

# Uma nota sobre discriminante mínimo\*

Cátia Regina de Oliveira Quilles<sup>†</sup>

Antonio Aparecido de Andrade,

Departamento de Matemática, IBILCE, UNESP,

15054-000, São José do Rio Preto, SP

E-mail: catia.quilles@pop.com.br, andrade@ibilce.unesp.br.

## 1 Introdução

Os reticulados têm se mostrado bastante úteis em aplicações na teoria das comunicações. Contudo os reticulados de maior interesse são aqueles com maior densidade de empacotamento, o qual podemos obter tomando o discriminante mínimo. Neste trabalho apresentamos algumas formas para o cálculo do discriminante e encontramos alguns discriminantes mínimos.

## 2 Caracteres de Dirichlet

Nesta seção apresentamos os caracteres de Dirichlet, seus condutores e algumas propriedades que serão úteis para o cálculo do discriminante de subcorpos. 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 2.1** *Sejam  $G$  um grupo,  $\mathbb{K}$  um corpo e  $\mathbb{K}^*$  o grupo multiplicativo dos elementos inversíveis de  $\mathbb{K}$ . Um homomorfismo de grupos  $\sigma : G \rightarrow \mathbb{K}^*$  é chamado de caracter de  $G$  em  $\mathbb{K}$ .*

### Observação 2.1

1. Pelo Lema de Dedekind temos que se  $\{\sigma_1, \dots, \sigma_n\}$  são caracteres distintos de  $G$  em  $\mathbb{K}^*$ , então  $\{\sigma_1, \dots, \sigma_n\}$  é linearmente independente.
2. O conjunto dos caracteres forma um grupo.

**Definição 2.2** *Um homomorfismo multiplicativo  $\chi : (\mathbb{Z}/n\mathbb{Z})^* \rightarrow \mathbb{C}^*$  é chamado de caracter de Dirichlet, definido módulo  $n$ .*

**Observação 2.2** *Um caracter de Dirichlet módulo  $n$  é uma função  $\chi$  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  $m$  e  $a$  inteiros positivos,

\*Realização SBMAC

<sup>†</sup>Aluna de mestrado

4.  $\chi(a) = 0$ , para todo  $a$  tal que  $\text{mdc}(a, n) \neq 1$ .

**Exemplo 2.1** *Uma função  $\chi$  dada por  $\chi(a) = (-1)^{\frac{a-1}{2}}$ , para todo  $a$  ímpar e  $\chi(a) = 0$ , para todo  $a$  par, é um caracter de Dirichlet módulo 4, pois satisfaz as condições da Observação 2.2, para  $n = 4$ .*

**Observação 2.3** *Sejam  $n$  e  $m$  inteiros positivos. Se  $n$  divide  $m$ , então o caracter  $\chi : (\mathbb{Z}/n\mathbb{Z})^* \rightarrow (\mathbb{C})^*$  induz um homomorfismo  $\chi' : (\mathbb{Z}/m\mathbb{Z})^* \rightarrow (\mathbb{C})^*$ , via a composição com o homomorfismo canônico sobrejetor  $\theta : (\mathbb{Z}/m\mathbb{Z})^* \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$ .*

**Definição 2.3** *Seja  $\chi$  um caracter de Dirichlet. Definimos o condutor de  $\chi$  e denotamos por  $f_\chi$ , o menor valor de  $n$  para o qual  $\chi$  está definido.*

**Observação 2.4** *Podemos estender o homomorfismo  $\chi$  a uma função  $\chi' : \mathbb{Z} \rightarrow \mathbb{C}$  tomando  $\chi(a) = 0$  se  $\text{mdc}(a, f_\chi) \neq 1$ .*

**Exemplo 2.2** *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:*

	$\chi_0$	$\chi_1$	$\chi_2$	$\chi_3$
1	1	1	1	1
3	1	1	-1	-1
7	1	-1	1	-1
9	1	-1	-1	1
$f_\chi$	1	5	5	5

Os caracteres  $\chi_1, \chi_2$  e  $\chi_3$  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  $\chi_i$  é  $f_{\chi_i} = 5$ ,  $i = 1, 2, 3$ .

