Discriminante mínimo de subcorpos de $Q(\zeta_{p^r})$

Cátia Regina de Oliveira Quilles e Antonio Aparecido de Andrade

***Resumo*— No presente trabalho apresentamos o cálculo do discriminante de subcorpos de $\mathbb{Q}(\zeta_{p^r})$, usando caracteres de Dirichlet e seus condutores, e encontramos alguns discriminantes mínimos. Com isto podemos obter reticulados com empacotamentos mais densos. Neste sentido, apresentamos o conceito de reticulado, empacotamento e suas propriedades.**

***Palavras-Chave*— Corpos ciclotômicos, Caracteres de Dirichlet, Condutores, Discriminantes, Reticulados, Empacotamentos.**

***Abstract*— In this work we present the computing of the discriminant of subfields of $\mathbb{Q}(\zeta_{p^r})$, by using Dirichlet characters and their conductors, and we find some minimum discriminants. With this, we can obtain lattices with dense packings. In this sense, we present the concept of lattice, packing, and their proprieties.**

***Keywords*— Cyclotomic fields, Dirichlet characters, Conductors, Discriminants, Lattices, Packings.**

I. Introdução

Os reticulados tem se mostrado bastante úteis na teoria das comunicações. Contudo os reticulados de maior interesse são aqueles com maior densidade de empacotamento, e o cálculo do discriminante mínimo pode ser utilizado nesta busca. Encontrar um corpo de números de um grau previamente determinado e discriminante mínimo é um problema clássico e as poucas soluções que se conhecem são para corpos de grau baixo. A solução para tal problema tem implicações imediatas em outras áreas do conhecimento, especialmente na teoria da informação, quando se constrói codificadores de fontes baseados em reticulados algébricos [1]. Neste trabalho apresentamos algumas formas para o cálculo do discriminante mínimo de subcorpos de $\mathbb{Q}(\zeta_{p^r})$, com p um primo ímpar e r um inteiro positivo, e encontramos alguns discriminantes mínimos [2]. Deste modo, na Seção II faremos um estudo de caracteres de Dirichlet e suas propriedades. Na Seção III, veremos algumas propriedades de caracteres de Dirichlet tendo por condutor uma potência de primo. Na Seção IV, veremos o cálculo de alguns discriminantes usando os caracteres de Dirichlet. Na Seção V, veremos condições para o cálculo do discriminante mínimo para certos corpos numéricos. Na Seção VI, apresentamos a definição de reticulados e suas principais propriedades. Na Seção VII, veremos reticulados via corpos numéricos e a forma da densidade de centro usando o discriminante. Na Seção VIII, daremos nossas conclusões.

II. Caracteres de Dirichlet

Nesta seção apresentamos os caracteres de Dirichlet, seus condutores e algumas propriedades, que serão úteis para o cálculo do discriminante dos subcorpos de $\mathbb{Q}(\zeta_{p^r})$. Esses caracteres descrevem parte da aritmética de um corpo abeliano e mostram que qualquer grupo abeliano finito pode ser analisado como um subgrupo de um grupo de Galois de um corpo ciclotômico $\mathbb{Q}(\zeta_n)$.

Definição II.1: Sejam G um grupo, $\mathbb{K}$ um corpo e $\mathbb{K}^*$ o grupo multiplicativo dos elementos inversíveis de $\mathbb{K}$. Um homomorfismo de grupos $\sigma : G \longrightarrow \mathbb{K}^*$ é chamado de caracter de G em $\mathbb{K}$.

Observação II.1: O conjunto dos caracteres forma um grupo.

Definição II.2: Um homomorfismo $\chi : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ multiplicativo é chamado de um caracter de Dirichlet.

Observação II.2: Um caracter de Dirichlet módulo n é uma função χ que satisfaz as seguintes propriedades:

1) $\chi(1) = 1$,
2) $\chi(a) = \chi(a+n)$, para todo a inteiro positivo,
3) $\chi(ma) = \chi(m)\chi(a)$, para quaisquer m ea inteiros positivos,
4) $\chi(a) = 0$, para todo a tal que $mdc(a,n) \neq 1$.

Observação II.3: Sejam n e m inteiros positivos. Se $n|m$, então o caracter $\chi : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow (\mathbb{C})^*$ induz um homomorfismo $\chi' : (\mathbb{Z}/m\mathbb{Z})^* \longrightarrow (\mathbb{C})^*$, via a composição com o homomorfismo canônico sobrejetor $\theta : (\mathbb{Z}/m\mathbb{Z})^* \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$.

Definição II.3: Seja χ um caracter de Dirichlet. Definimos o condutor de χ e denotamos por f_χ, o menor valor de n que satisfaça a condição 2 da Observação II.2.

Exemplo II.1: Seja $G = (\mathbb{Z}/10\mathbb{Z})^* = \{1,3,7,9\}$. O grupo de caracteres de Dirichlet de G é $\{\chi_0, \chi_1, \chi_2, \chi_3\}$ e podemos descrevê-los através da seguinte tabela:

	χ_0	χ_1	χ_2	χ_3
1	1	1	1	1
3	1	1	-1	-1
7	1	-1	1	-1
9	1	-1	-1	1
f_χ	1	5	5	5

Os caracteres χ_1, χ_2 e χ_3 podem ser definidos módulo 5, pois $\chi_i(a+5) = \chi_i(a)$, para todo a e $i = 1,2,3$. Assim, como 5 é o mínimo que isso ocorre, segue que o condutor de χ_i é $f_{\chi_i} = 5$, $i = 1,2,3$.

Teorema II.1: [3] Seja χ um caracter de Dirichlet definido módulo m. Se $n|m$, então o condutor de χ é n se, e somente se, quando $mdc(a,m) = 1$ e $a \equiv 1(mod\ n)$, $\chi(a) = 1$.

Definição II.4: Um caracter de Dirichlet definido módulo o seu condutor é chamado caracter primitivo.

Observação II.4:

1) A vantagem de usarmos caracteres de Dirichlet primitivos é evidente quando tomamos um produto de vários

Departamento of Matematica - Ibilce - Unesp, Rua Cristovão Colombo, 2265, 15054-000, São José do Rio Preto, SP, Brasil, E-mail: catia.quilles@pop.com.br., andrade@ibilce.unesp.br

caracteres com vários condutores, pois o módulo de definição cresce rapidamente.

2) Algumas vezes é vantajoso pensar nos caracteres de Dirichlet como os caracteres dos grupos de Galois de corpos ciclotômicos. Se identificarmos $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ com $(\mathbb{Z}/n\mathbb{Z})^*$, então o caracter de Dirichlet módulo n é um caracter de Galois.

