UNIVERSIDADE ESTADUAL DE CAMPINAS
FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO
DEPARTAMENTO DE TELEMÁTICA

RETICULADOS EM CORPOS ABELIANOS

Por

André Luíz Flores

Licenciado em Matemática - UNESP/São José do Rio Preto
Mestre em Matemática - IMECC/UNICAMP

Orientador: Prof. Dr. Trajano Pires da Nóbrega Neto - IBILCE/UNESP
Co-Orientador: Reginaldo Palazzo Júnior - FEEC/UNICAMP

Banca Examinadora:

Prof. Dr. Trajano Pires da Nóbrega Neto - (presidente)
Prof. Dr. Orlando Stanley Juriaans - IME/USP
Prof. Dr. Antonio Andrade e Silva - UFPB
Prof. Dr. Walter da Cunha Borelli - FEEC/UNICAMP
Prof. Dr. Ivanil Sebastião Bonatti - FEEC/UNICAMP

Tese apresentada à Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas, como requisito parcial para a obtenção do título de DOUTOR EM ENGENHARIA ELÉTRICA.

maio de 2000

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA - BAE - UNICAMP

F663r

Flores, André Luiz
Reticulados em corpos abelianos / André Luiz Flores.--Campinas, SP: [s.n.], 2000.

Orientadores: Trajano Pires da Nóbrega Neto e Reginaldo Palazzo Júnior.
Tese (doutorado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Teoria dos reticulados. 2. Teoria dos números. 3. Teoria da informação. 4. Modulação digital. 5. Teoria da codificação. I. Nobrega Neto, Trajano Pires da . II. Palazzo Júnior, Reginaldo. IV. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. V. Título.

Dedico com amor ao meu
filho André Henrique, que
nestes três anos de convivência
tanta felicidade me trouxe.

Agradecimentos

Em especial, ao orientador Prof. Dr. Trajano Nóbrega Neto, pelo constante estímulo e valiosas sugestões, baseadas no seu vasto conhecimento técnico. Também pela paciência e amizade, sempre presentes desde os tempos da graduação.

Ao Prof. Dr. Reginaldo Palazzo Jr., pela co-orientação, sugestões baseadas em sua visão generalista, atenção e amizade.

Aos professores da banca examinadora.

Ao Prof. Dr. José Carmelo Interlando, pela revisão dos artigos e sugestões.

À minha esposa Maria, pelo companheirismo e paciência.

Ao CNPq, pelo suporte financeiro.

À todos que de alguma forma contribuiram para a realização deste trabalho.

Resumo

Neste trabalho, apresentamos novos resultados ao descrever reticulados gerados a partir da representação geométrica de ideais de corpos de números abelianos. O principal parâmetro pesquisado é a densidade de centro dos reticulados considerados. Deste modo, estendemos a família de Craig, no sentido de que existe uma contribuição para cada dimensão. São apresentados reticulados eficientes para o canal Rayleigh com desvanecimento e ligações entre os reticulados estudados e códigos BCH são estabelecidas.

Abstract

In this work we present new results in describing algebraic lattices generated from geometric representation of ideals in abelian number fields. The main parameter in this research is the center density of the considered lattices. This way, we extend the Craig's family in the sense that there is a contribution to each dimension. Efficient lattices to the Rayleigh fading channel are presented and some links between the studied lattices and BCH codes are established.

Índice

1 - Apresentação 1
1.1 - Sistema de Comunicações Digitais 1
1.2 - Motivação e Descrição do Trabalho 5

2 - Corpos de Números 13
2.1 - Números Algébricos 13
2.2 - Decomposição de Ideais 25
2.3 - Reticulados e Densidades de Centro 33

3 - Corpos de Números Abelianos 41
3.1 - Reticulados em $\mathbb{Q}(\zeta_{p^r})$ 42
3.2 - Ideais em $\mathbb{Q}(\zeta_{p^r})$, $r \geq 2$ 47
3.3 - Subcorpos de $\mathbb{Q}(\zeta_p)$ 51
3.4 - Cúbicas Reais Contidas em $\mathbb{Q}(\zeta_p)$ 58
3.5 - Subcorpos de $\mathbb{Q}(\zeta_{pq})$ 65

4. - Os Canais Gaussiano e Rayleigh com Desvanecimento 81
4.1 - Terminologia 82
4.2 - O Canal Gaussiano 83
4.3 - O Canal Rayleigh com Desvanecimento 88
4.4 - Versões Rotacionadas de Λ_3 91
4.5 - Constelações Construídas a partir de Ideais 96

5 - Códigos n-ários via Reticulados Algébricos 103
5.1 - Partição de Reticulados Via Potências de Ideais 104
5.2 - Códigos BCH n-ários Via Reticulados Algébricos 108

6 - Conclusões e Propostas para Trabalhos Futuros 118
6.1 - Conclusões 118
6.2 - Sugestões para Pesquisas Futuras 121

Apêndice 124

Bibliografia 127

Índice de Símbolos

$A[X]$: anel dos polinômios sobre A
A^*: $A - \{0\}$
AB (A, B anéis): Adjunção do anel B ao anel A.
A/B (A, B anéis, corpos ou grupos): quociente de A por B.
$a \mid b$: a divide b
a^{-1}: inverso multiplicativo do elemento a
$B(1)$: Bola de raio 1 no $\mathbb{R}^n$
$card(X)$: cardinalidade do conjunto X
$\mathbb{C}$: corpo dos números complexos
$d_{\min}$: distância mínima do reticulado
d_{eucl}: distância euclidiana
d_{Lee}: distância de Lee
$det(M)$: determinante da matriz M
$D(x_1, ..., x_n)$: discriminante da n-upla $(x_1, ..., x_n)$
$\mathcal{D}(\mathfrak{p})$: grupo de decomposição do ideal $\mathfrak{p}$
$\mathfrak{D}_K$: Discriminante do corpo K
E: energia da constelação
E_b: energia por bit
e: índice de ramificação
$erfc$: função erro
f: grau residual
$f^{-1}(X)$: imagem inversa de X pela função f
$f'(X)$: derivada da função $f(X)$
$Gal(L, K)$: grupo de Galois de L sobre K
G_a: ganho assintótico
i: $\sqrt{-1}$
$irr(x, K)$: polinômio minimal de x sobre K
$I(z)$: parte imaginária do número complexo z
$Ker(f)$: núcleo do homomorfismo f
L: diversidade

M^t: transposta da matriz M
$min(X)$: mínimo do conjunto X
$N_{L|K}$: norma com relação a L e K
$N(\mathfrak{a})$: norma do ideal $\mathfrak{a}$
$\mathbb{N}$: conjunto dos números naturais
N_0: potência do ruído
$Ord_n(p)$: ordem de p módulo n
$\mathcal{O}_K$: anel dos inteiros do corpo K
P_e: probabilidade de erro
$\mathbb{Q}$: corpo dos números racionais
$R(z)$: parte real do número complexo z
$\mathbb{R}$: corpo dos números reais
r_2: metade do número de imersões complexas de um corpo de números em $\mathbb{C}$
SNR: relação sinal-ruído
$Tr_{L|K}$: traço com relação a L e K
$v(\Lambda)$: volume da região fundamental do reticulado Λ
V_Λ: região de Voronoi do reticulado Λ
$\overline{x}$: conjugado complexo de x.
$\mathbb{Z}$: anel dos números inteiros
$\mathbb{Z}_n$: anel dos resíduos módulo n

γ: ganho fundamental de codificação
$\delta(\Lambda)$: densidade de centro do reticulado Λ
Δ: densidade de empacotamento esférico
$\zeta(n)$: função zeta de Riemann
ζ_n: $e^{2\pi i/n}$
τ: número e vizinhos
η: eficiência espectral
θ: conjugação complexa
Λ: reticulado no $\mathbb{R}^n$
$\prod$: produto
ρ: raio de empacotamento
σ: homomorfismo de Minkowski
$\sum$: soma
$\phi(m)$: número de elementos de $(\mathbb{Z}/m\mathbb{Z})^*$ (função de Euler)
$\phi_n(X)$: polinômio minimal de ζ_n sobre $\mathbb{Q}$

$!$: fatorial

$\simeq$: isomorfo

$\in$: pertence

$\equiv$: côngruo

$\subseteq$: está contido

$| x |$: valor absoluto de x

$|| x ||$: norma do vetor x no espaço euclidiano n-dimensional

$| M |$: (M matriz) determinante de M

$[x]$: maior inteiro menor ou igual a x.

$[L : K]$ (corpos): grau de L sobre K

$(G : H)$ (grupos): índice de H em G.

(m, n): maior divisor comum de m e n

$\binom{m}{n}$: número de combinações de n elementos tomados em um conjunto com m elementos

Capítulo 1

Apresentação

1.1 Sistema de Comunicações Digitais

Nos últimos anos, tem havido uma crescente demanda por transmissão digital de dados. Esta demanda vem sendo acelerada pela necessidade de transmissão de um volume cada vez maior de informações e que seja ao mesmo tempo segura.

Descreveremos brevemente um modelo de um típico sistema de transmissão digital (representado por um diagrama de blocos, conforme figura) para depois compreendermos o que se pretende analisar neste trabalho.

Em um sistema de comunicações digitais, o objetivo é transmitir dados de uma fonte até um usuário. Para isso, as seguintes etapas estão envolvidas:

Fonte: A fonte de informação pode ser uma pessoa ou uma máquina (por exemplo um computador), cuja saída pode ser um sinal analógico ou uma sequência de símbolos de um alfabeto discreto. O meio usado para esta transmissão é chamado de canal, que pode ser uma linha telefônica, um cabo coaxial, fibra óptica, a atmosfera (no caso de ondas de rádio), etc.

No caso de fonte contínua, faz-se a conversão para símbolos discretos. Assim, pode-se

considerar que os dados gerados pela fonte são símbolos de um alfabeto A.

Codificador de Fonte: Como cada símbolo gerado pela fonte tem sua probabilidade de ocorrência, estes dados são processados pelo codificador de fonte, com o objetivo de eliminar redundância, ou seja, tornar os símbolos equiprováveis e desta forma compactar a informação.

Codificador de Canal: As sequências geradas pelo codificador de fonte são então processadas pelo codificador de canal, que introduz redundância gerando sequências de símbolos de A que são chamadas de palavras código.

Os códigos podem ser de blocos ou códigos convolucionais. O codificador para o código de blocos divide a sequência de informação em blocos de k símbolos $u = (u_1, ..., u_k) \in A^k$, chamado de bloco de mensagem. O codificador transforma cada um desses blocos em uma n-upla $v = (v_1, ..., v_n) \in A^n$. A palavra código v depende apenas de u; assim o codificador de blocos é desprovido de memória.

Analogamente, o codificador convolucional associa a cada bloco de mensagem u de comprimento k uma palavra código v de comprimento n, que depende não somente de u, mas de m blocos de mensagem anteriores. Neste caso o codificador é dito ter memória de ordem m. Em ambos os tipos de código, o número $R = \frac{k}{n}$ é a chamada taxa do código.

Modulador: Símbolos discretos não são adequados para a transmisão em um canal físico. Para a transmissão, o modulador então associa a cada palavra código x um símbolo analógico, que é então enviado pelo canal.

Dois importantes parâmetros são a velocidade de transmissão de informação e a largura de faixa do canal. Supondo que cada símbolo codificado seja transmitida a cada T segundos, então a taxa de transmissão de símbolo é $\frac{1}{T}$ símbolos por segundo. Em um sistema codificado, se a taxa do código é $\frac{k}{n}$, a taxa de transmissão de informação será de $\frac{R}{T}$ símbolos por segundo, ou seja, é reduzida por um fator R se comparada a um sistema não codificado. Portanto, para manter a taxa de transmissão, é necessário uma expansão

da largura da faixa por um fator $\frac{1}{R}$. Assim, a velocidade de transmissão de informação e a largura de faixa do canal são parâmetros intrinsicamente relacionados.

Canal: O canal em geral está sujeito a vários tipos de ruídos, imperfeições e interferências que geram distorções, de forma que o sinal recebido nem sempre coincide com o enviado.

Um canal muito frequente em sistemas de comunicação digital é o canal com ruído gaussiano branco aditivo (AWGN). Se o sinal transmitido é s, o sinal recebido é

$$r = s + \mu \ ,$$

onde $\mu = (\mu_1, \ldots \mu_n)$ é um processo aleatório gaussiano com média 0 e densidade espectral de potência N_0.

Um outro ruído bastante presente em sistemas de comunicação digital é o ruído multiplicativo (canal Rayleigh com desvanecimento). Quando um sinal s é transmitido através de um canal com tal ruído, o sinal recebido é

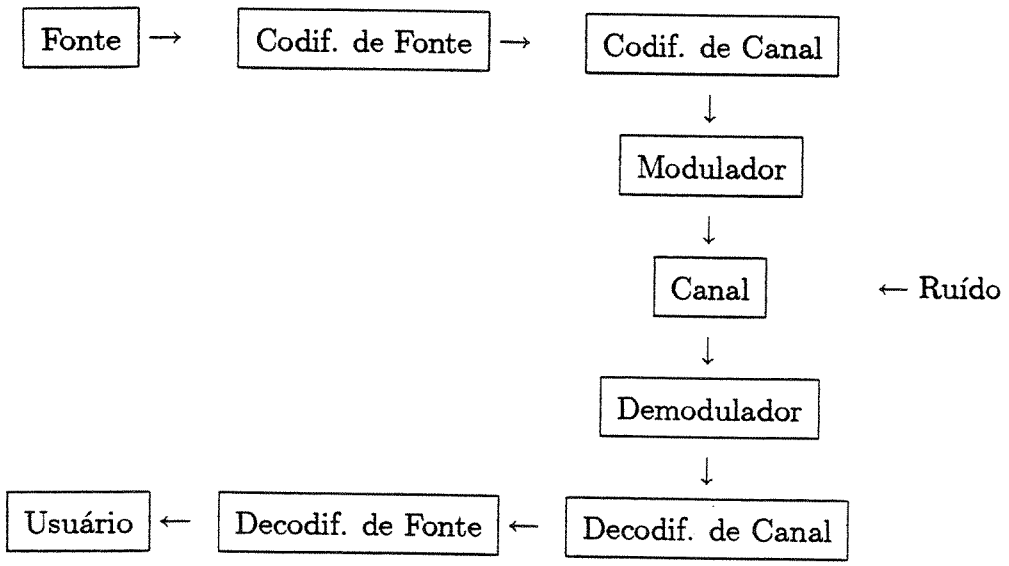
$$r = \alpha * s + \mu,$$

onde $\mu = (\mu_1, ..., \mu_n)$ é um ruído gaussiano e $\alpha = (\alpha_1, ..., \alpha_n)$ são os coeficientes de desvanecimento com segundo momento unitário e $*$ representa o produto componente a componente.