**Teorema 2.1** [1] *Seja  $\chi$  um caracter de Dirichlet definido módulo  $m$ . Se  $n$  divide  $m$ , então o condutor de  $\chi$  é  $n$  se, e somente se, quando  $\text{mdc}(a, m) = 1$  e  $a \equiv 1 \pmod{n}$ ,  $\chi(a) = 1$ .*

**Exemplo 2.3** *Seja  $G = (\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$ . 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:*

	$\chi_0$	$\chi_1$	$\chi_2$	$\chi_3$
1	1	1	1	1
3	1	1	-1	-1
5	1	-1	1	-1
7	1	-1	-1	1
$f_\chi$	1	8	4	8

Pelo Teorema 2.1 o condutor do caracter  $\chi_2$  é  $f_{\chi_2} = 4$ , pois  $4|8$ ,  $\text{mdc}(5, 8) = 1$ ,  $5 \equiv 1 \pmod{4}$  e  $\chi_2(5) = 1$ .

**Definição 2.4** Um caracter de Dirichlet definido módulo o seu condutor é chamado caracter primitivo.

**Exemplo 2.4** No Exemplo 2.3 os caracteres  $\chi_1$  e  $\chi_3$  definidos módulo 8 são primitivos. O caracter  $\chi_2$  não é primitivo, pois seu condutor é  $f_{\chi_2} = 4$ .

### Observação 2.5

1. A vantagem de usarmos caracteres de Dirichlet primitivos é evidente quando tomamos um produto de vários 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  $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$  com  $(\mathbb{Z}/n\mathbb{Z})^*$ , então o caracter de Dirichlet módulo  $n$  é um caracter de Galois.

**Exemplo 2.5** No Exemplo 2.2, temos que  $(\mathbb{Z}/10\mathbb{Z})^* \simeq \text{Gal}(\mathbb{Q}(\zeta_{10})/\mathbb{Q})$ . Mas temos que  $\mathbb{Q}(\zeta_5) \subseteq \mathbb{Q}(\zeta_{10})$  e  $[\mathbb{Q}(\zeta_{10}) : \mathbb{Q}] = 2 = [\mathbb{Q}(\zeta_5) : \mathbb{Q}]$ , logo  $\mathbb{Q}(\zeta_{10}) = \mathbb{Q}(\zeta_5)$ . Então um caracter módulo 10 e um módulo 5 são caracteres do mesmo grupo de Galois.

**Exemplo 2.6** No Exemplo 2.3, temos que  $(\mathbb{Z}/8\mathbb{Z})^* \simeq \text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ . O núcleo do caracter  $\chi_2$  é  $\{1, 5 \pmod{10}\}$ . Assim, seja  $\mathbb{K}$  o corpo fixo por  $\{\sigma_1, \sigma_5\}$ . Como  $\zeta_8^8 = 1$  e  $\zeta_8^4 = -1$  segue que  $\sigma_5(a_0 + a_1\zeta_8 + a_2\zeta_8^2 + a_3\zeta_8^3) = a_0 + a_1\zeta_8^2 + a_2\zeta_8^{10} + a_3\zeta_8^{15} = a_0 - a_1\zeta_8 + a_2\zeta_8^2 - a_3\zeta_8^3$ . Temos que  $\zeta_8^2$  é uma raiz 4-ésima da unidade e  $\{1, \zeta_8^2\}$  gera  $\mathbb{Q}(\zeta_4)$ , então  $\mathbb{K} = \mathbb{Q}(\zeta_4)$ . Assim,  $\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}(\zeta_4)) \simeq \{\sigma_1, \sigma_5\}$ , e temos que  $\chi_2 : \frac{(\mathbb{Z}/8\mathbb{Z})^*}{\{1, 5\}} \rightarrow \mathbb{C}^*$ , mas  $\frac{(\mathbb{Z}/8\mathbb{Z})^*}{\{1, 5\}} \simeq \frac{\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})}{\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}(\zeta_4))} \simeq \text{Gal}(\mathbb{Q}(\zeta_4)/\mathbb{Q}) \simeq (\mathbb{Z}/4\mathbb{Z})^*$ . Portanto,  $\chi_2$  é um caracter de  $(\mathbb{Z}/4\mathbb{Z})^*$ .

**Definição 2.5** Se  $\chi$  é um caracter de Dirichlet do grupo de Galois  $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$  e  $\mathbb{K}$  o corpo fixo do núcleo de  $\chi$ , então  $\mathbb{K}$  é chamado corpo associado a  $\chi$ .

### Observação 2.6

1. O corpo  $\mathbb{K}$  associado a  $\chi$  é um subcorpo de  $\mathbb{Q}(\zeta_n)$ , e se  $n$  é o menor valor, então é o condutor de  $\chi$ .
2. O corpo  $\mathbb{K}$  depende somente de  $\chi$ .