Definição II.5: Sejam χ um caracter de Dirichlet do grupo de Galois $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ e $\mathbb{K}$ o corpo fixo do núcleo de χ. O corpo $\mathbb{K}$ é chamado corpo associado a χ.

Observação II.5:

1) O corpo $\mathbb{K}$ associado a χ é um subcorpo de $\mathbb{Q}(\zeta_n)$, e se n é o menor valor, então n é o condutor de χ.
2) O corpo $\mathbb{K}$ depende somente de χ.
3) Se X é um grupo finito de caracteres de Dirichlet e $mmc(f_{\chi_i}) = n$, onde $\chi_i \in X$, então X é um subgrupo do grupo dos caracteres de Dirichlet. Sejam H a intersecção dos núcleos destes caracteres e $\mathbb{K}$ o corpo fixado por H. Assim, $\mathbb{K}$ é o corpo associado a X. Além disso, como X é isomorfo a $Gal(\mathbb{K}/\mathbb{Q})$, o grau de $\mathbb{K}/\mathbb{Q}$ é igual a ordem de χ.

Exemplo II.2: Se X é o grupo de caracteres de $(\mathbb{Z}/m\mathbb{Z})^*$ satisfazendo $\chi(-1) = 1$, então a conjugação complexa $(\zeta_n \mapsto \zeta_n^{-1})$ está no núcleo de cada $\chi_i \in X$. O corpo $\mathbb{K}$ associado a X é $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, que é o subcorpo maximal real de $\mathbb{Q}(\zeta_n)$. Analogamente se χ é um caracter, então $\mathbb{K}$ é real se, e somente se, $\chi(-1) = 1$.

Exemplo II.3: Consideremos o grupo $G = (\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\}$. O grupo de caracteres de Dirichlet associado a G é $X = \{\chi_0, \chi_1, \chi_2, \chi_3\}$ e podemos descrevê-los pela tabela abaixo:

	χ_0	χ_1	χ_2	χ_3	
1	1	1	1	1	σ_1
5	1	1	-1	-1	σ_5
7=-5	1	-1	-1	1	σ_7
11=-1	1	-1	1	-1	σ_{11}
f_χ	1	4	12	3	

Os subgrupos multiplicativos do grupo de Galois são:

$$H_0 = \{\sigma_1\} \qquad H_1 = \{\sigma_1, \sigma_5\}$$
$$H_2 = \{\sigma_1, \sigma_{11}\} \quad H_3 = \{\sigma_1, \sigma_7\}$$
$$H_4 = G.$$

Assim, temos que $\mathbb{K}_0 = \mathbb{Q}(\zeta_{12}) = \mathbb{Q}(\sqrt{-3})\mathbb{Q}(\sqrt{-1})$ é fixado por H_0, $\mathbb{K}_1$ é fixado por H_1 e os caracteres associados são $\{\chi_0, \chi_1\}$, logo $\mathbb{K}_1$ tem condutor 4, e segue que $\mathbb{K}_1 = \mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-1})$. $\mathbb{K}_2$ é fixado por H_2, e os caracteres associados são $\{\chi_0, \chi_2\}$, logo $\mathbb{K}_2$ tem condutor 12, e segue que $\mathbb{K}_2 = \mathbb{Q}(\zeta_{12}) = Q(\sqrt{3})$. O fato que $\chi_2(-1) = 1$ informa que $\mathbb{K}_2$ é o subcorpo real. $\mathbb{K}_3$ é fixado por H_3 e os caracteres associados são $\{\chi_0, \chi_3\}$, logo $\mathbb{K}_3$ tem condutor 3 e daí $\mathbb{K}_3 = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$, e $\mathbb{Q}$ é fixado por G.

Proposição II.1: [3] Se G é um grupo abeliano finito e $\hat{G}$ é o grupo dos homomorfismos multiplicativos de G em $\mathbb{C}^*$, então G é isomorfo a $\hat{G}$ e G é isomorfo a $\hat{\hat{G}}$.

Proposição II.2: [3] Se H é um subgrupo de G e $H^\perp = \{\chi \in \hat{G} : \chi(h) = 1, \ \forall h \in H\}$, então $H^\perp$ é isomorfo a $(G/H)\hat{}$, $\hat{H}$ é isomorfo a $\hat{G}/H^\perp$ e $(H^\perp)^\perp = H$.

III. Caracteres de Dirichlet módulo p^r

Nesta seção apresentamos algumas propriedades particulares dos caracteres com condutores potência de primo.

Sejam g um inteiro tal que $\bar{g} \equiv g(\text{mod } p^r)$ é um gerador do grupo $(\mathbb{Z}/p^r\mathbb{Z})^*$ e χ um caracter de Dirichlet. Assim existem $(p-1)p^{r-1}$ caracteres de Dirichlet definidos sobre $(\mathbb{Z}/p^r\mathbb{Z})^*$, uma vez que $(\mathbb{Z}/p^r\mathbb{Z})^*$ tem ordem $(p-1)p^{r-1}$ e tais caracteres são completamente determinados pela imagem de $\bar{g}$. Por outro lado, pelo Teorema II.1, temos que

$$1 = \chi(\bar{1}) = \chi(g^{(p-\bar{1})p^{r-1}}) = \chi(\bar{g})^{(p-1)p^{r-1}}.$$

Logo $\chi(g)$ é uma raíz $(p-1)p^{r-1}$ - ésima da unidade. Assim, dado um caracter de Dirichlet módulo p^r, existe um inteiro i, onde $0 \leq i \leq (p-1)p^{r-1}$, tal que $\chi(\bar{g}) = \zeta^i_{(p-1)p^{r-1}}$. Como existem $(p-1)p^{r-1}$ caracteres e $(p-1)p^{r-1}$ possibilidades para i, concluimos que todos os caracteres definidos módulo p^r são da forma

$$\chi_i(\bar{g}) = \zeta^i_{(p-1)p^{r-1}},$$

para $i = 0, 1, \cdots, (p-1)p^{r-1}$.

Teorema III.2: [4] Se i é um inteiro tal que $0 \leq i \leq (p-1)p^{r-1}$, então o condutor f_{χ_i} de χ_i é p^{r-j} se, e somente se, $p^j = mdc(i, p^r)$.

IV. Cálculo do discriminante

Nesta seção apresentamos o valor do discriminante de um corpo de números $\mathbb{K}$, contido em uma extensão ciclotômica do tipo $\mathbb{Q}(\zeta_{p^r})$.

