{\alpha_0 + \alpha_1}),$$

temos

$Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) = Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(3(\alpha_0\overline{\alpha_0} + \alpha_1\overline{\alpha_1}) - (\alpha_0 + \alpha_1)(\overline{\alpha_0 + \alpha_1})) =$
$3Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(\alpha_0\overline{\alpha_0}) + 3Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(\alpha_1\overline{\alpha_1}) - Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}((\alpha_0 + \alpha_1)(\overline{\alpha_0 + \alpha_1})) =$
$3 \cdot 12 + 3 \cdot 30 - 36 = 90$, *e isto não ocorre pois 90 não é múltiplo de* $2 \cdot 39$. *Quando* $n_A = 1$ *e* $n_B = 2$ *a verificação é análoga. Portanto* $Tr_{\mathbb{L}/\mathbb{Q}}(x\overline{x}) \geq 4.39 = 156$. *O elemento* $x = 1 - \zeta_{39}^3 - \zeta_{39}^{13} + \zeta_{39}^{16}$ *pertence ao ideal* $\mathfrak{p}$ *e observando que* $\underline{x} = (1, 0, 0, -1, 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$, *pela Proposição* 4.3.7, *temos que* $Tr(x\overline{x}) = 156$. *Portanto,* $\rho(\sigma_{\mathbb{L}}(\mathfrak{p})) = \dfrac{\sqrt{78}}{2} = \sqrt{\dfrac{39}{2}}$ *e a densidade de centro é dada por:*

$$\delta(\sigma_{\mathbb{L}}(\mathfrak{p})) = \frac{2^{12}\left(\sqrt{\frac{39}{2}}\right)^{24}}{3^{12}13^{12}} = 1.$$

Para dimensão 24 a densidade de centro obtida neste exemplo é a maior conhecida, e corresponde a densidade de centro do reticulado conhecido na literatura Λ_{24}. (Conway; Sloane, 1999, p.15).