Demodulador: O demodulador recebe o sinal r e faz então a melhor estimativa, fornecendo uma sequência de símbolos de A.

Decodificador de canal: Devido ao ruído, é possível que a sequência de símbolos na saída do demodulador não seja uma palavra código. Então o decodificador de canal associará uma palavra código, que é a melhor estimativa.

Decodificador de fonte: Finalmente, o decodificador de fonte associará a esta palavra código a suposta sequência original de símbolos enviada. Quando a fonte é contínua, neste momento o sinal discreto é convertido em sinal contínuo. Em um sistema eficiente, a estimativa será uma reprodução fiel do sinal gerado pela fonte.



Neste trabalho enfocaremos, principalmente, o bloco do modulador.

Recentemente, constelações multidimensionais têm sido alvo de intensas pesquisas em sistemas de comunicação. Em particular, os pontos de uma constelação n-dimensional S, contendo $M = 2^m$ sinais, são escolhidos nas primeiras camadas de um reticulado Λ, de forma que o conjunto de sinais se aproxima da forma esférica. Tais constelações têm a característica de fornecer simultaneamente bom desempenho e baixa complexidade de implementação.

A eficiência espectral é medida em número de bits por duas dimensões,

$$\eta = \frac{2m}{n}.$$

Um dos aspectos tratados neste trabalho é a busca de esquemas de modulação eficientes para os canais gaussiano e Rayleigh com desvanecimento.

1.2 Motivação e Descrição do Trabalho

A seguir, citaremos alguns aspectos históricos, que serviram de motivação para o presente trabalho. O objetivo é uma melhor compreensão do contexto geral e de alguns aspectos específicos relacionados com o assunto.

1.2.1 Relações entre empacotamento esférico e Teoria da Comunicação

A Teoria dos Códigos Corretores de Erros nasceu em 1948, com o famoso trabalho de Shannon ([26]), onde foi demonstrado o Teorema da Capacidade do Canal. Em linhas gerais, este resultado diz que para transmissão de dados abaixo de uma certa taxa C (símbolos por segundo), chamada de capacidade do canal, é possível obter probabilidade de erro tão pequena quanto se deseja, para isso necessitando, porém, de códigos corretores de erros eficientes.

A prova do Teorema da Capacidade do Canal implica que no caso de valores altos da relação sinal-ruído (SNR), um código de bloco ótimo para um canal com ruído gaussiano branco aditivo (AWGN), limitado em faixa consiste em um empacotamento denso de sinais dentro de uma esfera, no espaço euclidiano n-dimensional, para n suficientemente grande. Assim, se estabeleceu o vínculo entre empacotamento esférico e Teoria da Informação.

Depois disto, Leech mostrou como usar códigos corretores de erros para construir empacotamentos esféricos densos no $\mathbb{R}^n$ e Conway e Sloane [27] provaram que reticulados satisfazendo a cota de Minkowski (dada pela Equação 1.1) são equivalentes a códigos atingindo a capacidade do canal.

O problema clássico do empacotamento esférico consiste em encontrar um arranjo de esferas com mesmo raio no espaço Euclidiano n-dimensional de forma que a fração do

espaço coberto por essas esferas seja a maior possível. Isto pode ser visto como a versão euclidiana do 18° Problema de Hilbert, proposto em 1900.

Usando diferentes técnicas, vários trabalhos têm contribuído com soluções parciais. Embora relevantes, estas contribuições estão longe de resolver o problema em sua forma mais geral.

Dentre os métodos de geração de reticulados, o homomorfismo de Minkowski apresenta características interessantes. Usando Teoria Algébrica dos Números, Craig reproduziu o reticulado de Leech Λ_{24} através da representação geométrica de um ideal no anel de inteiros de $\mathbb{Q}(\zeta_{39})$. Com o mesmo método, ainda obteve a família A_n^m em dimensões $n = p - 1$, através de $\mathbb{Q}(\zeta_p)$, onde p é um número primo.

Ao estudar a densidade de empacotamento, um dos principais problemas é a obtenção de reticulados com alta densidade e que sejam ao mesmo tempo construtíveis. Uma ilustração desta dificuldade pode ser vista no trabalho de Shafarevich e Golod (cf. [25]), onde os autores descrevem uma família de reticulados com boa densidade, porém de difícil manipulação.

Para cada n, Minkowski provou a existência de reticulados no espaço euclidiano n-dimensional com densidade de empacotamento esférico Δ satisfazendo

$$\Delta \geq \frac{\zeta(n)}{2^{n-1}} ,$$

onde ζ é a função zeta de Riemann. Como consequência, obtem-se

$$\frac{1}{n} \log_2 \Delta > -1. \tag{1.1}$$

Contudo, esta prova é não construtiva. Famílias construtivas com boa densidade são conhecidas apenas em dimensões particulares. Por exemplo, os reticulados BW_n (cf. [27], pp. 234) são descritos em dimensão $n = 2^m$, e assintoticamente,

$$\frac{1}{n}\log_2 \Delta \simeq -\frac{1}{4}\log_2 n.$$

Reticulados construídos a partir de códigos BCH em dimensões $n = 2^m$ e os reticulados de Craig, A_n^m em dimensões $n = p-1$, p primo, têm desempenho assintótico satisfazendo

$$\frac{1}{n}\log_2 \Delta \simeq -\frac{1}{2}\log_2 \log_2 n.$$

1.2.2 O canal Rayleigh com desvanecimento

Conforme comentado, para o canal gaussiano, podemos obter constelações eficientes via reticulados com alta densidade de empacotamento esférico. Assim, constelações com baixa energia e com boas propriedades de simetria são obtidas.

Analogamente, para o canal Rayleigh com desvanecimento, fixados a eficiência espectral e a probabilidade de erro, o objetivo é construir constelações que minimizam a energia.

Uma nova técnica para obter conjuntos de sinais casados com o canal Rayleigh com desvanecimento foi proposta por Giraud e Belfiore ([15]). A idéia é usar famílias particulares de corpos de números, por exemplo corpos totalmente reais (cf. definição 2.3.2) para obter constelações (reticulados) úteis para estes canais.

As constelações foram construídas em dimensões $n \leq 8$ através de corpos de números totalmente reais com discriminante mínimo. A principal propriedade destas constelações é a diversidade máxima, ou seja, o maior número possível de coordenadas não nulas.

Contudo, o desempenho das constelações obtidas, quando utilizadas no canal gaussiano, é negativo, ou seja, apresentam densidade de empacotamento esférico inferior à de $\mathbb{Z}^n$. Reciprocamente, as constelações boas (conhecidas) para o canal gaussiano usual-

mente apresentam baixa diversidade, e portanto têm baixo desempenho no canal Rayleigh com desvanecimento.

Assintoticamente, a probabilidade de erro dois a dois para o canal Rayleigh é dominada por $\left(\frac{1}{SNR}\right)^L$, onde L é a diversidade e SNR é a relação sinal-ruído. (cf. [15]). Portanto, um meio para obter constelações eficientes para ambos os canais é buscar reticulados densos com diversidade máxima.

Uma técnica eficiente para aumentar a diversidade é rotacionar constelações QAM. Uma das vantagens é que se conservam as propriedades para o canal gaussiano. Em dimensão 2, não é difícil obter o ângulo de rotação ótimo que maximiza a chamada distância produto. Para outras dimensões, contudo, este método se torna impraticável.

Posteriormente, Boutros et al. ([4]) construíram "versões rotacionadas" dos reticulados conhecidos Λ_4, K_{12}, e Λ_{16} através de $\mathbb{Q}(\zeta_8)$, $\mathbb{Q}(\zeta_{21})$, e $\mathbb{Q}(\zeta_{40})$, respectivamente, obtendo constelações eficientes para ambos os canais. Um interesse prático é que tais constelações podem ser usadas na transmissão de dados entre um móvel e uma base ou entre um móvel e um satélite, através do mesmo sistema de modulação/demodulação, entre outras possíveis aplicações.

Também tais constelações podem ser usadas no canal riceano, que está entre o gaussiano e o Rayleigh com desvanecimento.

1.2.3 Descrição do Trabalho

A Teoria de Reticulados Algébricos tem se mostrado extremamente útil para aplicações em Teoria da Informação.

Classicamente, o problema do empacotamento esférico para o canal gaussiano e ultimamente, constelações construídas a partir do anel de inteiros de corpos de números abelianos totalmente reais ([15], [4] e [3]) nos motivaram à realização deste trabalho.

Nesta linha, os resultados existentes na literatura se restringem a casos particulares de corpos ciclotômicos, com técnicas de manipulação apropriadas.

Um dos objetivos centrais deste trabalho é estudar a representação geométrica de ideais do anel de inteiros algébricos de corpos de números abelianos.

O Teorema de Kronecker-Weber (cf. [29]) diz que todo corpo de números abeliano está contido em um corpo ciclotômico $\mathbb{Q}(\zeta_n)$, para algum n. Assim, estudar corpos abelianos equivale a estudar subcorpos de corpos ciclotômicos, que no caso geral é extremamente abrangente.

Nesta linha, direcionamos nosso trabalho sobretudo ao estudo de subcorpos de $\mathbb{Q}(\zeta_{p^r})$ e $\mathbb{Q}(\zeta_{pq})$, p e q primos, dando assim um passo significativo em direção ao caso geral.

Quando se trata do canal gaussiano, o principal parâmetro é a densidade de centro, que para um ideal não nulo $\mathfrak{a}$ pode ser calculada por

$$\delta = \frac{2^{r_2}.\rho^n}{|\,\mathfrak{D}_K\,|^{1/2}\,N(\mathfrak{a})}, \tag{1.2}$$

onde ρ é o chamado raio de empacotamento do reticulado, $\mathfrak{D}_K$ é o discriminante do corpo K, $N(\mathfrak{a})$ é a norma do ideal $\mathfrak{a}$ e r_2 é a metade do número de imersões complexas de K em $\mathbb{C}$. Assim, calcular a densidade de empacotamento da representação geométrica de ideais de corpos abelianos envolve:

- O cálculo da norma do ideal $\mathfrak{a}$;

- O cálculo do discriminante $\mathfrak{D}_K$;

- A minimização dos comprimentos dos vetores da representação geométrica de $\mathfrak{a}$.

A norma do ideal em questão é relativamente simples de ser obtida e está relacionada com a teoria de decomposição de ideais em uma extensão.

O discriminante é de cálculo mais complexo. No nosso caso, em que tratamos de corpos abelianos, enfocamos o cálculo do discriminantes de subcorpos de corpos ciclotômicos.

Dentre estes parâmetros, calcular a menor distância do reticulado é sem dúvida o trabalho mais árduo, já que equivale a minimizar a forma quadrática $Tr_{K/\mathbb{Q}}(x\overline{x})$ (cf. Prop. 2.3.8), para $x \in \mathfrak{a}$, que é uma forma quadrática positiva definida em n variáveis com entradas inteiras e obedecendo a certas restrições (que caracterizam o ideal).

Para o canal Rayleigh com desvanecimento, o principal parâmetro é a diversidade, que pode ser maximizada com os corpos de números totalmente reais. Aqui, serão enfocados subcorpos reais de corpos ciclotômicos, portanto abelianos.

1.3 Organização do trabalho

Este trabalho foi organizado em 5 capítulos, com subdivisões em seções e subseções.

Quando um resultado enunciado está presente na literatura, é colocada a fonte do mesmo entre parêntese e com excessão no capítulo 2, quando a fonte não é citada, o resultado é original.

Cada capítulo traz o seguinte conteúdo:

Capítulo 2 - Corpos de Números - Este capítulo é dedicado à apresentação de resultados básicos da Teoria Algébrica dos Números e reticulados. Os resultados aqui reunidos, bem como suas demonstrações, podem ser obtidos nas referências [10], [17] e [24].

Procuramos introduzir exemplos, para uma melhor compreensão dos resultados enunciados.

Os assuntos tratados foram, nesta ordem, elementos integrais sobre um anel, elementos algébricos sobre um corpo, normas e traços de elementos, norma de um ideal, corpos ciclotômicos e discriminante. Também são expostos resultados sobre fatoração de ideais em domínios de Dedekind e decomposição em uma extensão abeliana.

Apresentamos ainda as definições de reticulado, empacotamento esférico, densidade de empacotamento esférico e densidade de centro. Em seguida é apresentado o método de Minkowski, para obtenção de reticulados via representação geométrica de ideais em anéis de inteiros algébricos. Veremos que a representação geométrica de um ideal é um reticulado e explicitamos a fórmula geral para o cálculo da densidade de centro destes reticulados.

Capítulo 3 - Corpos de Números Abelianos - Iniciamos este capítulo com o estudo de subcorpos de $\mathbb{Q}(\zeta_{p^r})$, p primo, com obtenção da forma quadrática associada. Estudamos a representação geométrica das potências do ideal primo $\mathfrak{p}$ de $\mathbb{Z}[\zeta_{p^r}]$ acima de p.

A partir de subcorpos de $\mathbb{Q}(\zeta_p)$, geramos um reticulado para cada dimensão n. A família $\mathcal{A}_n$ então construída tem a melhor densidade conhecida em infinitas dimensões, inclusive em dimensões relativamente baixas. A densidade de empacotamento Δ para tais reticulados satisfaz

$$\frac{1}{n}\log_2(\Delta) \geq -\frac{1}{2}\log_2\log_2 n.$$

Com esta família, introduzimos constelações que têm máxima diversidade e boa densidade de empacotamento, que fazem estes reticulados úteis para uso nos canais gaussiano e Rayleigh com desvanecimento.

Uma das diferenças entre a família aqui apresentada e as demais da literatura, é que aqui as contelações são obtidas para qualquer dimensão n.

Em seguida, fazemos um estudo de cúbicas reais contidas em $\mathbb{Q}(\zeta_p)$, p primo.

Finalmente, concluímos este capítulo estudando subcorpos de $\mathbb{Q}(\zeta_{pq})$, iniciando com a obtenção da forma quadrática associada e decomposição em $\mathbb{Q}(\zeta_{pq})$. Em seguida, apresentamos um novo método que simplifica a obtenção do mínimo da forma quadrática associada. Fazemos uma nova prova para a construção dos reticulados K_{12} e Λ_{24} e obtemos diversas versões rotacionadas de um reticulado com a máxima densidade conhecida em dimensão 8.