Definição IV.6: Sejam $\mathbb{L}$ uma extensão de um corpo $\mathbb{K}$, onde $\mathbb{K}$ é finito ou tem característica zero. Sejam $\sigma_1, \ldots, \sigma_n$ os distintos $\mathbb{K}$-isomorfismos de $\mathbb{L}$ sobre $\mathbb{K}$. Definimos o discriminante de $\mathbb{K}$ sobre $\mathbb{L}$ por

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

Teorema IV.3: [3] (Fórmula do condutor discriminante) Se $\mathbb{K}$ é o corpo de números associado ao grupo X de caracteres de Dirichlet, então o discriminante de $\mathbb{K}$ é dado por

$$D(\mathbb{K}/\mathbb{Q}) = (-1)^{r_2} \prod_{\chi \in \mathbb{X}} f_\chi,$$

onde r_2 é a metade do número de automorfismos complexos de $\mathbb{K}$.

Lema IV.1: [4] Se g é um inteiro tal que $\bar{g} \equiv g(\text{mod } p^r)$ é o gerador do grupo multiplicativo $(\mathbb{Z}/p^r\mathbb{Z})^*$, onde p é um número primo ímpar e r um inteiro positivo, então, para todo $0 < j \leq r$, temos que $g^k \equiv 1(mod\ p^j)$ se, e somente se, $k \equiv 0(mod\ (p-1)p^{j-1})$

Sejam p um primo ímpar, r um inteiro positivo e $\mathbb{K}$ um subcorpo de $\mathbb{Q}(\zeta_{p^r})$. Como o grau de $\mathbb{K}$ sobre $\mathbb{Q}$ é um divisor de $(p-1)p^{r-1}$, segue que $[\mathbb{K} : \mathbb{Q}] = up^j$, onde u é um divisor de $(p-1)$ e $0 < j \leq r-1$. Sejam $\mathbb{H}$ o subgrupo de Galois $Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ isomorfo a $(\mathbb{Z}/p^r\mathbb{Z})^*$que fixa $\mathbb{K}$ e $X_\mathbb{K}$ o grupo dos caracteres associados a $\mathbb{K}$, isto é, o conjunto $\{\chi \in (\mathbb{Z}/\hat{p^r\mathbb{Z}})^* \text{ tal que } \chi(i) = 1, \text{ para todo } i \in H\}$.

Teorema IV.4: [4] Se $\mathbb{K}$ é um subcorpo de $\mathbb{Q}(\zeta_{p^r})$ com $[\mathbb{K} : \mathbb{Q}] = up^j$, onde p é um primo ímpar, r um inteiro positivo, u um divisor de $(p-1)$ e $0 < j \leq r-1$, então

$$|D(\mathbb{K}/\mathbb{Q})| = p^{\beta(u,j)},$$

onde $\beta_{(u,j)} = u[(j+2)p^j - \frac{p^{j+1}-1}{p-1}] - 1$.

Corolário IV.1: [4] O discriminante do corpo ciclotômico $\mathbb{Q}(\zeta_{p^r})$, onde p é um primo ímpar e r um inteiro positivo é dado por

$$|D(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})| = p^{\beta_{(1,r-1)}},$$

onde $\beta_{(1,r-1)} = (p-1)[(r+1)p^{r-1} - \frac{p^r-1}{p-1}] - 1$.

Corolário IV.2: [4] Se $\mathbb{K}$ é um subcorpo de $\mathbb{Q}(\zeta_p)$, onde p é um primo ímpar, então o discriminante de $\mathbb{K}$ é dado por

$$|D(\mathbb{Q}(\zeta_p)/\mathbb{Q})| = p^{[\mathbb{K}:\mathbb{Q}]-1}.$$

Corolário IV.3: [4] Se $\mathbb{K} \subseteq \mathbb{Q}(\zeta_{p^r})$ é uma cúbica, então $D(\mathbb{K}/\mathbb{Q}) = p^2$ se $p \neq 3$ ou $D(\mathbb{K}/\mathbb{Q}) = 81$ se $p = 3$.

Exemplo IV.4: Se $n = 3^2$, então o grupo G tem ordem $(p-1)p^{r-1} = 2.3 = 6$ e é dado por $G = (\mathbb{Z}/9\mathbb{Z})^* = \{1,2,4,5,7,8\}$. O grupo de Galois de $\mathbb{Q}(\zeta_9)$ sobre $\mathbb{Q}$ é $G = \{\sigma_1, \sigma_2, \sigma_4, \sigma_5, \sigma_7, \sigma_8\}$. Caracterizamos o grupo $\hat{G}$ pela tabela :

	χ_0	χ_1	χ_2	χ_3	χ_4	χ_5	
$2^0 = 1$	1	1	1	1	1	1	σ_1
$2^1 = 2$	1	ζ_6	ζ_6^2	-1	ζ_6^4	ζ_6^5	σ_2
$2^2 = 4$	1	ζ_6^2	ζ_6^4	1	ζ_6^2	ζ_6^4	σ_4
$2^3 = 8$	1	-1	1	-1	1	-1	σ_8
$2^4 = 7$	1	ζ_6^4	ζ_6^2	1	ζ_6^4	ζ_6^2	σ_7
$2^5 = 5$	1	ζ_6^5	ζ_6^4	-1	ζ_6^2	ζ_6	σ_5
f_{χ_i}	1	3	3^2	3	3^2	3	

Os subgrupos multiplicativos do grupo de Galois são:
$H_0 = \{\sigma_1\}$ $H_2 = \{\sigma_1, \sigma_4, \sigma_7\}$
$H_1 = \{\sigma_1, \sigma_8\}$ $H_3 = G = \{\sigma_1, \sigma_2, \sigma_4, \sigma_8, \sigma_7, \sigma_5\}$.
Assim, temos que $\mathbb{K}_0 = \mathbb{Q}(\zeta_9)$ é fixado por H_0, $\mathbb{K}_1$ é fixado por H_1, $\mathbb{K}_2$ é fixado por H_2 e $\mathbb{Q}$ é fixado por G. Dessa forma os caracteres associados a $\mathbb{K}_0$ são $H_0^\perp = \hat{G}$, a $\mathbb{K}_1$ são $H_1^\perp = \{\chi_0, \chi_2, \chi_4\}$, a $\mathbb{K}_2$ são $H_2^\perp = \{\chi_0, \chi_3\}$ e a $\mathbb{Q}$ são $H_3^\perp = \{\chi_0\}$. Agora, para $\mathbb{K}_1$ temos que $[\mathbb{K}_1 : \mathbb{Q}] = 3$, logo nas condições do Teorema IV.4 temos que $u = 1$ e $j = 1$. Assim $|D(\mathbb{K}_1/\mathbb{Q})| = 3^{\beta_{(1,1)}}$, onde $\beta_{(1,1)} = (3.3 - \frac{3^2-1}{2}) - 1 = (9-4) - 1 = 4$. Portanto $|D(\mathbb{K}_1/\mathbb{Q})| = 3^4$. Analogamente para $\mathbb{K}_2$ temos que $[\mathbb{K}_2 : \mathbb{Q}] = 2$, logo novamente nas condições do Teorema IV.4 temos que $u = 2$ e $j = 0$ e segue que $|D(\mathbb{K}_2/\mathbb{Q})| = 3^{\beta_{(2,0)}}$, onde $\beta_{(2,0)} = 2(3.1 - \frac{2}{2}) - 1 = 2 - 1 = 1$. Portanto $|D(\mathbb{K}_2/\mathbb{Q})| = 3$. Para $\mathbb{K}_0 = \mathbb{Q}(\zeta_9)$ podemos aplicar o Corolário IV.1 e assim segue que $|D(\mathbb{K}_0/\mathbb{Q})| = 3^{\beta_{(1,1)}}$, onde $\beta_{(1,1)} = 2(3.3 - \frac{3^2-1}{3-1}) - 1 = 2(9-4) - 1 = 9$. Portanto $|D(\mathbb{K}_0/\mathbb{Q})| = 9$.