Mais geralmente, se  $X$  é um grupo finito de caracteres de Dirichlet e  $\text{mmc}(f_{\chi_i}) = n$ , onde  $\chi_i \in X$ , então  $X$  é um subgrupo do grupo dos caracteres de Dirichlet,  $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ .

**Definição 2.6** Seja  $X$  um grupo finito de caracteres de Dirichlet,  $H$  a intersecção dos núcleos destes caracteres e  $\mathbb{K}$  o corpo fixo de  $H$ . O corpo  $\mathbb{K}$  é chamado corpo associado a  $X$ .

### Observação 2.7

1. Como  $X$  é isomorfo a  $\text{Gal}(\mathbb{K}/\mathbb{Q})$ , o grau de  $\mathbb{K}/\mathbb{Q}$  é igual a ordem de  $X$ .
2. Se  $X$  é cíclico, gerado por  $\chi$ , então  $\mathbb{K}$  é precisamente o mesmo corpo associado a  $\chi$  mencionado acima.

**Exemplo 2.7** Se  $X$  é o grupo de caracteres de  $(\mathbb{Z}/n\mathbb{Z})^*$  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  $\mathbb{Q}(\zeta_n)$ .

**Exemplo 2.8** Seja  $G = (\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\}$ . 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:

	$\chi_0$	$\chi_1$	$\chi_2$	$\chi_3$	
1	1	1	1	1	$\sigma_1$
5	1	1	-1	-1	$\sigma_5$
7=-5	1	-1	-1	1	$\sigma_7$
11=-1	1	-1	1	-1	$\sigma_{11}$
$f_\chi$	1	4	12	3	

Os subgrupos multiplicativos do grupo de Galois são:

$$\begin{aligned} H_0 &= \{\sigma_1\} & H_1 &= \{\sigma_1, \sigma_5\} \\ H_2 &= \{\sigma_1, \sigma_{11}\} & H_3 &= \{\sigma_1, \sigma_7\} \\ H_4 &= G. \end{aligned}$$

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  $\mathbb{K}_2 = \mathbb{Q}(\zeta_{12}) = \mathbb{Q}(\sqrt{3})$ . 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  $G$ .

Estas noções preliminares podem ser usadas no conjunto dos caracteres dos grupos abelianos finitos, o que faremos agora.

**Proposição 2.1** [1] Se  $G$  é um grupo abeliano finito e  $\hat{G}$  é o grupo dos homomorfismos multiplicativos de  $G$  em  $\mathbb{C}^*$ , ou seja, dos caracteres de  $G$  em  $\mathbb{C}^*$ , então

1.  $G$  é isomorfo a  $\hat{\hat{G}}$ ,
2.  $G$  é isomorfo a  $\hat{G}$ .

**Proposição 2.2** [1] Se  $H$  é um subgrupo de  $G$  e  $H^\perp = \{\chi \in \hat{G} : \chi(h) = 1, \forall h \in H\}$ , então

1.  $H^\perp$  é isomorfo a  $(\widehat{G/H})$ ,
2.  $\hat{H}$  é isomorfo a  $\hat{G}/H^\perp$  e
3.  $(H^\perp)^\perp = H$ .

### 3 Discriminante

Pelo Teorema de Kronecker-Weber, se  $\mathbb{K}$  é um corpo de números abeliano, então  $\mathbb{K}$  está contido em algum corpo ciclotômico  $\mathbb{Q}(\zeta_m)$ . Deste modo, nosso objetivo aqui é apresentar formas para o cálculo do discriminante de subcorpos de corpos ciclotômicos.

**Teorema 3.1** [3] Se  $\mathbb{K}$  é um subcorpo de  $\mathbb{Q}(\zeta_{2^r})$ , onde  $r$  é um inteiro tal que  $r \geq 3$ , com  $[\mathbb{K} : \mathbb{Q}] = 2^{m-1}$  e  $H$  um subgrupo de  $\text{Gal}(\mathbb{Q}(\zeta_{2^r})/\mathbb{Q})$  que fixa  $\mathbb{K}$ , então

1.  $|D_{\mathbb{K}/\mathbb{Q}}| = 2^{2^{m-1}(m-1)}$  se  $H \simeq \langle \bar{5}^{2^{m-2}} \rangle$ ,
2.  $|D_{\mathbb{K}/\mathbb{Q}}| = 2^{m2^{m-1}-1}$ , se  $H \simeq \langle -1, \bar{5}^{2^{m-1}} \rangle$ .