Capítulo 4 - Os Canais Gaussiano e Rayleigh com Desvanecimento - Iniciamos com a obtenção de um algoritmo para o cálculo do número de vizinhos. Neste capítulo, são introduzidas novas técnicas de construção de constelações de sinais, a partir de ideais do anel de inteiros de um corpo de números. Desenvolvemos um método que de certa forma "transforma" uma constelação eficiente para o canal Rayleigh com desvanecimento em eficiente também para o canal gaussiano. Estas constelações são obtidas a partir de ideais do anel de inteiros de corpos de números totalmente reais com discriminante mínimo. Com relação às constelações de [15] construídas a partir do anel de inteiros de Corpos de Números, as constelações aqui apresentadas apresentam desempenho semelhante para o canal Rayleigh e considerável ganho no canal gaussiano.

Capítulo 5 - Códigos n-ários Via Reticulados Algébricos - Fazemos neste capítulo ligações entre a teoria aqui desenvolvida e outras áreas de Teoria da Comunicação. Em particular, construímos códigos BCH a partir de ideais do anel de inteiros de corpos de números. Mostramos que existe uma estreita relação entre a métrica de Lee do código correspondente ao ideal e as distâncias euclidiana e produto no reticulado correspondente.

Alguns resultados parciais são apresentados, como forma de motivação para pesquisa futura.

Capítulo 6 - Conclusões e Propostas para Trabalhos Futuros - É apresentada uma breve conclusão, contendo comentários sobre as principais contribuições do presente trabalho. São também colocadas sugestões e propostas de trabalhos futuros nas diversas linhas que derivam dos resultados aqui apresentados.

Apêndice - É apresentado um algoritmo implementado no GAP (Groups, Algorithms and Programming), que calcula o discriminante de subcorpos de $\mathbb{Q}(\zeta_{p^a q^b})$, p e q primos.

Capítulo 2

Corpos de Números

Neste capítulo, apresentamos uma coletânea de resultados básicos da Teoria Algébrica dos Números e reticulados algébricos. O objetivo é fornecer a base teórica para o desenvolvimento dos demais capítulos, além de fixar a notação. Admitimos que o leitor possua conhecimentos elementares de estruturas algébricas e álgebra linear, a nível de [17] e [16].

Neste capítulo, omitimos as demonstrações, e quando não é citada a fonte, os resultados podem ser encontrados nas referências acima mencionadas.

Optamos por apresentar os resultados na medida da necessidade deste trabalho. Assim, em diversas situações estes valem para casos mais gerais.

Dentre os resultados centrais do capítulo, destacamos o Teorema 2.2.1, que mostra a unicidade da fatoração de um ideal em ideais primos, o Teorema 2.3.7, que traz uma expressão para o volume do reticulado gerado por um ideal e a Proposição 2.3.8, para o cálculo de distâncias no reticulado gerado por um ideal.

2.1 Números Algébricos

Nesta seção, introduzimos elementos integrais sobre um anel, elementos algébricos sobre um corpo, extensões de corpos e suas propriedades. Tratamos ainda de norma e traço de um elemento, corpos ciclotômicos, discriminante de um corpo e norma de ideais.

2.1.1 Elementos integrais sobre um anel

Dados os anéis $A \subset R$, um elemento $x \in R$ é dito integral sobre A se este é raiz de um polinômio mônico com coeficientes em A.

Por exemplo, o elemento $x = \sqrt{2} \in \mathbb{R}$ é integral sobre $\mathbb{Z}$, pois x é raiz de $X^2 - 2$.

Mostra-se que se $A \subset R$ são anéis, então o conjunto dos elementos de R integrais sobre A é um subanel de R que contém A, chamado de fecho integral de A em R (cf. [24], pp. 35).

De modo geral, R é dito integral sobre A se todo elemento de R for integral sobre A.

Sejam R um anel e K um subcorpo de R. Um elemento $x \in R$ é dito algébrico sobre K se este é raiz de um polinômio mônico com coeficientes em K. Um elemento $x \in R$ não algébrico sobre K é dito transcendente sobre K. Se todo elemento de R for algébrico sobre K, dizemos que R é algébrico sobre K. No caso em que R é um corpo e R é algébrico sobre K, diz-se que R é uma extensão algébrica de K.

Uma caracterização dos elementos algébricos sobre um corpo K é:

$$x \text{ é algébrico sobre } K \iff [K[x] : K] \text{ é finito.}$$

Dado um elemento $x \in R$, consideremos o homomorfismo de anéis $\sigma_x : K[X] \mapsto R$ definido por $\sigma_x(a) = a$, para todo $a \in K$, e $\sigma_x(X) = x$.

A definição de elemento algébrico sobre K pode ser reformulada em termos do homomorfismo σ_x da seguinte forma:

$$x \text{ é algébrico sobre } K \iff Ker(\sigma_x) \neq \{0\}.$$

De modo geral, vale

$$K[x] \simeq K[X]/Ker(\sigma_x).$$

Consequentemente, se x for transcendente sobre K, então $K[x] \simeq K[X]$.

Sendo $K[X]$ um domínio principal, o ideal $Ker(\sigma_x)$ é gerado por um polinômio $f(X) \in K[X]$, não constante no caso em que x é algébrico sobre K. Podemos supor $f(X)$ mônico, já que K é um corpo. Dessa forma, $f(X)$ é único, sendo chamado de polinômio minimal de x sobre K. Será denotado por $irr(x, K)$ e mostra-se que é um polinômio irredutível em $K[X]$.

No caso em que x é algébrico sobre K, então $[K(x) : K]$ é igual ao grau de $irr(x, K)$.

Sejam K um corpo, L uma extensão finita de K, F uma extensão finita de L com bases $\{x_i\}$, $i = 1, ..., n$ e $\{y_j\}$, $j = 1, ..., m$, respectivamente. Mostra-se que o conjunto $\{x_i y_j \; ; \; i = 1, ..., n \; ; \; j = 1, ..., m\}$ é base de F sobre K e portanto $[F : K] = [F : L].[L : K]$.

Sejam K um corpo e L, L' extensões de K. Dá-se o nome de K-monomorfismo de L em L' a todo monomorfismo $\sigma : L \mapsto L'$ satisfazendo $\sigma(x) = x$, para todo $x \in K$.

Sejam K um corpo e $f(X) \in K[X]$ um polinômio não constante. Suponhamos que exista um corpo L satisfazendo as seguintes propriedades:

(i) $K \subseteq L$;
(ii) $f(X)$ é fatorado em polinômios de grau 1 em $L[X]$;
(iii) Se L' é um corpo que satisfaz (i) e (ii), então $L \subseteq L'$.

Nestas condições L é dito ser o corpo de raizes de f sobre K. Em outras palavras, o corpo de raizes de um polinômio $f(X) \in K[X]$ é o menor corpo contendo K e todas as raizes de $f(X)$.

Consideremos as extensões L e L' de um corpo K. Dizemos que dois elementos x, x' pertencentes a L e L', respectivamente, são conjugados se existir um K-monomorfismo

$\sigma : L \to L'$ tal que $\sigma(x) = x'$.

Definição 2.1.1 *Um corpo de números é uma extensão finita do corpo $\mathbb{Q}$ dos números racionais. Se a dimensão de um corpo de números K como $\mathbb{Q}$-espaço vetorial é n, diz-se que K é um corpo de números de grau n.*

O anel formado pelos elementos de um corpo de números K que são integrais sobre $\mathbb{Z}$ são chamados de inteiros de K e serão denotados por $\mathcal{O}_K$.

Proposição 2.1.2 *([24], pp. 56, Prop.1) Sejam K um corpo de números de grau n. Então o anel de inteiros $\mathcal{O}_K$ é um $\mathbb{Z}$-módulo livre de posto n.*

O resultado a seguir é de fundamental importância para a construção algébrica de reticulados.

Teorema 2.1.3 *([24], pp. 33, Theo.1) Sejam $K \subseteq L$ corpos de números, com $[L : K] = n$. Então existem n K-monomorfismos distintos de L em $\mathbb{C}$.*

2.1.2 Normas e traços

Sejam $K \subseteq L$ corpos de números, com $n = [L : K]$ e $\sigma_1, ..., \sigma_n$ os K-monomorfismos de L em $\mathbb{C}$. Dado um elemento $x \in L$, define-se o traço de x relativamente a L e K como sendo

$$Tr_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x).$$

Analogamente, define-se a norma de x relativamente a L e K como

$$N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x).$$

Definimos o polinômio característico de x relativamente a L e K como sendo

$$F_x(X) = \prod_{i=1}^{n}(X - \sigma_i(x)).$$

Mostra-se que

$$F_x(X) = irr(x, K)^{[L:K(x)]}.$$

Note que na expressão

$$F_x(X) = X^n - Tr_{L/K}(x)X^{n-1} + \cdots + (-1)^n N_{L/K}(x) \in K[X],$$

o traço e a norma são, a menos de sinal, coeficientes de $F_x(X)$; logo são elementos de K.

Exemplo 2.1.4 *Sejam* $L = \mathbb{Q}(\sqrt{2})$, $K = \mathbb{Q}$, $\beta = \{1, \sqrt{2}\}$ *uma* $\mathbb{Q}$*-base para* L *e* $x = a + b\sqrt{2} \in L$. *O grupo dos* $\mathbb{Q}$*-automorfismos de* L *é* $\{\sigma_1, \sigma_2\}$, *onde*

$$\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$$

e

$$\sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}.$$

Logo,

$$Tr_{L|K}(x) = 2a$$

e

$$N_{L|K}(x) = a^2 - 2b^2.$$

Sejam $K \subset L$ corpos, $[L : K] = n$; $x, y \in L$ e $a \in K$. Valem as seguintes propriedades:

$$Tr_{L/K}(x + y) = Tr_{L/K}(x) + Tr_{L/K}(y);$$
$$Tr_{L/K}(ax) = aTr_{L/K}(x);$$
$$Tr_{L/K}(a) = na;$$
$$N_{L/K}(xy) = N_{L/K}(x).N_{L/K}(y)\ ;$$
$$N_{L/K}(a) = a^n.$$

No caso $K \subseteq L \subseteq M$, dado $x \in M$, valem

$$Tr_{M/K}(x) = Tr_{L/K}(Tr_{M/L}(x))$$

e

$$N_{M/K}(x) = N_{L/K}(N_{M/L}(x)).$$

Em particular, se $x \in L$, então

$$Tr_{M/K}(x) = [M : L].Tr_{L/K}(x)$$

e

$$N_{M/K}(x) = N_{L/K}(x)^{[M:L]}.$$

Quando não houver ambiguidade, as notações denotaremos $N_{L|K}$ e $Tr_{L|K}$ por N e T, respectivamente.

2.1.3 Corpos ciclotômicos

O corpo $K = \mathbb{Q}(\zeta_n)$, onde $\zeta_n = e^{2\pi i/n}$ é chamado de n-ésimo corpo ciclotômico. Sabe-se que $\mathbb{Q}(\zeta_n)$ é um espaço vetorial sobre $\mathbb{Q}$ de dimensão $\phi(n)$, a função de Euler, que representa o número de elementos do conjunto $\{t \in \{1, ..., n\} \ ; \ (t, n) = 1\}$. Mostra-se que se p é primo, então $\phi(p^r) = (p-1)p^{r-1}$, e se $(a, b) = 1$, então $\phi(ab) = \phi(a)\phi(b)$, o que caracteriza completamente esta função.

Os resultados a seguir podem ser encontrados em [29] e estão aqui expostos para melhor compreensão de resultados do próximo capítulo.

O conjunto dos elementos ζ_n^j, $j = 0, ..., \phi(n) - 1$ forma uma base de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$.

Os elementos ζ_n^j tais que $1 \leq j \leq n$ e $(j, n) = 1$ são chamadas de raizes primitivas n-ésimas da unidade, e vale $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n^j)$, $j = 1, ..., n$ e $(j, n) = 1$.

Exemplo 2.1.5 *Definamos* $\sigma_i : \mathbb{Q}(\zeta_n) \to \mathbb{C}$ *por* $\sigma_i(\zeta_n) = \zeta_n^i$. *Então o grupo dos* $\mathbb{Q}$-*automorfismos de* $\mathbb{Q}(\zeta_n)$ *será*

$$G = \{\sigma_i; (i,n) = 1,\ i = 1, ..., n\}.$$

Assim, os conjugados de ζ_n são exatamente as raizes primitivas n-ésimas da unidade.

O polinômio minimal de ζ_n sobre $\mathbb{Q}$ será denotado por $\phi_n(X)$. Em particular, para p primo e $r \geq 1$, temos

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

De modo geral, vale

$$X^n - 1 = \prod_{d|n} \phi_d(X).$$

Veremos alguns resultados no caso particular $\mathbb{Q}(\zeta_p)$, p primo. Pelo que vimos acima, $\phi_p(X) = X^{p-1} + \cdots + X + 1$. A irredutibilidade de $\phi_p(X)$ implica em:

$$Tr(\zeta_p) = -1 \text{ e } Tr(1) = p - 1.$$

Logo $Tr(\zeta_p^j) = -1$, para $j = 1, ..., p-1$ e como consequência

$$Tr(1 - \zeta_p) = Tr(1 - \zeta_p^2) = \cdots = Tr(1 - \zeta_p^{p-1}) = p$$

Observe que os conjugados de $1 - \zeta_p$ são os elementos $1 - \zeta_p^j$, $j = 1, ..., p-1$. Da identidade

$$X^{p-1} + \cdots + X + 1 = \prod_{i=1}^{p-1} (X - \zeta_p^i),$$

substituindo X por 1 obtém-se

$$p = \prod_{i=1}^{p-1} (1 - \zeta_p^i) = N(1 - \zeta_p).$$

Mostraremos que

$$(1-\zeta_p)\mathbb{Z}[\zeta_p] \cap \mathbb{Z} = p\mathbb{Z}.$$

Sabemos que $p \in (1-\zeta_p)\mathbb{Z}[\zeta_p]$, o que implica

$$(1-\zeta_p)\mathbb{Z}[\zeta_p] \cap \mathbb{Z} \supset p\mathbb{Z}\ .$$

Suponhamos, por absurdo, que a igualdade de conjuntos acima seja falsa. Sendo $p\mathbb{Z}$ um ideal maximal de $\mathbb{Z}$, a relação $(1-\zeta_p)\mathbb{Z}[\zeta_p] \cap \mathbb{Z} \neq p\mathbb{Z}$ implica $(1-\zeta_p)\mathbb{Z}[\zeta_p] \cap \mathbb{Z} = \mathbb{Z}$, ou seja, $1-\zeta_p$ é uma unidade em $\mathbb{Z}[\zeta_p]$. Assim os conjugados $1-\zeta_p^j$ de $1-\zeta_p$ também são unidades; logo p é unidade em $\mathbb{Z}[\zeta_p] \cap \mathbb{Z}$, o que é evidentemente falso e portanto vale a igualdade.