Exemplo IV.5: Sejam $n = 3^3$ e o grupo $(\mathbb{Z}/27\mathbb{Z})^* = \{1,2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26\}$. O grupo de Galois de $\mathbb{Q}(\zeta_{27})$ sobre $\mathbb{Q}$ é dado por
$G = \{\sigma_1, \sigma_2, \sigma_4, \sigma_5, \sigma_7, \sigma_8, \sigma_{10}, \sigma_{11}, \sigma_{13}, \sigma_{14}, \sigma_{16}, \sigma_{17}, \sigma_{19}, \sigma_{20}, \sigma_{22}, \sigma_{23}, \sigma_{25}, \sigma_{26}\}$. Caracterizamos o grupo $\hat{G}$ pela Tabela abaixo.
Os subgrupos multiplicativos do grupo de Galois são:
$H_0 = \{\sigma_1\}, H_1 = \{\sigma_1, \sigma_{26}\}, H_2 = \{\sigma_1, \sigma_{10}, \sigma_{19}\}$,
$H_3 = \{\sigma_1, \sigma_8, \sigma_{10}, \sigma_{26}, \sigma_{19}, \sigma_{17}\}$,
$H_4 = \{\sigma_1, \sigma_4, \sigma_{16}, \sigma_{10}, \sigma_{13}, \sigma_{25}, \sigma_{19}, \sigma_{22}, \sigma_7\}$ e $H_5 = G$
Assim, temos que $\mathbb{K}_0 = \mathbb{Q}(\zeta_{27})$ é fixado por H_0, $\mathbb{K}_1$ é fixado por H_1, $\mathbb{K}_2$ é fixado por H_2, $\mathbb{K}_4$ é fixado por H_4 e $\mathbb{Q}$ é fixado por G. Dessa forma os caracteres associados a $\mathbb{K}_0$ são $H_0^\perp = \hat{G}$, a $\mathbb{K}_1$ são $H_1^\perp = \{\chi_0, \chi_2, \chi_4, \chi_6, \chi_8, \chi_{10}, \chi_{12}, \chi_{14}, \chi_{16}\}$, a $\mathbb{K}_2$ são $H_2^\perp = \{\chi_0, \chi_3, \chi_6, \chi_9, \chi_{12}, \chi_{15}\}$, a $\mathbb{K}_3$ são $H_3^\perp = \{\chi_0, \chi_6, \chi_{12}\}$, a $\mathbb{K}_4$ são $H_4^\perp = \{\chi_0, \chi_9, \}$ e a $\mathbb{Q}$ são $H_5^\perp = \{\chi_0\}$. Agora, para $\mathbb{K}_1$ temos que $[\mathbb{K}_1 : \mathbb{Q}] = 9 = 3^2$, logo nas condições do Teorema IV.4 temos que $u = 1$ e $j = 2$. Assim segue que $|D(\mathbb{K}_1/\mathbb{Q})| = 3^{\beta_{(1,2)}}$, onde $\beta_{(1,2)} = (4.3^2 - \frac{3^3-1}{2}) - 1 = 22$. Portanto $|D(\mathbb{K}_1/\mathbb{Q})| = 3^{22}$. Para $\mathbb{K}_2$ temos que $[\mathbb{K}_2 : \mathbb{Q}] = 6 = 2.3$, logo nas condições do Teorema IV.4 temos que $u = 2$ e $j = 1$. Assim $|D(\mathbb{K}_2/\mathbb{Q})| = 3^{\beta_{(2,1)}}$, onde $\beta_{(2,1)} = 2(3.3 - \frac{3^2-1}{2}) - 1 = 9$. Portanto $|D(\mathbb{K}_2/\mathbb{Q})| = 3^9$. Analogamente para $\mathbb{K}_3$ temos que $[\mathbb{K}_3 : \mathbb{Q}] = 3$, logo $u = 1$ e $j = 1$, e assim segue que $|D(\mathbb{K}_3/\mathbb{Q})| = 3^{\beta_{(1,1)}}$, onde $\beta_{(1,1)} = (3.3 - \frac{3^2-1}{2}) - 1 = 4$. Finalmente, para $\mathbb{K}_4$ temos que $[\mathbb{K}_4 : \mathbb{Q}] = 2$, logo $u = 2$ e $j = 0$, e assim segue que $|D(\mathbb{K}_4/\mathbb{Q})| = 3^{\beta_{(2,0)}}$, onde $\beta_{(2,0)} = 2(2 - \frac{3-1}{3-1}) - 1 = 1$. Portanto $|D(\mathbb{K}_4/\mathbb{Q})| = 3$. Para $\mathbb{K}_0 = \mathbb{Q}(\zeta_{27})$ podemos aplicar o Corolário IV.1 e assim segue que $|D(\mathbb{K}_0/\mathbb{Q})| = 3^{\beta_{(1,2)}}$, onde $\beta_{(1,2)} = 2(4.9 - \frac{3^3-1}{3-1}) - 1 = 2(36-13) - 1 = 45$. Portanto $|D(\mathbb{K}_0/\mathbb{Q})| = 3^{45}$.

Corolário IV.4: O discriminante do subcorpo maximal real $\mathbb{K} = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$ do corpo $\mathbb{Q}(\zeta_{p^r})$ é dado por

$$|D(\mathbb{K}/\mathbb{Q})| = p^{\beta_{(\frac{p-1}{2},r-1)}},$$

onde $\beta_{(\frac{p-1}{2},r-1)} = \frac{1}{2}((r+1)(p-1)p^{r-1} - p^r - 1)$.