**Corolário 3.1** [3] Se  $\mathbb{K}$  é um subcorpo de  $\mathbb{Q}(\zeta_{2^r})$ , tal que  $[\mathbb{K} : \mathbb{Q}] = 2^{m-1}$ , então

1. Se  $H \simeq \langle \bar{5}^{2^{m-2}} \rangle$ , o corpo fixo por  $H$  é  $\mathbb{K} = \mathbb{Q}(\zeta_{2^m})$
2. Se  $H \simeq \langle -1, \bar{5}^{2^{m-1}} \rangle$ , ou  $H \simeq \langle -\bar{5}^{2^{m-2}} \rangle$  o corpo fixo por  $H$  é  $\mathbb{K} \neq \mathbb{Q}(\zeta_{2^m})$ .

**Corolário 3.2** [3] O discriminante do corpo  $\mathbb{Q}(\zeta_{2^r})$  é dado por

$$|D(\mathbb{K})| = 2^{2^{r-1}(r-1)}$$

**Corolário 3.3** O discriminante do subcorpo maximal real  $\mathbb{K} = \mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$  do corpo  $\mathbb{Q}(\zeta_{2^r})$  é dado por

$$|D(\mathbb{K})| = 2^{(r-1)2^{r-2}-1}.$$

**Teorema 3.2** [2] Se  $\mathbb{K}$  é um subcorpo de  $\mathbb{Q}(\zeta_{p^r})$  tal que  $[\mathbb{K} : \mathbb{Q}] = up^j$ , onde  $p$  é um primo ímpar,  $r$  um inteiro positivo,  $u$  um divisor de  $(p-1)$  e  $0 < j \leq r-1$ , então

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

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

**Corolário 3.4** [2] O discriminante do corpo  $\mathbb{Q}(\zeta_{p^r})$  é dado por

$$|D(\mathbb{K})| = p^{\beta(p-1,r-1)},$$

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

**Corolário 3.5** 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

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

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

**Teorema 3.3** [4] Se  $\mathbb{K}$  é um subcorpo de  $\mathbb{Q}(\zeta_m)$ , onde  $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_n^{\alpha_n}$ , então

$$|D_{\mathbb{K}/\mathbb{Q}}| = \frac{m^{[\mathbb{K}:\mathbb{Q}]}}{n} \prod_{i=1}^n p_i^{\beta_i},$$

onde  $\beta_i = \sum_{r=1}^{\alpha_i} ([\mathbb{K} \cap \mathbb{Q}(\zeta_m/p_i^r) : \mathbb{Q}])$ .

**Corolário 3.6** [4] Se  $\mathbb{K}$  é um corpo de números de condutor  $m$  tal que  $\mathbb{K} \cap \mathbb{Q}(\zeta_m/p) = \mathbb{Q}$ , para todo divisor primo  $p$  de  $m$ , então  $|D_{\mathbb{K}/\mathbb{Q}}| = m^{[\mathbb{K}:\mathbb{Q}]-1}$ .

**Corolário 3.7** [4] Se  $\mathbb{K}$  é um corpo de números de grau primo  $p$  e condutor  $m$ , então  $|D_{\mathbb{K}/\mathbb{Q}}| = m^{p-1}$ .

**Exemplo 3.1** Se  $n = 3^2$ , então o grupo  $G$  tem ordem  $(p-1)p^{r-1} = 2 \cdot 3 = 6$  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 :

	$\chi_0$	$\chi_1$	$\chi_2$	$\chi_3$	$\chi_4$	$\chi_5$	
$2^0 = 1$	1	1	1	1	1	1	$\sigma_1$
$2^1 = 2$	1	$\zeta_6$	$\zeta_6^2$	-1	$\zeta_6^4$	$\zeta_6^5$	$\sigma_2$
$2^2 = 4$	1	$\zeta_6^2$	$\zeta_6^4$	1	$\zeta_6^2$	$\zeta_6^4$	$\sigma_4$
$2^3 = 8$	1	-1	1	-1	1	-1	$\sigma_8$
$2^4 = 7$	1	$\zeta_6^4$	$\zeta_6^2$	1	$\zeta_6^4$	$\zeta_6^2$	$\sigma_7$
$2^5 = 5$	1	$\zeta_6^5$	$\zeta_6^4$	-1	$\zeta_6^2$	$\zeta_6$	$\sigma_5$
$f_{\chi_i}$	1	3	3	3	3	3	