Cada conjugado $y_j(1-\zeta_p^j)$ de $y(1-\zeta_p)$ é múltiplo de $1-\zeta_p^j$ em $\mathbb{Z}[\zeta_p]$. Como

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

segue que $y_j(1-\zeta_p^j)$ é também múltiplo de $1-\zeta_p$. Sendo o traço a soma dos conjugados, temos

$$Tr(y(1-\zeta_p)) \in (1-\zeta_p)\mathbb{Z}[\zeta_p],$$

e pelo resultado anterior,

$$Tr(y(1-\zeta_p)) \in (1-\zeta_p)\mathbb{Z}[\zeta_p] \cap \mathbb{Z} = p\mathbb{Z}.$$

O resultado central desta seção é o seguinte

Teorema 2.1.6 *([29], pp. 35) O anel de inteiros de* $\mathbb{Q}(\zeta_n)$ *é* $\mathbb{Z}[\zeta_n]$.

2.1.4 Discriminante

O discriminante de um corpo de números desempenha um papel fundamental na teoria dos reticulados algébricos, pois como veremos na seção 2.3, este se relaciona com o cálculo da densidade de centro de reticulados gerados a partir de ideais.

Definição 2.1.7 *Seja K um corpo de números de grau n. Dá-se o nome de discriminante da n-upla $(x_1, ..., x_n) \in K^n$ ao elemento definido por*

$$D(x_1, ..., x_n) = det(Tr_{K/\mathbb{Q}}(x_i x_j)).$$

Prova-se que $D(x_1, ..., x_n) \in \mathbb{Q}$.

Lema 2.1.8 *([24], pp.38, Prop.1) Sejam $(x_1, ..., x_n)$, $(y_1, ..., y_n) \in K^n$ tais que $y_i = \sum_{j=1}^{n} a_{ij} x_j$, com $a_{ij} \in \mathbb{Q}$. Então*

$$D(y_1, ..., y_n) = (det(a_{ij}))^2 . D(x_1, ..., x_n).$$

Exemplo 2.1.9 *Dado o par $\{1, \sqrt{3}\}$, então*

$$D(1, \sqrt{3}) = \left| \begin{bmatrix} Tr(1) & Tr(\sqrt{3}) \\ Tr(\sqrt{3}) & Tr(3) \end{bmatrix} \right| = \left| \begin{bmatrix} 2 & 0 \\ 0 & 6 \end{bmatrix} \right| = 12.$$

Por outro lado,

$$\begin{bmatrix} 2+\sqrt{3} & 1+\sqrt{3} \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ \sqrt{3} \end{bmatrix},$$

ou seja,

$$D(2+\sqrt{3}, 1+\sqrt{3}) = 12.$$

Definição 2.1.10 *Sejam K um corpo de números de grau n e $\beta = \{x_1, ..., x_n\}$ uma $\mathbb{Z}$-base para o $\mathbb{Z}$-módulo livre $\mathcal{O}_K$. Então β é chamada de base integral de K.*

Do Lema 2.1.7, concluímos que os discriminantes de duas bases integrais quaisquer de K são iguais. Assim, faz sentido a seguinte

Definição 2.1.11 *Dá-se o nome de discriminante de K, e será indicado por $\mathfrak{D}_K$, ao discriminante de qualquer base integral de $\mathcal{O}_K$.*

Proposição 2.1.12 *([24], pp.39, Prop.3) Seja K um corpo de números de grau n e $\sigma_1, ..., \sigma_n$ os n $\mathbb{Q}$-monomorfismos distintos K em $\mathbb{C}$. Se $\{x_1, ..., x_n\}$ é uma $\mathbb{Q}$-base para K, então*

$$D(x_1, ..., x_n) = det(\sigma_i(x_j))^2 \neq 0.$$

Apresentaremos agora uma fórmula para o discriminante de uma n-upla da forma $(1, x, ..., x^{n-1})$.

Proposição 2.1.13 *([24], pp.41) Sejam $K = \mathbb{Q}(x)$ um corpo de números de grau n e $f(X) \in \mathbb{Z}[X]$ o polinômio minimal de x sobre K. Denotando por $f'(X)$ a derivada formal do polinômio $f(X)$, temos*

$$D(1, x, ..., x^{n-1}) = (-1)^{n(n-1)/2}.N_{K/\mathbb{Q}}(f'(x)).$$

Exemplo 2.1.14 *Veremos como a expressão acima pode ser útil no cálculo de discriminantes. O polinômio minimal de ζ_{p^r} sobre $\mathbb{Q}$ é*

$$f(X) = (X^{p^r} - 1)/(X^{p^{r-1}} - 1).$$

Sabemos que $\{1, \zeta_{p^r}, ..., \zeta_{p^r}^{\phi(p^r)-1}\}$ é base integral de $K = \mathbb{Q}(\zeta_{p^r})$. Pela Proposição 2.1.13, *temos que*

$$\mathfrak{D}_K = N_{K/\mathbb{Q}}(f'(\zeta_{p^r})) = N_{K/\mathbb{Q}}(p^r).N_{K/\mathbb{Q}}(\zeta_{p^r}^{p^r-1})/N_{K/\mathbb{Q}}(\zeta_{p^r}^{p^r-1} - 1). \qquad (2.1)$$

Fazendo o cálculo passo a passo, tem-se

$N_{K/\mathbb{Q}}(p^r) = p^{r(p-1)p^{r-1}}$;

$N_{K/\mathbb{Q}}(\zeta_{p^r}^{p^{r-1}}) = (N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p))^{p^{r-1}} = 1$;

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

Substituindo em 2.1, finalmente obtemos

$$\mathfrak{D}_K = \pm p^{p^{r-1}(p-1)r}.p^{-p^{r-1}} = \pm p^{p^{r-1}(pr-r-1)}.$$

Os resultados sobre discriminantes que nos serão úteis são listados a seguir:

Teorema 2.1.15 *([29], pp. 11, Theo. 2.6) Sejam K_1 e K_2 corpos de números linearmente disjuntos, ou seja, $[K_1K_2 : \mathbb{Q}] = [K_1 : \mathbb{Q}].[K_2 : \mathbb{Q}]$ e cujos discriminantes sejam inteiros relativamente primos. Então*

$$\mathfrak{D}_{K_1K_2} = \mathfrak{D}_{K_1}^{[K_2 : \mathbb{Q}]}.\mathfrak{D}_{K_2}^{[K_1 : \mathbb{Q}]}.$$

Teorema 2.1.16 *([29], pp. 12, Prop. 2.7) O discriminante do corpo $K = \mathbb{Q}(\zeta_n)$ vale*

$$\mathfrak{D}_K = (-1)^{\phi(n)/2}.\frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$

Teorema 2.1.17 *([12], pp. 45, Teor. 1) Sejam p um número primo e K um subcorpo de $\mathbb{Q}(\zeta_{p^r})$, com $[K : \mathbb{Q}] = up^j$ e p não divide u. Então*

$$| \mathfrak{D}(K) | = p^{u((j+2).p^j - \frac{p^{j+1}-1}{p-1})-1}.$$

Corolário 2.1.18 *No caso particular $K \subset \mathbb{Q}(\zeta_p)$, temos*

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

2.1.5 Norma de um ideal

Sejam K um corpo de números de grau n e x um elemento não nulo de $\mathcal{O}_K$. Em [24], pp. 62, tem-se

$$| N(x) | = card(\mathcal{O}_K/x\mathcal{O}_K).$$

Sejam $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_K$ e $x \in \mathfrak{a}$ um elemento não nulo. Então $x\mathcal{O}_K \subset \mathfrak{a}$, e portanto

$$card(\mathcal{O}_K/\mathfrak{a}) \leq card(\mathcal{O}_K/x\mathcal{O}_K)$$

e consequentemente $\mathcal{O}_K/\mathfrak{a}$ é finito. Assim, temos a seguinte

Definição 2.1.19 *Dá-se o nome de norma de* $\mathfrak{a}$, *e denotada por* $N(\mathfrak{a})$, *ao número* $card(\mathcal{O}_K/\mathfrak{a})$.

Proposição 2.1.20 *([24], pp.52, Prop.2) Sejam* K *corpo de números e* $\mathfrak{a}$, $\mathfrak{b}$ *ideais não nulos de* $\mathcal{O}_K$. *Então*

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}).$$

Exemplo 2.1.21 *Consideremos em* $\mathbb{Z}[i]$, *onde* $i = \sqrt{-1}$, *o ideal principal* $\mathfrak{a}$ *gerado por* $2 - i$. *Assim,*

$$\mathbb{Z}[i]/\mathfrak{a} = \{x + \mathfrak{a}; x \in \mathbb{Z}[i]\}.$$

Como $2 \equiv i \ (mod\ \mathfrak{a})$, *então para* $x = a + bi$, $a, b \in \mathbb{Z}$, *temos*

$$x = a + bi \equiv a + 2b \ (\mathrm{mod}\, \mathfrak{a}).$$

Visto que $(2+i)(2-i) = 5 \in \mathfrak{a}$, *segue que as classes laterais de* $\mathfrak{a}$ *em* $\mathbb{Z}[i]$ *são* $\{0, 1, -1, 2, -2\}$, *ou seja,* $N(\mathfrak{a}) = 5$.

Exemplo 2.1.22 *Em* $\mathbb{Z}[\zeta_p]$, *seja* $\mathfrak{p} = (1-\zeta_p)^i\mathbb{Z}[\zeta_p]$. *Pela propriedade multiplicativa da função norma, temos* $N(\mathfrak{p}^i) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1-\zeta_p)^i = p^i$.

Uma propriedade imediata que se tem é que se $\mathfrak{a}$ é um ideal não principal, então $N_{K|\mathbb{Q}}(x) > N(\mathfrak{a})$, para todo $x \in \mathfrak{a}$.

2.2 Decomposição de Ideais

Consideremos o anel de inteiros $A = \mathbb{Z}[\sqrt{-5}]$ de $\mathbb{Q}(\sqrt{-5})$. Note que $(1+\sqrt{-5})(1-\sqrt{-5}) = 2.3$, e estes fatores têm normas $6, 6, 4$ e 9, respectivamente. Note que $1+\sqrt{-5}$ não tem divisor não trivial em A, já que a norma deste divisor é também um divisor não trivial de 6; isto é impossível, pois as equações $a^2+5b^2 = 2$ e $a^2+5b^2 = 3$ não têm solução em $\mathbb{Z}$. Tomando normas, conclui-se que o primo $1+\sqrt{-5}$ não divide 2.3, de forma que a fatoração de 6 em irredutíveis de $\mathbb{Z}[\sqrt{-5}]$ não é única.

Contudo, Kummer (1810-1893) observou que em certos anéis a fatoração de ideais em ideais primos existe e é única. Estes anéis são chamados de "anéis de Dedekind ", que serão estudados a seguir. A principal propriedade destes anéis é a unicidade da fatoração em ideais primos.

Consideraremos também a fatoração de ideais em uma extensão e, em particular, em uma extensão galoisiana.

Um A-módulo M é dito Noetheriano se satisfaz uma das seguintes condições equivalentes:

(i) Toda coleção não vazia de submódulos de M contém um elemento maximal.

(ii) Toda cadeia crescente de submódulos de M é estacionária.

(iii) Todo submódulo de M é finitamente gerado.

Um anel A é dito Noetheriano se, visto como A-módulo, for um módulo Noetheriano.

Um domínio A é chamado de domínio de Dedekind se for integralmente fechado, Noetheriano e se todo ideal primo não nulo de A for maximal.

Teorema 2.2.1 *([24], pp.50, Teor.3) Sejam A um anel de Dedekind e $\mathfrak{a}$ um ideal não nulo de A. Então existem ideais primos não nulos $\mathfrak{p}_1,\ldots,\mathfrak{p}_n$ de A e inteiros positivos $e_1,\ldots,e_n$ tais que*

$$\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i},$$

e esta expressão é única, a menos da ordem dos fatores.

Veremos a seguir a decomposição de um ideal em uma extensão.

No restante desta seção, K e L denotarão corpos de números com $K \subset L$ e $[L:K] = n$.

Proposição 2.2.2 *([24], pp.71, Prop.1) Seja $\mathfrak{p}$ um ideal primo não nulo de $\mathcal{O}_K$ e*

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{q} \mathfrak{p}_i^{e_i}$$

a decomposição de $\mathfrak{p}\mathcal{O}_L$ em ideais primos de $\mathcal{O}_L$. Então os ideais $\mathfrak{p}_{i's}$ são precisamente os ideais primos $\mathfrak{q}$ de $\mathcal{O}_L$ tais que $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$.

Nas condições da Proposição 2.2.2, diremos que os $\mathfrak{p}_{i's}$ estão acima de $\mathfrak{p}$.

Indicaremos por f_i a dimensão $[\mathcal{O}_L/\mathfrak{p}_i : \mathcal{O}_K/\mathfrak{p}]$ e chamaremos de grau residual de $\mathfrak{p}_i$ sobre $\mathcal{O}_K$. O elemento e_i é chamado de índice de ramificação de $\mathfrak{p}_i$ sobre $\mathcal{O}_K$, e se $e_i > 1$ para algum índice i, diremos que $\mathfrak{p}$ se ramifica em $\mathcal{O}_L$.

Mais adiante daremos uma caracterização dos ideais de $\mathcal{O}_K$ que se ramificam em $\mathcal{O}_L$, mas antes veremos alguns resultados essenciais ao estudo da extensão de ideais:

Teorema 2.2.3 *([24], pp.71, Teor.1) (Igualdade Fundamental) Com as mesmas notações acima,*

$$\sum_{i=1}^{q} e_i f_i = [\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L : \mathcal{O}_K/\mathfrak{p}] = n.$$

Teorema 2.2.4 *([24], pp. 74, Teor.1) Seja K um corpo de números. Uma condição necessária e suficiente para que um ideal primo $p\mathbb{Z}$ de $\mathbb{Z}$ se ramifique em $\mathcal{O}_K$ é que p divida $\mathfrak{D}_K$.*

Como consequência do Teorema acima, pode-se concluir que existe apenas um número finito de ideais primos de $\mathbb{Z}$ que se ramificam em $\mathcal{O}_K$.