Exemplo IV.6: Para $n = 3^2$, o discriminante do subcorpo $\mathbb{K} = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$ do corpo $\mathbb{Q}(\zeta_9)$ é dado por $|D(\mathbb{K}/\mathbb{Q})| = 3^{\beta_{(1,1)}}$, onde $\beta_{(1,1)} = \frac{1}{2}(3.2.3 - 9 - 1) = \frac{1}{2}(18-10) = \frac{1}{2}(8) = 4$. Portanto $|D(\mathbb{K}/\mathbb{Q})| = 3^4$.

	χ_0	χ_1	χ_2	χ_3	χ_4	χ_5	χ_6	χ_7	χ_8	χ_9	χ_{10}	χ_{11}	χ_{12}	χ_{13}	χ_{14}	χ_{15}	χ_{16}	χ_{17}
2^0=1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$2^1 = 2$	1	ζ_{18}	ζ_{18}^2	ζ_{18}^3	ζ_{18}^4	ζ_{18}^5	ζ_{18}^6	ζ_{18}^7	ζ_{18}^8	-1	ζ_{18}^{10}	ζ_{18}^{11}	ζ_{18}^{12}	ζ_{18}^{13}	ζ_{18}^{14}	ζ_{18}^{15}	ζ_{18}^{16}	ζ_{18}^{17}
$2^2 = 4$	1	ζ_{18}^2	ζ_{18}^4	ζ_{18}^6	ζ_{18}^8	ζ_{18}^{10}	ζ_{18}^{12}	ζ_{18}^{14}	ζ_{18}^{16}	1	ζ_{18}^2	ζ_{18}^4	ζ_{18}^6	ζ_{18}^8	ζ_{18}^{10}	ζ_{18}^{12}	ζ_{18}^{14}	ζ_{18}^{16}
$2^3 = 8$	1	ζ_{18}^3	ζ_{18}^6	-1	ζ_{18}^{12}	ζ_{18}^{15}	1	ζ_{18}^3	ζ_{18}^6	-1	ζ_{18}^{12}	ζ_{18}^{15}	1	ζ_{18}^3	ζ_{18}^6	-1	ζ_{18}^{12}	ζ_{18}^{15}
$2^4 = 16$	1	ζ_{18}^4	ζ_{18}^8	ζ_{18}^{12}	ζ_{18}^{16}	ζ_{18}^2	ζ_{18}^6	ζ_{18}^{10}	ζ_{18}^{14}	1	ζ_{18}^4	ζ_{18}^8	ζ_{18}^{12}	ζ_{18}^{16}	ζ_{18}^2	ζ_{18}^6	ζ_{18}^{10}	ζ_{18}^{14}
$2^5 = 5$	1	ζ_{18}^5	ζ_{18}^{10}	ζ_{18}^{15}	ζ_{18}^2	ζ_{18}^7	ζ_{18}^{12}	ζ_{18}^{17}	ζ_{18}^4	-1	ζ_{18}^{14}	ζ_{18}^6	ζ_{18}^1	ζ_{18}^{16}	ζ_{18}^3	ζ_{18}^8	ζ_{18}^{13}	
$2^6 = 10$	1	ζ_{18}^6	ζ_{18}^{12}	1	ζ_{18}^6	ζ_{18}^{12}	1	ζ_{18}^6	ζ_{18}^{12}	1	ζ_{18}^6	ζ_{18}^{12}	1	ζ_{18}^6	ζ_{18}^{12}	1	ζ_{18}^6	ζ_{18}^{12}
$2^7 = 20$	1	ζ_{18}^7	ζ_{18}^{14}	ζ_{18}^3	ζ_{18}^{10}	ζ_{18}^{17}	ζ_{18}^6	ζ_{18}^{13}	ζ_{18}^2	-1	ζ_{18}^{16}	ζ_{18}^5	ζ_{18}^{12}	ζ_{18}^8	ζ_{18}^{15}	ζ_{18}^4		
$2^8 = 13$	1	ζ_{18}^8	ζ_{18}^{16}	ζ_{18}^6	ζ_{18}^{14}	ζ_{18}^4	ζ_{18}^{12}	ζ_{18}^2	ζ_{18}^{10}	1	ζ_{18}^8	ζ_{18}^{16}	ζ_{18}^6	ζ_{18}^{14}	ζ_{18}^4	ζ_{18}^{12}	ζ_{18}^2	ζ_{18}^{10}
$2^9 = 26$	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1
$2^{10} = 25$	1	ζ_{18}^{10}	ζ_{18}^2	ζ_{18}^{12}	ζ_{18}^4	ζ_{18}^{14}	ζ_{18}^6	ζ_{18}^{16}	ζ_{18}^8	1	ζ_{18}^{10}	ζ_{18}^2	ζ_{18}^{12}	ζ_{18}^4	ζ_{18}^{14}	ζ_{18}^6	ζ_{18}^{16}	ζ_{18}^8
$2^{11} = 23$	1	ζ_{18}^{11}	ζ_{18}^4	ζ_{18}^{15}	ζ_{18}^8	ζ_{18}^{12}	ζ_{18}^5	ζ_{18}^{16}	ζ_{18}^4	-1	ζ_{18}^4	ζ_{18}^{17}	ζ_{18}^{12}	ζ_{18}^7	ζ_{18}^2	ζ_{18}^{15}	ζ_{18}^{10}	ζ_{18}^7
$2^{12} = 19$	1	ζ_{18}^{12}	ζ_{18}^6	1	ζ_{18}^{12}	ζ_{18}^6	1	ζ_{18}^{12}	ζ_{18}^6	1	ζ_{18}^{12}	ζ_{18}^6	1	ζ_{18}^{12}	ζ_{18}^6	1	ζ_{18}^{12}	ζ_{18}^6
$2^{13} = 11$	1	ζ_{18}^{13}	ζ_{18}^8	ζ_{18}^3	ζ_{18}^6	ζ_{18}^{11}	ζ_{18}^6	ζ_{18}^{13}	ζ_{18}^{14}	-1	ζ_{18}^4	ζ_{18}^{18}	ζ_{18}^{12}	ζ_{18}^7	ζ_{18}^2	ζ_{18}^{15}	ζ_{18}^{10}	ζ_{18}^5
$2^{14} = 22$	1	ζ_{18}^{14}	ζ_{18}^{10}	ζ_{18}^6	ζ_{18}^2	ζ_{18}^{16}	ζ_{18}^{12}	ζ_{18}^8	ζ_{18}^4	1	ζ_{18}^{14}	ζ_{18}^{10}	ζ_{18}^6	ζ_{18}^2	ζ_{18}^{16}	ζ_{18}^{12}	ζ_{18}^8	ζ_{18}^4
$2^{15} = 17$	1	ζ_{18}^{15}	ζ_{18}^{12}	-1	ζ_{18}^6	ζ_{18}^3	1	ζ_{18}^{15}	ζ_{18}^{12}	-1	ζ_{18}^6	ζ_{18}^3	1	ζ_{18}^{15}	ζ_{18}^{12}	-1	ζ_{18}^6	ζ_{18}^3
$2^{16} = 7$	1	ζ_{18}^{16}	ζ_{18}^{14}	ζ_{18}^{12}	ζ_{18}^{10}	ζ_{18}^8	ζ_{18}^6	ζ_{18}^4	ζ_{18}^2	1	ζ_{18}^{16}	ζ_{18}^{14}	ζ_{18}^{12}	ζ_{18}^{10}	ζ_{18}^8	ζ_{18}^6	ζ_{18}^4	ζ_{18}^2
$2^{17} = 14$	1	ζ_{18}^{17}	ζ_{18}^{16}	ζ_{18}^{15}	ζ_{18}^{14}	ζ_{18}^{13}	ζ_{18}^{12}	ζ_{18}^{11}	ζ_{18}^{10}	-1	ζ_{18}^8	ζ_{18}^7	ζ_{18}^6	ζ_{18}^5	ζ_{18}^4	ζ_{18}^3	ζ_{18}^2	ζ_{18}
f_{χ_i}	1	3^3	3^3	3^2	3^3	3^3	3^2	3^3	3^3	3	3^3	3^3	3^2	3^3	3^3	3^2	3^3	3^3