Os subgrupos multiplicativos do grupo de Galois são:

$$H_0 = \{\sigma_1\} \quad H_2 = \{\sigma_1, \sigma_4, \sigma_7\}$$

$$H_1 = \{\sigma_1, \sigma_8\} \quad H_3 = G = \{\sigma_1, \sigma_2, \sigma_4, \sigma_8, \sigma_7, \sigma_5\}.$$

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 3.2 temos que  $u = 1$  e  $j = 1$ . Assim  $|D(\mathbb{K}_1)| = 3^{\beta(1,1)}$ , onde  $\beta(1,1) = (3 \cdot 3 - \frac{3^2-1}{2}) - 1 = (9-4) - 1 = 4$ . Portanto  $|D(\mathbb{K}_1)| = 3^4$ . Analogamente para  $\mathbb{K}_2$  temos que  $[\mathbb{K}_2 : \mathbb{Q}] = 2$ , logo novamente nas condições do Teorema 3.2 temos que  $u = 2$  e  $j = 0$  e segue que  $|D(\mathbb{K}_2)| = 3^{\beta(2,0)}$ , onde  $\beta(2,0) = 2(3 \cdot 1 - \frac{2}{2}) - 1 = 2 - 1 = 1$ . Portanto  $|D(\mathbb{K}_1)| = 3$ . Para  $\mathbb{K}_0 = \mathbb{Q}(\zeta_9)$  podemos aplicar o Corolário 3.4 e assim segue que  $|D(\mathbb{K}_0)| = 3^{\beta(2,1)}$ , onde  $\beta(2,1) = 2(3 \cdot 3 - \frac{3^2-1}{3-1}) - 1 = 2(9-4) - 1 = 9$ . Portanto  $|D(\mathbb{K}_0)| = 9$ .

**Exemplo 3.2** Se  $n = 2^3$ , então o grupo  $G$  tem ordem  $(p-1)p^{r-1} = 2^2 = 4$  e é dado por  $G = (\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$ . O grupo de Galois de  $\mathbb{Q}(\zeta_9)$  sobre  $\mathbb{Q}$  é  $G = \{\sigma_1, \sigma_3, \sigma_5, \sigma_7\}$ . Caracterizamos o grupo  $\hat{G}$  pela tabela :

	$\chi_0$	$\chi_1$	$\chi_2$	$\chi_3$	
$5^1 = 5$	1	$\zeta_4$	-1	$\zeta_4^3$	$\sigma_1$
$5^2 = 1$	1	-1	1	-1	$\sigma_1$
$5^3 = 3$	1	$\zeta_4^3$	-1	$\zeta_4$	$\sigma_3$
$5^4 = 7$	1	1	1	1	$\sigma_7$
$f_{\chi_i}$	1	1	1	1	

Os subgrupos multiplicativos do grupo de Galois são:

$$H_0 = \{\sigma_1\} \quad H_2 = \{\sigma_1, \sigma_3, \sigma_5, \sigma_7\}$$

$$H_1 = \{\sigma_1, \sigma_7\}$$

Assim, temos que  $\mathbb{K}_0 = \mathbb{Q}(\zeta_8)$  é fixado por  $H_0$ ,  $\mathbb{K}_1$  é fixado por  $H_1$  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  $H_1^\perp = \{\chi_0, \chi_2\}$  e a  $\mathbb{K}_2$  é  $H_2^\perp = \{\chi_0\}$ . Agora, para  $\mathbb{K}_1$  temos que  $[\mathbb{K}_1 : \mathbb{Q}] = 2$ , logo nas condições do Teorema 3.1 segue que  $m = 2$ , e como  $H \simeq \langle -1, \sqrt{2} \rangle$  temos que  $|D(\mathbb{K}_1)| = 2^m \cdot 2^{m-1} = 2^{2 \cdot 2 - 1} = 2^3$ . Portanto  $|D(\mathbb{K}_1)| = 2^3$ . Para  $\mathbb{K}_0 = \mathbb{Q}(\zeta_8)$  aplicando o Corolário 3.2 obtemos  $|D(\mathbb{K}_0)| = 2^{2^{n-1}(r-1)} = 2$ . Portanto  $|D(\mathbb{K}_0)| = 2$ .