Teorema 2.2.5 *(Kummer) ([4], pp. 186, Teor. 10.1) Sejam $K = \mathbb{Q}(x)$ um corpo de números, $x \in \mathcal{O}_K$ e $g(X)$ o polinômio minimal de x sobre $\mathbb{Q}$. Sejam ainda p um número primo que não divide $[\mathcal{O}_K : \mathbb{Z}[x]]$, $g_p(X)$ a redução de $g(X)$ em $(\mathbb{Z}/p\mathbb{Z})[X]$ e os polinômios irredutíveis e mônicos $\mu_i(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ tais que*

$$g_p(X) = \prod_{i=1}^{g} \mu_i(X)^{e_i}.$$

Então $p.\mathcal{O}_K$ pode ser fatorado como

$$p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i},$$

onde

$$\mathfrak{p}_i = p\mathcal{O}_K + \mu_i(x).\mathcal{O}_K,$$

são ideais primos de $\mathcal{O}_K$. *Além disso,* $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}]$ *é o grau de* $\mu_i(X)$ *e* $N(\mathfrak{p}_i) = p^{f_i}$.

Exemplo 2.2.6 *Pelo Teorema 2.1.16, o discriminante de* $K = \mathbb{Q}(\zeta_p)$ *é* $\pm p^{p-2}$. *Assim, o único primo que se ramifica em* $\mathcal{O}_K$ *é* p. *O ideal* $\mathfrak{p} = (1-\zeta_p)\mathbb{Z}[\zeta_p]$ *está acima de* $p\mathbb{Z}$, *já que* $N(\mathfrak{p}) = p$. *Da igualdade fundamental,*

$$p\mathbb{Z}[\zeta_p] = \mathfrak{p}^{p-1}.$$

Exemplo 2.2.7 *Sejam* $A = \mathbb{Z}[\zeta_{39}]$ *o anel de inteiros algébricos de* $K = \mathbb{Q}(\zeta_{39})$ *e*

$$g(X) = X^{24} - X^{23} + X^{21} - X^{20} + X^{18} - X^{17} + X^{15}$$
$$-X^{14} + X^{12} - X^{10} + X^9 - X^7 + X^6 - X^4 + X^3 - X + 1$$

o polinômio minimal de ζ_{39} *sobre* $\mathbb{Q}$. *Vamos obter uma fatoração de* $3\mathcal{O}_K$. *Com a notação acima, a redução de* $g(X)$ *módulo* 3 *é*

$$g_3(X) = \mu_1(X)^2.\mu_2(X)^2.\mu_3(X)^2.\mu_4(X)^2,$$

onde

$$\mu_1(X) = X^3 + 2X + 2;$$
$$\mu_2(X) = X^3 + X^2 + X + 2;$$
$$\mu_3(X) = X^3 + 2X^2 + 2X + 2;$$
$$\mu_4(X) = X^3 + X^2 + 2.$$

Logo, $e_i = 2$ *e sendo o grau residual igual ao grau de* $\mu_i(X)$ *concluímos que* $f_i = 1$, *para* $i = 1, 2, 3, 4$. *Portanto,*

$$3\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2\mathfrak{p}_4^2,$$

onde

$$\mathfrak{p}_i = 3\mathcal{O}_K + \mu_i(\zeta_{39})\mathcal{O}_K,\ i = 1, 2, 3, 4.$$

Para a fatoração de $13\mathcal{O}_K$*, temos*

$$g_{13}(X) = \gamma_1(X)^{12}\gamma_2(X)^{12},$$

onde

$$\gamma_1(X) = X + 4;$$
$$\gamma_2(X) = X + 10.$$

Analogamente, o índice de ramificação e o grau residual são 12 *e* 1*, respectivamente. Então*

$$13\mathcal{O}_K = \mathfrak{q}_1^{12}\mathfrak{q}_2^{12},$$

onde

$$\mathfrak{q}_i = 3\mathcal{O}_K + \gamma_i(\zeta_{39})\mathcal{O}_K,\ i = 1, 2.$$

Para a norma, vale

$$N(\mathfrak{q}_i) = 13,\ i = 1, 2.$$

Quando se trata de uma extensão galoisiana, a decomposição obtida na seção anterior assume características particulares.

A seguir, faremos uso de resultados clássicos de Teoria de Galois finita.

Definição 2.2.8 *Um corpo de números* K *é dito abeliano (resp. cíclico) quando* K *é uma extensão galoisiana de* K *e seu grupo de Galois é abeliano (resp. cíclico).*

Exemplos de extensões abelianas são os corpos ciclotômicos, juntamente com seus subcorpos, conforme o seguinte

Teorema 2.2.9 *([24], pp.87) Seja K um subcorpo de $\mathbb{Q}(\zeta_n)$. Então K é uma extensão abeliana de $\mathbb{Q}$, com grupo de Galois isomorfo a um subgrupo de $(\mathbb{Z}/n\mathbb{Z})^*$. Em particular, se n é um número primo, então K é uma extensão cíclica de $\mathbb{Q}$.*

Vimos no Exemplo 2.2.7 que em $\mathbb{Q}(\zeta_{39})$ os índices de ramificação e_i e os graus residuais f_i são idênticos. Como veremos a seguir, isto sempre ocorre em extensões galoisianas.

No restante desta seção, consideraremos que L é uma extensão galoisiana de K, com grupo de Galois G.

Diz-se que dois ideais $\mathfrak{q}$ e $\mathfrak{q}'$ de $\mathcal{O}_L$ são K-conjugados se existir $\sigma \in G$ tal que $\sigma(\mathfrak{q}) = \mathfrak{q}'$. Quando $K = \mathbb{Q}$, diremos apenas que são conjugados.

Proposição 2.2.10 *([24], pp.89, Prop.1) Sejam $K \subseteq L$ corpos e um ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$. Então os ideais primos $\mathfrak{p}_i$ de $\mathcal{O}_L$ acima de $\mathfrak{p}$ são conjugados dois a dois, têm os mesmos índices de ramificação e graus residuais. Portanto,*

$$\mathfrak{p}\mathcal{O}_L = (\prod_{i=1}^{r} \mathfrak{p}_i)^e,$$

onde $n = ref$.

Sejam K_1 e K_2 corpos de números linearmente disjuntos. Por [20], pp. 65, dado um número primo p, a decomposição de $p\mathcal{O}_{K_1K_2}$ em K_1K_2 pode ser obtida através da decomposição em K_1 e em K_2. Mais precisamente, sejam r_j, e_j e f_j os parâmetros associados à decomposição de $p\mathcal{O}_{K_j}$ em K_j, $j = 1, 2$. Em K_1K_2, os parâmetros r, e e f satisfazem: $r = r_1r_2$, $e = e_1e_2$ e $f = f_1f_2$. Cada ideal primo de $\mathcal{O}_{K_1}$ acima de p se estende em $\mathcal{O}_{K_1K_2}$ de maneira análoga à que p se estende em $\mathcal{O}_{K_2}$.

Definição 2.2.11 *Dado um ideal primo $\mathfrak{p}_i \in \mathcal{O}_L$ satisfazendo $\mathfrak{p}_i \cap \mathcal{O}_K = \mathfrak{p}$, os conjuntos*

$$\mathcal{D}(\mathfrak{p}_i) = \{\sigma \in G; \sigma(\mathfrak{p}_i) = \mathfrak{p}_i\}$$

$$e$$

$$\mathcal{E}(\mathfrak{p}_i) = \{\sigma \in G; \sigma(x) \equiv x(\ mod\ \mathfrak{p}_i\ ),\ para\ todo\ x \in \mathcal{O}_L\}$$

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

Quando G é abeliano, então $\mathcal{D}(\mathfrak{p}_i)$ depende apenas de p. Neste caso, denotaremos simplesmente por $\mathcal{D}(\mathfrak{p})$.

Teorema 2.2.12 *([20], pp.100, Teor.28) Seja $L_{\mathcal{D}(\mathfrak{p})}$ o subcorpo de L fixado por $\mathcal{D}(\mathfrak{p})$. Vale o seguinte diagrama:*

	graus	*indice de ramific.*	*grau inercial*
L			
|	ef	e	f
$L_{\mathcal{D}(\mathfrak{p})}$			
|	r	1	1
K			

Ainda sobre o diagrama, valem os seguintes resultados:

Teorema 2.2.13 *([20], pp. 104, Teor.29) Ainda com as mesmas notações, valem:*

(1) $L_{\mathcal{D}(\mathfrak{p})}$ é o maior subcorpo de L contendo K tal que $e = f = 1$;
(2) $L_{\mathcal{D}(\mathfrak{p})}$ é o menor subcorpo K', com $K \subseteq K' \subseteq L$ tal que existe um único ideal primo de $\mathcal{O}_L$ acima de $\mathfrak{p} \cap K'$.

Exemplo 2.2.14 *Em* $K = \mathbb{Q}(\zeta_{21})$ *a fatoração de* $7\mathcal{O}_K$ *em* $\mathcal{O}_K$ *é*

$$7\mathcal{O}_K = \mathfrak{q}_1^6\mathfrak{q}_2^6,$$

onde $\mathfrak{q}_1$ *e* $\mathfrak{q}_2$ *são ideais primos de* $\mathcal{O}_K$.

O grupo dos $\mathbb{Q}$*-automorfismos de* K *é*

$$G = \{\sigma_i; (i, 21) = 1, i = 1, ..., 21\},$$

onde

$$\sigma_i(\zeta_{21}) = \zeta_{21}^i.$$

O grupo de decomposição de $7\mathcal{O}_K$ *é*

$$\mathcal{D}(7\mathbb{Z}) = \{\sigma \in G; \sigma(\mathfrak{q}_1) = \mathfrak{q}_1\} = \{\sigma_1, \sigma_4, \sigma_{10}, \sigma_{13}, \sigma_{16}, \sigma_{19}\}.$$

Logo, o corpo fixo de $\mathcal{D}(7\mathbb{Z})$ *será* $\mathbb{Q}(\zeta_{21}^7) = \mathbb{Q}(\zeta_3)$. *Analogamente,* $\mathbb{Q}$ *é o corpo fixo de* $\mathcal{D}(3\mathbb{Z})$.

No corpo ciclotômico $\mathbb{Q}(\zeta_n)$, o número de ideais acima de um primo é dado pelo seguinte resultado:

Teorema 2.2.15 *([20] , pp. 34) Seja* p *um primo que não divide* n. *Então o número* r_p *de ideais primos distintos acima de* p *em* $\mathbb{Q}(\zeta_{p^s n})$ *é*

$$r_p = \frac{\phi(n)}{Ord_n(p)},$$

onde $Ord_n(p)$ *é a ordem de* p *módulo* n.

Como exemplo, a decomposição de $3\mathbb{Z}[\zeta_{39}]$ e $13\mathbb{Z}[\zeta_{39}]$ em $\mathbb{Z}[\zeta_{39}]$ pode ser obtida a partir deste resultado.

2.3 Reticulados e Densidade de Centro

Os reticulados têm se mostrado bastante úteis em aplicações na Teoria das Comunicações, sobretudo na geração de constelações de sinais com propriedades convenientes.

Intuitivamente, um reticulado em $\mathbb{R}^n$ é um conjunto infinito de pontos dispostos de forma regular.

Nas seções a seguir serão definidos a densidade de empacotamento esférico e a densidade de centro. Veremos, também, um método algébrico para geração de reticulados em $\mathbb{R}^n$, o chamado homomorfismo canônico, com respectivas propriedades. Mostraremos que a realização geométrica (via homomorfismo canônico) de um submódulo do anel de inteiros de um corpo de números de grau n é um reticulado em $\mathbb{R}^n$, cujo volume depende do discriminante do corpo em questão e do índice do módulo no anel de inteiros.

2.3.1 Reticulados em $\mathbb{R}^n$

Sejam V um espaço vetorial de dimensão finita n sobre um corpo K, A um subanel de K e $v_1, ..., v_m$, $m \leq n$, vetores linearmente independentes de V. Dá-se o nome de A-reticulado (ou simplesmente reticulado) com base $\{v_1, ..., v_m\}$ ao conjunto

$$\{x = \sum_{i=1}^{m} a_i v_i \ ; \ a_i \in A, \ i = 1, ..., m\}.$$

Nosso interesse maior será pelos casos em que $K = \mathbb{R}$, $A = \mathbb{Z}$, $V = \mathbb{R}^n$ e $m = n$. Quando nos referimos a um reticulado Λ, fica implícito que estaremos assumindo as condições acima.

Um empacotamento esférico em $\mathbb{R}^n$ é uma distribuição de esferas de mesmo raio em $\mathbb{R}^n$ de tal forma que estas esferam tenham no máximo um ponto em comum. A isso, chamaremos simplesmente de empacotamento. Pode-se descrever um empacotamento

simplesmente indicando o conjunto dos centros das esferas e o raio destas. Um empacotamento reticulado é um empacotamento em que o conjunto dos centros forma um reticulado Λ de $\mathbb{R}^n$ e, a menos que se diga o contrário, daqui em diante todos os empacotamentos considerados serão reticulados; diremos neste caso que o empacotamento é associado a Λ.

Intuitivamente, a densidade de empacotamento de um reticulado é a "proporção" do espaço $\mathbb{R}^n$, coberto pelas esferas.

A seguir, introduziremos os elementos básicos que possibilitarão obter uma definição formal e uma expressão para a densidade de um empacotamento.

Dado um reticulado $\Lambda \subset \mathbb{R}^n$ com $\mathbb{Z}$-base $\beta = \{v_1, ..., v_n\}$, denomina-se região fundamental de Λ, com relacão à base β, o conjunto

$$\Lambda_\beta = \{x \in \mathbb{R}^n; x = \sum_{i=1}^n \lambda_i v_i \, , \, 0 \leq \lambda_i < 1\}.$$

O espaço euclidiano $\mathbb{R}^n$ é a união disjunta de translações da região fundamental Λ_β por vetores de Λ. Consideremos um empacotamento associado a Λ. Para o cálculo da proporção coberta pelas esferas, basta calcular a proporção em uma região fundamental Λ_β ; é o que faremos a seguir.