Exemplo IV.7: Para $n = 3^3$, o discriminante do subcorpo $\mathbb{K} = \mathbb{Q}(\zeta_{27} + \zeta_{27}^{-1})$ do corpo $\mathbb{Q}(\zeta_{27})$ é dado por $|D(\mathbb{K}/\mathbb{Q})| = 3^{\beta_{(1,2)}}$, onde $\beta_{(1,2)} = \frac{1}{2}(4.2.9 - 27 - 1) = \frac{1}{2}(44) = 22$. Portanto $|D(\mathbb{K}/\mathbb{Q})| = 3^{22}$.

V. Discriminante mínimo

Nesta seção apresentamos alguns resultados para o cálculo do discriminante mínimo de subcorpos de $\mathbb{Q}(\zeta_{p^r})$.

Proposição V.3: [2] Se $\mathbb{K}$ é um corpo de números abeliano com $[\mathbb{K} : \mathbb{Q}] = p$ primo, então o discriminante mínimo de $\mathbb{K}$ é o menor valor entre $p^{2(p-1)}$ e $(kp+1)^{p-1}$, onde k é inteiro positivo e $(kp+1)$ é primo.

Exemplo V.8: O discriminante mínimo de uma cúbica galoisiana é 49.

Teorema V.5: [2] Se $\mathbb{K}$ é um corpo de números de condutor p^α, então

$$\frac{p^{\alpha[\mathbb{K}:\mathbb{Q}]}}{p^{p^\alpha - 1}} \leq \mid D(\mathbb{K}/\mathbb{Q}) \mid \leq p^{\alpha([\mathbb{K}:\mathbb{Q}]-1)}.$$

Teorema V.6: [2] Se $\mathbb{K}$ é um corpo de números de condutor p^α, então

$$p^{\alpha(1-1/p)[\mathbb{K}:\mathbb{Q}]} \leq \mid D(\mathbb{K}/\mathbb{Q}) \mid \leq p^{\alpha([\mathbb{K}:\mathbb{Q}]-1)}.$$

VI. Reticulados

Nesta seção apresentamos as definições de reticulado, empacotamento esférico, densidade de empacotamento, densidade de centro e homomorfismo canônico. Através do homomorfismo canônico, obtemos um método para gerar reticulados no $\mathbb{R}^n$. Os reticulados obtidos desta maneira dependem diretamente do anel de inteiros do corpo de números. Lembramos que os reticulados de maior interesse são aqueles com maior densidade de empacotamento.

Definição VI.7: Seja V um espaço vetorial de dimensão finita n sobre um corpo $\mathbb{K}$, $A \subset \mathbb{K}$ um anel e $v_1, \cdots, v_m$ vetores de V linearmente independentes sobre $\mathbb{K}$, com $m \leq n$. Chama-se reticulado com base $\beta = \{v_1, \cdots, v_m\}$ ao conjunto de elementos de V da forma

$$\left\{ x = \sum_{i=1}^{m} a_i v_i, \text{com } a_i \in A \right\},$$

que será denotado por $\mathcal{H}_\beta$.

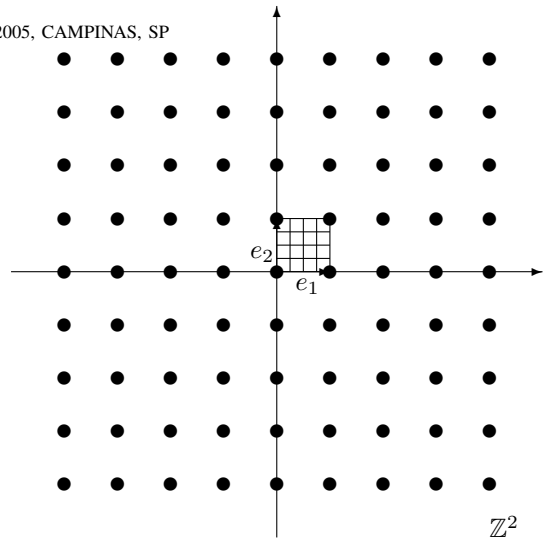
Definição VI.8: Seja $\mathcal{H}_\beta \subset \mathbb{R}^n$ um reticulado, com $\mathbb{Z}$-base $\beta = \{v_1, \cdots, v_m\}$. O conjunto

$$\mathcal{P}_\beta = \left\{ x \in \mathbb{R}^n : x = \sum_{i=1}^{n} \lambda_i v_i, 0 \leq \lambda_i < 1 \right\},$$

é chamado de região fundamental de $\mathcal{H}_\beta$, com relação a base $\{v_1, \cdots, v_m\}$.

Se $\mathcal{H}_\beta$ é um reticulado com base $\beta = \{v_1, \cdots, v_m\}$ e se $\{e_1, \cdots, e_n\}$ são elementos quaisquer de $\mathcal{H}_\beta$, então $e_i = \sum_{j=1}^{n} a_{ij} v_j$, com $a_{ij} \in \mathbb{Z}$. Temos que uma condição necessária e suficiente para que $\{e_1, \cdots, e_m\}$ seja uma base de $\mathcal{H}_\beta$ é que $det(a_{ij})$ seja um elemento inversível de $\mathbb{Z}$.