## 4 Reticulados

### Definição 4.1

1. Um subgrupo discreto  $\Lambda \subseteq \mathbb{R}^n$  é discreto se  $\Lambda \cap C$  é finito, para todo subconjunto compacto  $C \subseteq \mathbb{R}^n$ .
2. Um subgrupo discreto  $\Lambda \subseteq \mathbb{R}^n$  gerado como um  $\mathbb{Z}$ -módulo por  $n$  vetores linearmente independentes sobre  $\mathbb{R}$  é chamado um reticulado do  $\mathbb{R}^n$ .
3. Um empacotamento no  $\mathbb{R}^n$ , é uma distribuição de esferas de mesmo raio no  $\mathbb{R}^n$  de forma que a intersecção de quaisquer duas esferas tenha no máximo um ponto.
4. Dado um empacotamento no  $\mathbb{R}^n$ , associado a um reticulado  $\Lambda_\beta$ , com  $\beta = \{v_1, v_2, \dots, v_n\}$  uma  $\mathbb{Z}$ -base, definimos sua densidade de empacotamento como sendo a proporção do espaço  $\mathbb{R}^n$  coberta pela união das esferas.

Estamos interessados no empacotamento associado a um reticulado  $\Lambda_\beta$  em que as esferas tenham raio máximo. Observamos que  $\rho = \Lambda_\beta/2$  é o maior raio para o qual é possível distribuir esferas centradas nos pontos de  $\Lambda_\beta$  e obter um empacotamento. Denotando por  $B(\rho)$  a esfera com centro na origem e raio  $\rho$  temos que a densidade de empacotamento de  $\Lambda_\beta$  é dada por

$$\Delta(\Lambda_\beta) = \frac{\text{vol}(B(\rho))}{\text{vol}(\Lambda_\beta)} = \frac{\rho^n}{\text{vol}(\Lambda_\beta)} = \delta(\Lambda_\beta).$$

Portanto o problema se reduz ao estudo de um outro parâmetro, a densidade de centro  $\delta(\Lambda_\beta)$ .

Sejam  $\mathbb{K}$  um corpo de números de grau  $n$ ,  $\mathcal{O}_K$  o anel dos inteiros de  $\mathbb{K}$  e  $\mathcal{A}$  um ideal não nulo de  $\mathcal{O}_K$ . Se  $\sigma$  é o homomorfismo de Minkowsk de  $\mathbb{K}$ , então  $\sigma(\mathcal{A})$  é um reticulado e sua densidade de é dada por

$$\delta(\sigma(\mathcal{A})) = \frac{2^{r_2}(\rho(\sigma_K(\mathcal{A})))^n}{|D(K)|^{1/2}N(\mathcal{A})},$$

onde  $r_2$  é o número de monomorfismos imaginários. Deste modo, observamos que para obtermos reticulados com maior densidade de centro devemos procurar corpos de números com discriminantes mínimos.

## 5 Discriminante mínimo

Nesta seção apresentamos alguns resultados para o cálculo do discriminante mínimo de subcorpos.

**Proposição 5.1** [4] 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 5.1** O discriminante mínimo de uma cúbica galoisiana é 49.

**Teorema 5.1** [4] Se  $\mathbb{K}$  é um corpo de números de con-

dutor  $m = \prod_{i=1}^k p_i^{\alpha_i}$ , então

1.  $\frac{m^{[\mathbb{K}:\mathbb{Q}]}}{k \prod_{i=1}^k p_i^{\frac{\phi(m)}{p_i-1}}} \leq |D(\mathbb{K})| \leq m^{([\mathbb{K}:\mathbb{Q}]-1)}$ .
2.  $m^{(1-\frac{1}{p})[\mathbb{K}:\mathbb{Q}]} \leq |D(\mathbb{K})| \leq m^{([\mathbb{K}:\mathbb{Q}]-1)}$

## 6 Conclusões

Neste trabalho apresentamos o cálculo do discriminante de subcorpos e alguns discriminantes mínimos. Observamos através da densidade de centro que tomando o discriminante mínimo conseguimos reticulados com maior densidade de empacotamento, com o qual obtemos melhores reticulados.

## Referências

- [1] L. Washington. *Introduction on cyclotomic fiels*. Springer-Verlag, New York, 1997.
- [2] T.P. Nóbrega N., J.O.D. Lopes and J.C. Interlando. *On computing discriminants of subfields  $\mathbb{Q}(\xi_{p^r})$* . Journal of Number Theory, No. 96, pp. 319-325, 2002.
- [3] J.O.D. Lopes. *The discriminant of subfields of  $\mathbb{Q}(\xi_{2^r})$* . Journal of Algebra and Its Applications, vol. 2, No. 4, pp. 463-469, Dezember 2003.
- [4] T.P. Nóbrega Neto, J.O.D. Lopes e J.C. Interlando, "The discriminant of the abelian number fields." To appear.