Fazendo $v_i = (v_{i1}, ..., v_{in})$, $i = 1, ..., n$; o volume $v(\Lambda_\beta)$ de Λ_β é igual ao módulo do determinante da matriz

$$B = \begin{bmatrix} v_{11} & \cdots & v_{1n} \\ \vdots & \ddots & \vdots \\ v_{n1} & \cdots & v_{nn} \end{bmatrix}.$$

Se β' é uma outra base para Λ, segue que $v(\Lambda_\beta) = v(\Lambda_{\beta'})$ já que β e β' diferem pelo produto de uma matriz inversível com entradas inteiras. Dessa forma, faz sentido definir o volume de Λ como sendo o volume da região fundamental de uma base qualquer, e será denotado por $v(\Lambda)$.

Interessará o empacotamento associado ao reticulado Λ tal que as esferas tenham raio máximo. Para a determinação deste raio, observe que fixado $k > 0$, a intersecção do conjunto compacto $\{x \in \mathbb{R}^n; \mid x \mid \leq k\}$ com o reticulado Λ é um conjunto finito, isto é, Λ é discreto, de onde segue que o número

$$d_{min} = min\{\mid v \mid; v \in \Lambda,\, v \neq 0\}$$

está bem definido.

Podemos observar que $\rho = d_{min}/2$ é o maior raio dentre os quais é possível distribuir esferas centradas nos pontos de Λ e obter um empacotamento. Dessa forma, estudar os empacotamentos reticulados equivale ao estudo dos reticulados. Com isto, quando citamos densidade do reticulado Λ, ficará implícito que estamos falando da densidade do empacotamento com esferas de raio ρ associado a este reticulado, e que será denotada por $\Delta(\Lambda)$.

Indicando por $B(\rho)$ a esfera com centro na origem e raio ρ, temos

$$\Delta(\Lambda) = \frac{volume\ da\ região\ fundamental\ coberta\ pelas\ esferas}{volume\ da\ região\ fundamental} = \frac{v(B(\rho))}{v(\Lambda)} =$$

$$= \frac{v(B(1)).\rho^n}{v(\Lambda)},$$

$$\text{onde } v(B(1)) = \begin{cases} \dfrac{\pi^{n/2}}{(n/2)!} & \text{, se } n \text{ é par;} \\ \dfrac{2^n \pi^{(n-1)/2}((n-1)/2)!}{n!} & \text{, se } n \text{ é ímpar.} \end{cases}$$

Visto que $v(B(\rho)) = \rho^n.v(B(1))$, é conveniente o uso de um outro parâmetro, a saber a densidade de centro,

$$\delta(\Lambda) = \frac{\rho^n}{v(\Lambda)}.$$

Exemplo 2.3.1 *Para o reticulado* $\mathbb{Z}^n$, *temos* $\rho = \frac{1}{2}$ *e* $v(\mathbb{Z}^n) = 1$. *Assim,*

$$\delta(\mathbb{Z}^n) = \frac{1}{2^n}.$$

Um outro parâmetro bastante usado em aplicações é o chamado ganho fundamental, dado por

$$\gamma(\Lambda) = \frac{d^2_{\min}}{v(\Lambda)^{2/n}}.$$

2.3.2 O homomorfismo canônico de um corpo de números

A seguir descreveremos o homomorfismo canônico para a geração de reticulados via ideais de corpos de números. Faremos, inicialmente, considerações para o caso em que todas as imersões são reais e depois para o caso em que todas as imersões são complexas.

Definição 2.3.2 *Um corpo de números* K *de grau* n *é dito totalmente real quando para todo* $\mathbb{Q}$*-monomorfismos* $\sigma_i : K \to \mathbb{C}$, $i = 1, \ldots, n$, *valer*

$$\sigma_i(K) \subseteq \mathbb{R}.$$

K *será chamado totalmente complexo quando*

$$\sigma_i(K) \not\subseteq \mathbb{R},$$

para $i = 1, \ldots, n$.

Sejam K um corpo de números totalmente real de dimensão n e $\sigma_1, ..., \sigma_n$ os $\mathbb{Q}$-monomorfismos de K em $\mathbb{C}$. A aplicação $\sigma : K \mapsto \mathbb{R}^n$, dada por

$$\sigma(x) = (\sigma_1(x), ..., \sigma_n(x)),$$

define um homomorfismo de $\mathbb{Z}$-módulos de K em $\mathbb{R}^n$.

Exemplo 2.3.3 *Seja $K = \mathbb{Q}(\sqrt{3})$, com a $\mathbb{Q}$-base $\{1, \sqrt{3}\}$ e grupo de automorfismos $\{\sigma_1, \sigma_2\}$, onde σ_1 é a identidade e σ_2 a conjugação, ou seja, $\sigma_2(a + b\sqrt{3}) = a - b\sqrt{3}$, $a, b \in \mathbb{Q}$. Então a imagem de $x = a + b\sqrt{3}$, $a, b \in \mathbb{Q}$ pelo homomorfismo σ é*

$$\sigma(x) = (\sigma_1(x), \sigma_2(x)) = (a + b\sqrt{3}, a - b\sqrt{3}).$$

Consideremos agora um corpo de números totalmente complexo K, de dimensão n, e sejam $\sigma_1, ..., \sigma_n$ os n $\mathbb{Q}$-monomorfismos de K em $\mathbb{C}$. Suponhamos os $\sigma_{i's}$ ordenados de forma que $\sigma_{i+n/2} = \overline{\sigma_{n/2}}$, para $i = 1, ..., n/2$. Como $\sigma_i(K)$ não está contido em $\mathbb{R}$, para todo i, então aplicando o processo acima estaremos gerando vetores em $\mathbb{C}^n \simeq \mathbb{R}^{2n}$. Neste caso, o número n é par, já que a cada σ_i está associado seu conjugado complexo $\overline{\sigma_i}$. Sendo assim, uma maneira de gerar vetores em $\mathbb{R}^n$ é definindo $\sigma : K \mapsto \mathbb{R}^n$ por

$$\sigma(x) = (R\sigma_1(x), I\sigma_1(x), ..., R\sigma_{n/2}(x), I\sigma_{n/2}(x)),$$

onde $R(z)$ e $I(z)$ representam a parte real e imaginária do número complexo z, respectivamente.

Exemplo 2.3.4 *Sejam o corpo quadrático $K = \mathbb{Q}(i)$, $i = \sqrt{-1}$ e $\{\sigma_1, \sigma_2\}$ o grupo dos $\mathbb{Q}$-monomorfismos de K em $\mathbb{C}$, onde σ_1 é a aplicação inclusão e σ_2 é a conjugação complexa. Para $x = a + bi \in K$, $a, b \in \mathbb{Q}$, temos*

$$\sigma(x) = (R\sigma_1(x), I\sigma_1(x)) = (a, b).$$

O homomorfismo σ é chamado de homomorfismo canônico de K em $\mathbb{R}^n$. Sua definição estende-se naturalmente ao caso geral.

Uma das vantagens do método é a geração de reticulados em $\mathbb{R}^n$, dos quais os principais parâmetros podem ser obtidos via Teoria Algébrica dos Números, através de propriedades herdadas de K. Isto pode ser visto de maneira formal nos resultados que seguem.

Teorema 2.3.5 *([24], pp.56, Prop.1) Sejam K um corpo de números de grau n, $\sigma_1, ..., \sigma_n$ os $\mathbb{Q}$-monomorfismos de K em $\mathbb{C}$ e $M \subseteq K$ um $\mathbb{Z}$-módulo livre de posto n com $\mathbb{Z}$-base $\{x_1, ..., x_n\}$. Então*

a) $\sigma(M)$ é um reticulado em $\mathbb{R}^n$;

b) $v(\sigma(M)) = 2^{-r_2} \mid det(\sigma_i(x_j)) \mid$,

onde $r_2 = \frac{1}{2} card\{\sigma_i \mid \sigma_i(K) \not\subseteq \mathbb{R}\}$

Exemplo 2.3.6 *Tomemos $K = \mathbb{Q}(\sqrt{3})$ como no exemplo anterior e $M = \mathbb{Z}[\sqrt{3}]$ seu anel de inteiros, com base $\mathbb{Z}$-base $\{1, \sqrt{3}\}$. Como K é real, então $r_2 = 0$, e*

$$v(\sigma(M)) = \left|\left[\begin{array}{cc} \sigma_1(1) & \sigma_1(\sqrt{3}) \\ \sigma_2(1) & \sigma_2(\sqrt{3}) \end{array}\right]\right| = \left|\left[\begin{array}{cc} 1 & \sqrt{3} \\ 1 & -\sqrt{3} \end{array}\right]\right| = 2\sqrt{3}.$$

Note que $\mathbb{Z}[\sqrt{3}] \subseteq \mathbb{R}$ é um conjunto denso, no sentido de que todos seus pontos são de acumulação. No entanto, a imagem do homomorfismo canônico

$$\sigma : \mathbb{Z}[\sqrt{3}] \subseteq \mathbb{R} \rightarrow \mathbb{R}^2$$

é um reticulado de posto 2 em $\mathbb{R}^2$.

Um caso particularmente interessante ocorre quando M é um ideal ordinário não nulo de K. Neste caso, a expressão para o volume do reticulado fica totalmente determinada, como mostra o

Teorema 2.3.7 *([24], pp. 57, Prop.2) Sejam K um corpo de números de grau n e $\mathfrak{a}$ um ideal ordinário não nulo de $\mathcal{O}_K$. Então $\sigma(\mathcal{O}_K)$ e $\sigma(\mathfrak{a})$ são reticulados de $\mathbb{R}^n$, e vale*

$$v(\sigma(\mathfrak{a}\,)) = 2^{-r_2}.\mid \mathfrak{D}_K \mid^{1/2}.N(\mathfrak{a}\,).$$

Chamaremos de realização geométrica de um ideal $\mathfrak{a}$ ao reticulado $\sigma(\mathfrak{a})$. A expressão para a densidade de centro destes reticulados assume a forma

$$\delta(\sigma(\mathfrak{a})) = \frac{2^{r_2}.\rho^n}{\mid \mathfrak{D}_K \mid^{1/2} N(\mathfrak{a})}. \tag{2.2}$$

Podemos medir distâncias em $\sigma(K) \subseteq \mathbb{R}^n$ através de parâmetros de teoria algébrica dos números, conforme a seguinte

Proposição 2.3.8 *([27], pp. 225) Sejam K um corpo de números e $x \in K$. Então*

$$\mid \sigma(x) \mid^2 = c_K.Tr_{K/\mathbb{Q}}(x.\overline{x}),$$

onde

$$c_K = \begin{cases} \dfrac{1}{2}, & \text{se } K \text{ for totalmente complexo;} \\ 1, & \text{se } K \text{ for totalmente real.} \end{cases}$$

Exemplo 2.3.9 *Sejam $K = \mathbb{Q}(\zeta_3)$ e $x = a + b\zeta_3 \in \mathcal{O}_K$. Temos*

$$N_{K/\mathbb{Q}}(x) = a^2 + b^2 - ab.$$

Por outro lado, sendo σ o homomorfismo canônico de K, vale

$$\mid \sigma(x) \mid^2 = a^2 + b^2 - ab = N_{K/\mathbb{Q}}(x).$$

Seja $x \in \mathcal{O}_K$ *e* $\mathfrak{a} = x\mathcal{O}_K$. *Então todo* $y \in \mathfrak{a}$ *é da forma* $y = xz$, *com* $z \in \mathcal{O}_K$. *Logo*

$$| \sigma(y) |^2 = | \sigma(zx) |^2 = N_{K/\mathbb{Q}}(xz) = N_{K/\mathbb{Q}}(x).N_{K/\mathbb{Q}}(z) \geq N_{K/\mathbb{Q}}(x),$$

pois $| N_{K/\mathbb{Q}}(z) | \geq 1$. *Consequentemente, o menor valor assumido por* $| \sigma(y) |^2$, *para* $y \in \mathfrak{a}$ *e* $y \neq 0$, *é* $| N_{K/\mathbb{Q}}(x) |$.

Logo,

$$\rho = \frac{\sqrt{| N_{K/\mathbb{Q}}(x) |}}{2},$$

e a densidade de centro é

$$\delta(\mathfrak{a}) = \frac{2 | N(x) |}{4 | N(x) | . | \mathfrak{D}_K |^{1/2}} = \frac{1}{2\sqrt{3}}.$$

Observação: Como neste caso particular o anel $\mathbb{Z}[\zeta_3]$ é principal, a densidade de centro independe da escolha do ideal. Obtém-se o reticulado Λ_2, o reticulado mais denso em dimensão 2.

Capítulo 3

Corpos de Números Abelianos

Uma classe particular dos corpos de números são os corpos abelianos, ou seja, extensões galoisianas de $\mathbb{Q}$ com grupo de Galois abeliano.

O Teorema de Kronecker-Weber ([29],pp. 319) diz que todo corpo de números abeliano está contido em um corpo ciclotômico $\mathbb{Q}(\zeta_n)$, para algum n. Portanto, estudar os corpos de números abelianos equivale a estudar os subcorpos de corpos ciclotômicos.

A Proposição 3.1.1 caracteriza os elementos do ideal principal $(1-\zeta_{p^r})^t.\mathbb{Z}[\zeta_{p^r}]$ e o Teorema 3.1.3 exibe a forma quadrática em $\mathbb{Q}(\zeta_{p^r})$.

O Teorema 3.3.1 é o principal resultado da seção 3.3 e serve de base para a construção da família $\mathcal{A}_n$. Em seguida são apresentados tabelas e gráficos referentes à respectiva família.

A seção 3.4 faz um estudo de extensões cúbicas contidas em $\mathbb{Q}(\zeta_p)$, p primo, sendo o Teorema 3.4.1 e a Proposição 3.4.4 os resultados centrais da seção.

Finalmente, a seção 3.5 traz técnicas de construções algébricas de reticulados densos em subcorpos de $\mathbb{Q}(\zeta_{pq})$. Destacamos o Corolário 3.5.5 e as técnicas usadas na subseção 3.5.3, que trata das construções algébricas propriamente ditas.

3.1 Reticulados em $\mathbb{Q}(\zeta_{p^r})$

Quando p é um número primo, Maurice Craig estudou a representação geométrica do ideal principal $\mathfrak{p}$ de $\mathbb{Z}[\zeta_p]$ gerado por $1-\zeta_p$ e suas potências (cf. [27], pp. 223). Tais representações geométricas são reticulados em dimensão $n = p-1$. Para sua construção, fixado um número primo p e $i \geq 1$, define-se A^i_{p-1} a representação geométrica do ideal $\mathfrak{p}^i$.