Exemplo VI.9: $\mathcal{H}_\beta = \mathbb{Z}^2$ é um reticulado gerado pelos vetores $e_1 = (1, 0)$ e $e_2 = (0, 1)$ com região fundamental descrita na figura abaixo.



Definição VI.9: Um subconjunto $\mathcal{H}$ do $\mathbb{R}^n$ é discreto se para qualquer subconjunto compacto $\mathbb{K}$ do $\mathbb{R}^n$, tivermos que $\mathcal{H} \cap \mathbb{K}$ finito.

Exemplo VI.10: $\mathbb{Z}^n$ é um exemplo de subconjunto discreto do $\mathbb{R}^n$.

O próximo teorema afirma que um reticulado é gerado sobre $\mathbb{Z}$ por uma base do $\mathbb{R}^n$.

Teorema VI.7: [5] Se $\mathcal{H}$ é um subgrupo discreto do $\mathbb{R}^n$, então $\mathcal{H}$ é gerado como um $\mathbb{Z}$-módulo por r vetores linearmente independentes sobre $\mathbb{R}$, com $r \leq n$.

Observação VI.6: Do Teorema VI.7 segue que qualquer subgrupo discreto do $\mathbb{R}^n$ é um reticulado.

Definição VI.10: Seja $\mathcal{H} \subset \mathbb{R}^n$ um reticulado, $\beta = \{v_1, \cdots, v_n\}$ uma base de $\mathcal{H}$ e $\mathcal{P}_v$ a região fundamental. Se $v_i = (v_{i1}, \cdots, v_{in})$, para $i = 1, \cdots, n$, definimos o volume da região fundamental $\mathcal{P}_\beta$ como o módulo do determinante da matriz

$$\begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ v_{n1} & v_{n2} & \cdots & v_{nn} \end{pmatrix}.$$

Proposição VI.4: [6] O volume da região fundamental $Vol(\mathcal{P}_\beta)$ independe da base β de $\mathcal{H}$.

Observamos que, sendo β' uma outra base de $\mathcal{H}_\beta$, segue que Vol$(\mathcal{H}_\beta)$ = Vol$(\mathcal{H}_{\beta'})$, pois β e β' diferem pelo produto de uma matriz inversível com entradas inteiras. Dessa forma, faz sentido definir o volume de $\mathcal{H}_\beta$ como sendo o volume de uma região fundamental.

Definição VI.11:

1) Um empacotamento esférico, ou simplesmente um empacotamento no $\mathbb{R}^n$, é uma distribuição de esferas de mesmo raio no $\mathbb{R}^n$ de forma que a interseção de quaisquer duas esferas tenha no máximo um ponto. Pode-se descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio.
2) Um empacotamento reticulado é um empacotamento em que o conjunto dos centros das esferas formam um reticuldo $\mathcal{H}_\beta$ de $\mathbb{R}^n$.
3) Dado um empacotamento no $\mathbb{R}^n$, associado a um reticulado $\mathcal{H}_\beta$, com $\rho = \{v_1, \cdots, v_n\}$ uma $\mathbb{Z}$-base, definimos a densidade de empacotamento como sendo a proporção do espaço $\mathbb{R}^n$ coberto pela união das esferas.

Estamos interessados no empacotamento associado a um reticulado $\mathcal{H}_\beta$ em que as esferas tenham raio máximo. Para a determinação deste raio, observe que fixado $k > 0$, a interseção do conjunto compacto $\{x \in \mathbb{R}^n; |x| \leq k\}$ com o reticulado $\mathcal{H}_\beta$ é um conjunto finito, de onde segue que o número $\mathcal{H}_{\beta_{min}} = min\{|\lambda|; \lambda \in \mathcal{H}_\beta, \lambda \neq 0\}$ está bem definido e $(\mathcal{H}_{\beta_{min}})^2$ é chamado de norma mínima. Observamos que $\rho = \frac{\mathcal{H}_{\beta_{min}}}{2}$ é o maior raio para o qual é possível distribuir esferas centradas nos pontos de $\mathcal{H}_\beta$ e obter um empacotamento. Dessa forma, estudar os empacotamentos reticulados equivale ao estudo dos reticulados.

Denotando por $\mathcal{B}(\rho)$ a esfera com centro na origem e raio ρ, temos que a densidade de empacotamento de $\mathcal{H}_\beta$ é dada por

$$\Delta(\mathcal{H}_\beta) = \frac{\text{volume da região coberta pelas esferas}}{\text{volume da região fundamental}} = \\ = \frac{\text{Vol}(\mathcal{B}(\rho))}{\text{Vol}(\mathcal{H}_\beta)} = \frac{\text{Vol}(\mathcal{B}(1))\rho^n}{\text{Vol}(\mathcal{H}_\beta)}.$$

Portanto, o problema se reduz ao estudo de um outro parâmetro, chamado densidade de centro, que é dado por $\delta(\mathcal{H}_\beta) = \frac{\rho^n}{\text{Vol}(\mathcal{H}_\beta)}$.

Exemplo VI.11: Se $\mathcal{H}_\beta = \mathbb{Z}^2$ com base $(1,0)$ e $(0,2)$, temos que $\rho = 1/2$, $\text{Vol}(\mathcal{B}(1)) = \pi$, o volume do reticulado $\text{Vol}(\mathcal{H}_\beta) = 2$, a densidade de empacotamento é $\Delta(\mathcal{H}_\beta) = \text{Vol}(\mathcal{B}(1)).\frac{\rho^2}{\text{Vol}(\mathcal{H}_\beta)} = \pi\frac{1}{4}\frac{1}{2} = \frac{\pi}{8}$ e a densidade de centro é $\delta(\mathcal{H}_\beta) = 1/8$.

VII. Reticulados via corpos de números

Nesta seção descrevemos o método de Minkowiski, para a geração de reticulados via ideais de corpos de números.