Generalizaremos esta família para $\mathbb{Q}(\zeta_p)$ e subcorpos de $\mathbb{Q}(\zeta_p)$, obtendo para estes últimos novos reticulados densos.

3.1.1 Caracterização do ideal gerado por $(1-\zeta_{p^r})^i$ em $\mathbb{Q}(\zeta_{p^r})$

Proposição 3.1.1 *Sejam $\mathfrak{p}$ o ideal de $\mathbb{Z}[\zeta_{p^r}]$ gerado por $1-\zeta_{p^r}$, $x \in \mathbb{Z}[\zeta_{p^r}]$ e $f(X) \in \mathbb{Z}[X]$ tal que $x = f(\zeta_{p^r})$. Então para $0 \leq i < m$, onde $m = \phi(p^r)$, vale*

$$x \in \mathfrak{p}^{i+1} \Leftrightarrow f(1) \equiv f'(1) \equiv \cdots \equiv f^{(i)}(1) \equiv 0 \pmod{p},$$

onde $f^{(i)}(X)$ denota a i-ésima derivada de f.

Demonstração: O polinômio minimal de ζ_{p^r} sobre $\mathbb{Q}$ é

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

Assim, $x \in \mathfrak{p}^{i+1}$ é equivalente à existência de $u(X) \in \mathbb{Z}[X]$ tal que

$$f(X) \equiv (1-X)^{i+1}u(X) \pmod{h(X)},$$

e a última equação é equivalente à existência de $v(X) \in \mathbb{Z}[X]$ satisfazendo

$$f(X) = (1-X)^{i+1}u(X) + \frac{X^{p^r}-1}{X^{p^{r-1}}-1}v(X).$$

De

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

obtemos,

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

Agora, podemos encontrar $t(X) \in \mathbb{Z}[X]$ tal que

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

ou equivalentemente, existe $u(X) \in \mathbb{Z}[X]$ para o qual

$$f(X) = (1-X)^{i+1}v(X) + pu(X).$$

Assim, $f(\zeta_{p^r}) \in \mathfrak{p}^{i+1}$ é equivalente à expressão acima, sendo esta equivalente à enunciada. □

3.1.2 A forma quadrática associada

Nesta seção, veremos que a forma quadrática que mede distâncias em $\sigma(\mathcal{O}_K)$, $K = \mathbb{Q}(\zeta_{p^r})$, é a soma de p^{r-1} formas quadráticas simétricas, sendo cada uma delas em $p-1$ variáveis.

Dado um elemento $x = \sum_{i=0}^{m-1} a_i \zeta_{p^r}^i \in \mathbb{Z}[\zeta_{p^r}]$, $m = \phi(p^r)$, existe uma única representação sob a forma

$$x = \sum_{j=0}^{t} x_j \zeta_{p^r}^j \tag{3.1}$$

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

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

Dado um elemento $x = a_0 + a_1 \zeta_{p^r} + \cdots + a_{m-1} \zeta_{p^r}^{m-1} \in \mathbb{Z}[\zeta_{p^r}]$, frequentemente usaremos a expressão

$$x\overline{x} = A_0 + \sum_{i=1}^{m-1} A_i \alpha_i \tag{3.2}$$

onde

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

Identificaremos o elemento x com a m-upla correspondente $\underline{x} = (a_0, ..., a_{m-1})$.

Teorema 3.1.2 *Sejam p um número primo e r um inteiro positivo. Então*

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

Demonstração: O polinômio minimal de ζ_{p^r} sobre $\mathbb{Q}$ é

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

Assim, para $r > 1$, temos $Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}) = 0$. Quando k é um inteiro primo com p^r, então $\zeta_{p^r}^k$ é um conjugado de ζ_{p^r}, e seus traços são idênticos.

Para $(k, p^r) > 1$, consideraremos três casos:

1º caso: $(k, p^r) < p^{r-1}$: Pondo $(k, p^r) = p^s$, onde $s < r$, então $\zeta_{p^r}^k = \zeta_{p^r}^{p^s j} = \zeta_{p^{r-s}}^j$, com j primo com p. Assim,

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

2º caso: $(k, p^r) = p^{r-1}$: O polinômio minimal de ζ_p sobre $\mathbb{Q}$ é

$$X^{p-1} + X^{p-2} + \cdots + X + 1 \, .$$

Logo, $Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p) = -1$, e por $\zeta_{p^r}^k = \zeta_{p^r}^{p^{r-1}j} = \zeta_p^j$ temos

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

3º caso: $(k, p^r) > p^{r-1}$: Neste caso, $(k, p^r) = p^r$, e

$$Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_{p^r}^k) = Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1) = (p-1)p^{r-1}.$$

Quando $r = 1$, estaremos no segundo ou terceiro casos. □

Para cada inteiro n, seja Q_n a forma quadrática dada por

$$Q_n(X_1, ..., X_n) = \sum_{i=1}^{n} X_i^2 + \sum_{1 \le i < j \le n} (X_i - X_j)^2. \tag{3.3}$$

Teorema 3.1.3 *Sejam p um número primo, r um inteiro positivo, $K = \mathbb{Q}(\zeta_{p^r})$, $m = \phi(p^r)$ e x um elemento de $\mathcal{O}_K$,*

$$x = a_0 + a_1\zeta_{p^r} + \cdots + a_{m-1}\zeta_{p^r}^{m-1}.$$

Então

$$| \sigma(x) |^2 = \frac{p^{r-1}}{2} \left(\sum_{i=0}^{t} Q_{p-1}(\underline{x_i}) \right),$$

onde $t = p^{r-1} - 1$ *e os* $x_{j's}$ *são como na Equação. 3.1.*

Demonstração: Seja

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

a representação como na Equação 3.2. O Teorema 3.1.2 mostra que os elementos $\zeta_{p^r}^k$, com $(k, p^r) < p^{r-1}$ têm traço nulo. Como vale $Tr_{K|\mathbb{Q}}(\alpha_k) = 2Tr_{K|\mathbb{Q}}(\zeta_{p^r}^k)$, é suficiente considerar os coeficientes dos elementos α_k tais que $(k, p^r) \geq p^{r-1}$. Quando $(k, p^r) > p^{r-1}$, então $(k, p^r) = p^r$ e portanto $k \geq p^r > (p-1)p^{r-1}$. Contudo, isto não ocorre, já que $k \leq m-1$. Logo, podemos considerar somente os índices k tais que $(k, p^r) = p^{r-1}$. Disso segue

$$| \sigma(x) |^2 = \frac{1}{2} \left(Tr_{K/\mathbb{Q}}(A_0) + \sum_{i=1}^{m-1} Tr_{K/\mathbb{Q}}(A_i \alpha_i) \right)$$

$$= \frac{p^{r-1}}{2} \left((p-1).(A_0) - 2. \sum_{j=1}^{p-2} A_{jp^{r-1}} \right)$$

$$= \frac{p^{r-1}}{2} \left((p-1) \sum_{i=0}^{t} \sum_{j \equiv i (\mathrm{mod}\, p^{r-1})} a_j^2 - 2 \sum_{i=0}^{t} \sum_{j \equiv i (\mathrm{mod}\, p^{r-1}), i<j} a_i a_j \right)$$

$$= \frac{p^{r-1}}{2} . \sum_{i=0}^{t} \left((p-1) \sum_{j \equiv i (\mathrm{mod}\, p^{r-1})} a_j^2 - 2 \sum_{j \equiv i (\mathrm{mod}\, p^{r-1}), i<j} a_i a_j \right)$$

$$= \frac{p^{r-1}}{2} \left(\sum_{i=0}^{t} Q_{p-1}(\underline{x_i}) \right) . \ \square$$

3.2 Ideais em $\mathbb{Q}(\zeta_{p^r})$, $r \geq 2$

Nesta seção, estudaremos a densidade de empacotamento do reticulado $\sigma(\mathfrak{p}^i)$, no caso $r \geq 2$, que equivale à generalização da família de Craig A_n^m para este caso. Para isso, precisamos determinar o raio de empacotamento do reticulado associado, através de sua forma quadrática.

Como vimos, a forma quadrática Q_n está relacionada com o cálculo de distâncias nos reticulados considerados.

A forma quadrática Q_n pode ser escrita como

$$Q_n(X_1, ..., X_n) = (n+1).\sum_{i=1}^{n} X_i^2 - \left(\sum_{i=1}^{n} X_i\right)^2. \tag{3.4}$$

Note que Q_n é positiva definida e simétrica, ou seja,

$$Q_n(X_1, ..., X_n) = Q_n(X_{\sigma(1)}, ..., X_{\sigma(n)}),$$

onde σ é uma permutação qualquer do conjunto $\{1, ..., n\}$.

A seguir, estudaremos propriedades da forma quadrática Q_n, iniciando por encontrar o menor valor assumido por Q_n, considerando entradas inteiras não todas nulas.

Lema 3.2.1 *([11], pp. 64) (i) O menor valor atingido por Q_n com entradas inteiras não todas nulas, é n.*

(ii) Para $a \in \mathbb{Z}^n$, $Q_n(a) = n$ quando $a = \pm(1, 1, .., 1)$ ou $a = \pm e_i$, $i = 1, ..., n$, onde $\{e_i\}$, $i = 1, ..., n$ é a $\mathbb{Z}$-base canônica de $\mathbb{Z}^n$.

Proposição 3.2.2 *Para $r \geq 2$, o menor valor atingido por $\sum_{i=0}^{t} Q_{p-1}(\underline{x_i})$, para $x \in \mathfrak{p}$ e $x \neq 0$, é $2(p-1)$.*

Demonstração: Tomando $z = 1 - \zeta_{p^r} \in \mathfrak{p}$, então $\sum_{i=0}^{t} Q_{p-1}(\underline{z_i}) = 2(p-1)$. Tal valor é mínimo. De fato, seja $x \in \mathfrak{p}$ e x_i como na Equação 3.1. Se consideramos apenas um dos $x_{i's}$ não nulos, então este necessariamente está em $\mathfrak{p}$, e daí $Q_{p-1}(\underline{x_j}) \geq 2p$. Sendo $p-1$ o menor valor assumido por $Q_{p-1}(a)$, com $a \in \mathbb{Z}^{p-1}$, segue que se o número de $x_{i's}$ não nulos é maior que 1, então $\sum_{i=0}^{t} Q_{p-1}(\underline{x_i}) \geq 2(p-1)$. □

A seguir, determinaremos a densidade de centro de reticulados $\sigma(\mathfrak{p}^i)$.

Teorema 3.2.3 *Sejam p um número primo, $r > 2$ e $\mathfrak{p} = (1-\zeta_{p^r}).\mathbb{Z}[\zeta_{p^r}]$. Então a maior densidade de centro entre os reticulados $\sigma(\mathfrak{p}^i)$, $i = 1, ..., (p-1)p^{r-2}$, ocorre em $i = 1$.*

Demonstração: Da congruência $1 - \zeta_{p^r}^{(p-1)p^{r-2}} \equiv (1-\zeta_{p^r})^{(p-1)p^{r-2}} (\mathrm{mod}\, p)$ e de $p = (1-\zeta_{p^r})^{(p-1)p^{r-1}}$ chegamos a $y = 1 - \zeta_{p^r}^{(p-1)p^{r-2}} \in \mathfrak{p}^{(p-1)p^{r-2}}$. Além disso, $\sum_{i=0}^{t} Q_{p-1}(\underline{y_i}) = 2(p-1)$, e para cada $i \in \{1, ..., (p-1)p^{r-2}\}$, a densidade de centro é

$$\delta(\mathfrak{p}^i) = \frac{((p-1)p^{r-1})^{m/2}}{2^{m/2}. \mid \mathfrak{D}_K \mid^{1/2} .p^i}, \tag{3.5}$$

onde $m = \phi(p^r)$ e $\mid \mathfrak{D}_K \mid = p^{p^{r-1}(pr-r-1)}$. Isto mostra que $\sigma(\mathfrak{p})$ é o reticulado mais denso dentre as potências consideradas. □

Teorema 3.2.4 *Sejam $p > 2$ um número primo, $r = 2$ e $\mathfrak{p} = (1-\zeta_{p^r}).\mathbb{Z}[\zeta_{p^r}]$. Então a maior densidade de centro dentre os reticulados $\sigma(\mathfrak{p}^i)$, $i = 1, ..., p$, ocorre em $i = 2$.*

Demonstração: Mostraremos que para $x \in \mathfrak{p}^i$,o menor valor assumido por $\sum_{i=0}^{t} Q_{p-1}(\underline{x_i})$, para $i = 2, ..., p$, é $2p$. Começaremos com o caso $i = 2$.

Sejam $x \in \mathfrak{p}^2$ e $x_{i's}$ como na Equação 3.1. Se apenas um dos $x_{i's}$ é não nulo, podemos recorrer ao caso $r = 1$, que dá $\sum_{i=0} Q_{p-1}(\underline{x_i}) \geq 2p$. Se o número de $x_{i's}$ não nulos é maior que 2, então $\sum_{i=0}^{t} Q_{p-1}(\underline{x_i}) \geq 3(p-1) \geq 2p$. Assim, resta mostrar para o caso em que dois dos $x_{i's}$ são não nulos, digamos x_i e x_j.

Mostraremos que neste caso $Q_{p-1}(\underline{x_i}) + Q_{p-1}(\underline{x_j})$ não assume o valor $2(p-1)$. De fato, se isto ocorre, então $Q(\underline{x_i}) = Q(\underline{x_j}) = (p-1)$, e pelo Lema 3.2.1 isto ocorre somente para $x_i, x_j \in \{\pm\zeta_{p^r}^{jp^{r-1}}, j = 0, ..., p-1\}$.

Pondo $x_i = \zeta_{p^r}^{ap^{r-1}}$ e $x_j = -\zeta_{p^r}^{bp^{r-1}}$, com $a, b \in \{0, ..., p-2\}$, então

$$x = \zeta_{p^r}^{ap^{r-1}+i} - \zeta_{p^r}^{bp^{r-1}+j} .$$

Como $x \in \mathfrak{p}^2$, o Lema 3.1.1 dá

$$ap^{r-1} + i - bp^{r-1} - j \equiv i - j \equiv 0 (\mathrm{mod}\, p),$$

contradizendo a hipótese sobre x_i e x_j.