Sejam $\mathbb{K}$ um corpo de números e n seu grau. Temos que existem n monomorfismos distintos $\sigma_i : \mathbb{K} \to \mathbb{C}$, pois o polinômio minimal de um elemento primitivo de $\mathbb{K}$ sobre $\mathbb{Q}$ tem somente n raízes em $\mathbb{C}$. Se $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$ diz-se que σ_i é real, caso contrário, σ_i é dito imaginário. Quando todos os monomorfismos são reais diz-se que $\mathbb{K}$ é um corpo totalmente real e quando os monomorfismos são todos imaginários diz-se que $\mathbb{K}$ é um corpo totalmente imaginário. Se $\alpha : \mathbb{C} \to \mathbb{C}$ é a conjugação complexa, então para todo $i = 1, \ldots, n$, temos que $\alpha \circ \sigma_i = \sigma_k$, para algum $1 \leq k \leq n$, e que $\sigma_i = \sigma_k$ se, e somente se, $\sigma_i(\mathbb{K}) \subset \mathbb{R}$. Assim, usando r_1 para denotar o número de índices, tal que $\sigma_i(\mathbb{K}) \subset \mathbb{R}$, podemos ordenar os monomorfismos $\sigma_1, \ldots, \sigma_n$ de tal modo que $\sigma_1, \ldots, \sigma_{r_1}$ sejam os monomorfismos reais e que $\sigma_{r_1+r_2+i} = \overline{\sigma_{r_1+i}}$, para $i = 1, \ldots, r_2$. Então $n - r_1$ é um número par, assim podemos escrever $r_1 + 2r_2 = n$. Daí, para cada $x \in \mathbb{K}$, temos que o homomorfismo $\sigma_k : \mathbb{K} \longrightarrow \mathbb{R}^n$ definido por

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

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

$$\sigma_k(x) = (\sigma_1(x), \ldots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)),$$

onde as notações $\Re(x)$ e $\Im(x)$ representam as partes real e imaginária do número complexo x, respectivamente.

Uma das aplicações deste homomorfismo é a geração de reticulados no $\mathbb{R}^n$, onde os principais parâmetros podem ser obtidos via teoria algébrica dos números, através de propriedades herdadas de $\mathbb{K}$. Isto pode ser visto de maneira formal nos resultados que seguem.

Proposição VII.5: [5] Seja $\mathbb{K}$ um corpo de números de grau n. Se $M \subseteq \mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto n e se $(x_j)_{1\leq j\leq n}$ é uma $\mathbb{Z}$-base de M, então $\sigma_k(M)$ é um reticulado no $\mathbb{R}^n$, com volume dado por

$$\mathcal{V}ol(\sigma_k(M)) = 2^{-r_2}|\det_{1\leq j,\, k\leq n}(\sigma_j(x_k))|.$$

Definição VII.12: Sejam $\mathbb{K}$ um corpo de números de grau finito n e $I_\mathbb{K}(A)$ o seu anel de inteiros. A norma de um ideal $\mathcal{A}$ do anel $I_\mathbb{K}(A)$ é definida como $\mathcal{N}(\mathcal{A}) = \#I_\mathbb{K}(A)/\mathcal{A}$.

Proposição VII.6: [5] Seja $\mathbb{K}$ um corpo de números de grau n. Sejam $D_\mathbb{K}$ o discriminante de $\mathbb{K}$, $I_\mathbb{K}(A)$ o anel dos inteiros de $\mathbb{K}$ e $\mathcal{A}$ um ideal não nulo de $I_\mathbb{K}(A)$. Então, $\sigma_k(I_\mathbb{K}(A))$ e $\sigma_k(\mathcal{A})$ são reticulados, com respectivos volumes,

$$\mathcal{V}ol(\sigma_k(I_\mathbb{K}(A))) = 2^{-r_2}|D_\mathbb{K}|^{\frac{1}{2}} \quad \text{e} \\ \mathcal{V}ol(\sigma_k(\mathcal{A})) = 2^{-r_2}|D_\mathbb{K}|^{\frac{1}{2}}\mathcal{N}(\mathcal{A}),$$

onde r_2 é o número de monomorfismos imaginários.

Como conseqüência das Proposições $VII.5$ e $VII.6$, temos que a densidade de centro destes reticulados é dada por

$$\delta(\sigma_k(\mathcal{A})) = \frac{2^{r_2}(\rho(\sigma_k(\mathcal{A})))^n}{|D_\mathbb{K}|^{\frac{1}{2}}\mathcal{N}(\mathcal{A})}.$$

Exemplo VII.12: Seja o corpo ciclotômico $\mathbb{Q}(\zeta_9)$. Temos que o seu grau é 6, $\mathbb{K} = \mathbb{Q}(\zeta_9+\zeta_9^{-1})$ tem grau 3 e $\mathbb{Z}[\zeta_9+\zeta_9^{-1}]$. Pelo Corolário IV.3 temos que o discriminante de $\mathbb{K}$ é 81 e assim a densidade de centro de $\sigma_k(I_\mathbb{K}(\mathbb{Z}[\alpha]))$ é igual a $0,041667$. Para dimensão 3, o reticulado conhecido com maior densidade de centro é da família dos laminados, cuja densidade de centro é $0,17678$. Deste modo, do ponto de vista do empacotamento esférico este reticulado não tem bom desempenho. Entretanto, tomando o ideal principal $\mathcal{A} = \langle 2-\alpha\rangle$ temos que a densidade de centro do reticulado $\sigma_k(I_\mathbb{K}(\mathcal{A}))$ é igual a $0,125$, superando a densidade de centro do reticulado $\sigma_k(I_\mathbb{K}(\mathbb{Z}[\alpha]))$, mas muito distante da densidade de centro de Λ_3.

VIII. Conclusões

Neste trabalho apresentamos o estudo do cálculo de discriminante de subcorpos de $\mathbb{Q}(\zeta_{p^r})$, alguns resultados para a obtenção de discriminante mínimo de seus subcorpos e a conexão desses resultados com a teoria da informação. Esta conexão está fundamentada na busca de reticulados algébricos, com boa densidade de centro, obtidos via homomorfismo de Minkowisk. Uma vez que a fórmula da densidade de centro de tais reticulados envolve o discriminante de um corpo de números, o objetivo principal deste trabalho foi de dar condições para a obtenção de corpos com discriminante mínimo.

Agradecimentos

Agradecemos a Capes pelo apoio.

REFERÊNCIAS

[1] J.H. Conway, N.J.A Sloane, *Sphere packing, lattices and groups.* Springer-Verlag, 1988.

[2] T.P. Nóbrega Neto, J.O.D. Lopes e J.C. Interlando, "The discriminant of the abelian number fields."To appear.

[3] L.C. Washington, *Introduction to Ciclotomic Fields*. Springer-Verlag, 1982.

[4] T.P. Nóbrega Neto, J.O.D. Lopes, e J.C. Interlando, "On computing discriminants of subfields $\mathbb{Q}(\zeta_{p^r})$," *Journal of Number Theory*, No.96, pp. 319-325, 2002.

[5] P. Samuel, *Algebraic theory of numbers*. Herman, 1967.

[6] O. Endler, *Teoria dos Números Algébricos*. Projeto Euclides, 1986.