Para os demais casos, mostraremos de forma análoga que $Q_{p-1}(\underline{x_i}) = Q_{p-1}(\underline{x_j}) = p-1$ também não ocorre. Note que o elemento $x = 1 - \zeta_{p^2}^{p}$ está em $\mathfrak{p}^i$, para $i = 1, ..., p$, e $\sum_{i=0}^{t} Q_{p-1}(\underline{x_i}) = 2p$. O valor $2p-1$ também não é atingido. Com isto, mostramos que $Q_{p-1}(\underline{x_i}) + Q_{p-1}(\underline{x_j})$ não assume o valor $2(p-1)$.

Das considerações acima, concluímos que os raios de empacotamento são idênticos, para $i = 2, ..., p$, e isto nos permite concluir que o ideal de menor norma, que é $\mathfrak{p}^2$, produzirá o reticulado mais denso dentre aqueles do tipo $\sigma(\mathfrak{p}^i)$, $i = 2, ..., p$. Confrontando as densidades de centro de $\sigma(\mathfrak{p})$ e $\sigma(\mathfrak{p}^2)$, conclui-se a prova. □

Em $\mathbb{Q}(\zeta_9)$, o reticulado $\sigma(\mathfrak{p}^2)$ coincide com E_6, e apresenta a maior densidade de centro conhecida em dimensão 6 .

Adequado à nossa notação, temos o seguinte

Lema 3.2.5 *([27], pp. 223) Sejam* $K = \mathbb{Q}(\zeta_p)$ *e* $\mathfrak{p} = (1-\zeta_p)\mathcal{O}_K$. *Então para* $x \in \mathfrak{p}^i$, $i = 1, \ldots, (p-1)/2$, *vale*

$$Tr_{K/\mathbb{Q}}(x\overline{x}) \geq 2pi. \tag{3.6}$$

Proposição 3.2.6 *Para* $r \geq 2$, $i \leq (p-1)/2$ *e* $x \in (1-\zeta_{p^r})^{i.p^{r-1}}.\mathbb{Z}[\zeta_{p^r}]$, *vale*

$$Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(x\overline{x}) \geq 2p^r i \ .$$

Demonstração: Seja $x = (1-\zeta_{p^r})^{i.p^{r-1}}.z$, onde $z \in \mathbb{Z}[\zeta_{p^r}]$. Tal z pode ser escrito sob a forma

$$z = a_0 + a_1\zeta_{p^r} + \cdots + a_{m-1}\zeta_{p^r}^{m-1} = \sum_{j=0}^{t} z_j\zeta_{p^r}^j,$$

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

$$z_j = \sum_{\substack{i=0 \\ i\equiv j(\mathrm{mod}\ p^{r-1})}}^{m-1} a_i\zeta_{p^r}^i \ .$$

Além disso,

$$(1-\zeta_{p^r})^{i.p^{r-1}} = \sum_{k=0}^{m-1} b_k\zeta_{p^r}^{k.i.p^{r-1}},$$

que nos dá

$$x = \left(\sum_{k=0}^{m-1} b_k\zeta_{p^r}^{k.i.p^{r-1}}\right)\left(\sum_{j=0}^{t} z_j.\zeta_{p^r}^j\right)$$

$$= \sum_{j=0}^{t}\left(\sum_{k=0}^{m-1} b_k\zeta_{p^r}^{k.i.p^{r-1}}\right)\left(\sum_{\substack{i=0 \\ i\equiv j(\mathrm{mod}\ p^{r-1})}}^{m-1} a_i\zeta_{p^r}^i\right)\zeta_{p^r}^j$$

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

Assim, cada x_j está em $\mathfrak{p}^{ip^{r-1}}$. Além disso, $Tr_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(x\overline{x})$ é mínimo quando apenas um dos $x_{j's}$ é não nulo. Podemos ver a equação acima como os múltiplos de $(1-\zeta_p)^i$ em $\mathbb{Z}[\zeta_p]$, $i = 1, ..., (p-1)/2$, que juntamente com o Lema 3.2.5 e o Teorema 3.1.3 nos permite concluir o resultado. □

Teorema 3.2.7 *Sejam p primo,* $K = \mathbb{Q}(\zeta_{p^r})$ *e* $\mathfrak{p} = (1-\zeta_{p^r}).\mathbb{Z}[\zeta_{p^r}]$. *Então*

$$\delta(\sigma(\mathfrak{p}^{ip^{r-1}})) \geq \left(\frac{i}{2}\right)^{\frac{(p-1)p^{r-1}}{2}} .p^{p^{r-1}(\frac{1-2i}{2})}. \tag{3.7}$$

Demonstração: Pela Proposição 3.2.6, o raio de empacotamento satisfaz

$$\rho \geq \frac{\sqrt{c_K.2p^r i}}{2},$$

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

Pelo Teorema 2.1.17, o discriminante de K satisfaz

$$|\mathfrak{D}_K| = p^{p^{r-1}(pr-r-1)}.$$

A norma de $\mathfrak{p}^{ip^{r-1}}$ é $p^{ip^{r-1}}$. Cálculos mostram a expressão enunciada. □

Fixados p e i, a expressão acima é uma função decrescente de r. Assim, as melhores densidades são obtidas para $r = 1$, que coincide justamente com a família de Craig A_n^m.

3.3 Subcorpos de $\mathbb{Q}(\zeta_p)$

Nesta seção, construiremos a família de reticulados $\mathcal{A}_n$ a partir de subcorpos de $\mathbb{Q}(\zeta_p)$. O principal resultado é o Teorema que se segue:

Teorema 3.3.1 *Sejam $L = \mathbb{Q}(\zeta_p)$, K o subcorpo de L de grau $(p-1)/t$, $\mathfrak{p} = (1-\zeta_p).\mathbb{Z}[\zeta_p]$ e $\mathfrak{p}_K = \mathfrak{p} \cap K$. Então*

$$\delta(\sigma(\mathfrak{p}_K^i)) \geq \left(\frac{i}{2}\right)^{\frac{p-1}{2t}} p^{\frac{(1-2i)}{2}}. \tag{3.8}$$

Demonstração: Visto que $\mathfrak{p}_K$ se ramifica completamente em L, então

$$\mathfrak{p}_K^i \mathcal{O}_L = \mathfrak{p}^{ti}.$$

Pelo Lema 3.3.5, se $x \in \mathfrak{p}_K^i$, $i = 1, ..., (p-1)/2$, então $Tr_{L/\mathbb{Q}}(x\overline{x}) \geq 2pti$, que implica

$$Tr_{K/\mathbb{Q}}(x\overline{x}) = \frac{1}{t} Tr_{L/\mathbb{Q}}(x\overline{x}) \geq \frac{1}{t} 2pti = 2pi. \tag{3.9}$$

Assim, o raio de empacotamento satisfaz

$$\rho \geq \frac{\sqrt{c_K.2pi}}{2},$$

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

Pelo Corolário 2.1.18, o discriminante de K é

$$\mathfrak{D}_K = \pm p^{\frac{p-1}{t}-1},$$

e a norma de $\mathfrak{p}_K^i$ é p^i.

Assim, a densidade de centro satisfaz

$$\delta(\mathfrak{p}_K^i) \geq \frac{2^{r_2} \cdot (\sqrt{c_K.2pi}/2)^{\frac{p-1}{t}}}{p^{\frac{p-1-t}{2t}} \cdot p^i} = \left(\tfrac{i}{2}\right)^{\frac{p-1}{2t}} p^{\frac{(1-2i)}{2}}. \ \square$$

Quando p e t são fixados, verifica-se que tomando $i = \frac{p-1}{2t\ln p}$ a função atinge seu máximo. Assim., o limitante inferior na expressão 3.8 é maximizado para i igual a um dos inteiros mais próximos de $\frac{p-1}{2t\ln p}$. Isso pode ser verificado no gráfico da figura 3.1, onde está representado o gráfico de $\delta(\sigma(\mathfrak{p}_K^i))$ em função de i, para $p = 31$. Observe que o máximo ocorre no inteiro mais próximo de $\frac{30}{2\ln 31}$, que é 4.

Dado $n \in \mathbb{N} - \{0\}$, existem infinitos primos p tais que $p \equiv 1 \pmod{n}$. Sejam

$$p_n = \min\{p \mid p \text{ é primo e } p \equiv 1 (\mathrm{mod}\, n)\}$$

e i_0 o inteiro mais próximo de $\frac{p-1}{2t\ln p}$, onde $t = \dfrac{p_n - 1}{n}$.

Denotaremos por $\mathcal{A}_n$ a representação geométrica do ideal $\mathfrak{p}_K^{i_0} = \mathfrak{p}^{i_0} \cap K \subseteq \mathcal{O}_K$, onde K é o subcorpo de $\mathbb{Q}(\zeta_{p_n})$ de grau n.

As Tabelas 3-1 e 3-2 mostram o logaritmo na base 2 da densidade de centro e o ganho fundamental de codificação

$$\gamma_n = \frac{d_{\min}^2}{vol(\mathcal{A}_n)^{2/n}},$$

dos reticulados $\mathcal{A}_n$.

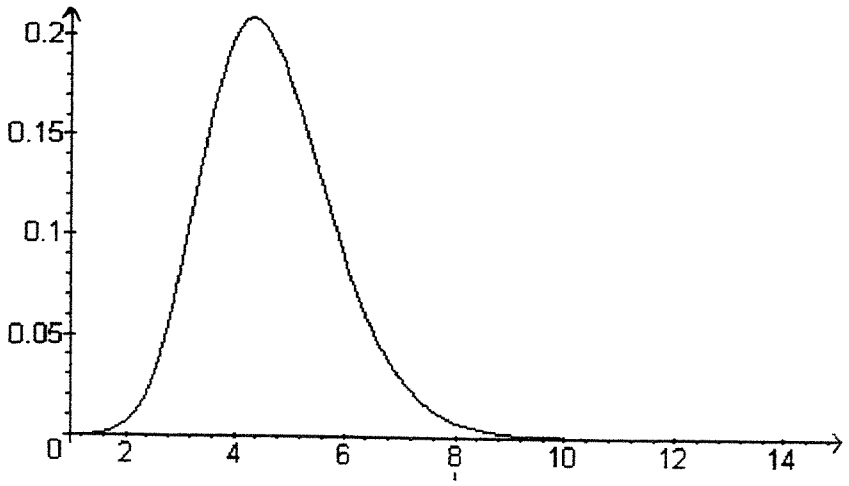


Figure 3-1: Densidade de centro de $\sigma(\mathfrak{p}_K^i)$, $p = 31$

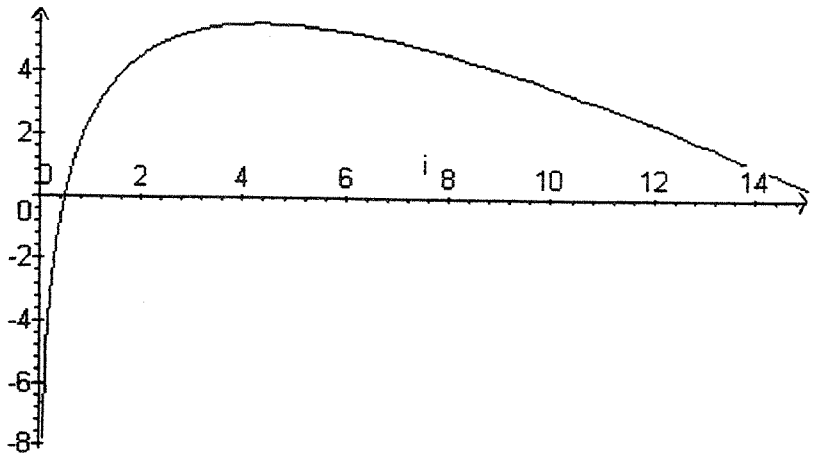


Figure 3-2: Ganho fundamental γ (dB) de $\sigma(\mathfrak{p}_K^i)$, $p = 31$

n	p	$\log_2 \delta$	γ_n		n	p	$\log_2 \delta$	γ_n
2	3	-1.792	0.624		15	31	-7.432	3.038
3	7	-2.903	0.193		16	17	-5.539	3.936
4	5	-3.161	1.263		17	103	-10.029	2.468
5	11	-4.229	0.927		18	19	-5.355	4.229
6	7	-4.211	1.795		19	191	-11.366	2.419
7	29	-5.929	0.921		20	41	-7.544	3.749
8	17	-6.044	1.472		21	43	-7.423	3.892
9	19	-6.372	1.758		22	23	-4.832	4.698
10	11	-5.189	2.896		23	47	-7.159	4.146
11	23	-6.785	2.307		24	73	-8.455	3.899
12	13	-5.551	3.236		25	101	-9.333	3.772
13	53	-8.591	2.041		26	53	-6.715	4.465
14	29	-7.287	2.887		27	109	-9.023	4.008

Tabela 3-1 Densidade de centro e ganho fundamental de $\mathcal{A}_n$

n	p	$\log_2 \delta$	γ_n		n	p	$\log_2 \delta$	γ_n
496	1489	660.59	14.039		509	1019	706.56	14.378
497	6959	595.10	13.229		510	1021	708.56	14.385
498	499	722.12	14.751		511	3067	657.14	13.763
499	1997	652.76	13.896		512	7681	619.79	13.309
500	3001	636.23	13.681		513	2053	679.81	14.001
501	5011	616.13	13.424		514	1543	695.81	14.170
502	503	730.31	14.779		515	1031	718.57	14.421
503	3019	641.90	13.704		516	1033	720.58	14.428
504	1009	696.57	14.342		517	2069	687.62	14.028
505	5051	623.57	13.454		518	2591	678.97	13.912
506	1013	700.56	14.356		519	1039	726.59	14.449
507	2029	668.19	13.955		520	521	767.46	14.906
508	509	742.66	14.822		521	16673	606.48	13.029

Tabela 3-2 Densidade de centro e ganho fundamental de $\mathcal{A}_n$

Em [18], são obtidos reticulados via códigos ternários e quaternários ótimos. É apresentada respectiva tabela de densidade de centro, para dimensões pares $n \leq 100$ ([18], pp. 244). A família $\mathcal{A}_n$ apresenta ganho sobre estes reticulados para as dimensões $n = 78$, 82, 88, 96 e 100.

Note que nas dimensões onde não há na literatura citação de reticulados densos conhecidos, a família $\mathcal{A}_n$ contribui com valores bastante próximos e, algumas vezes, maiores que os valores conhecidos.

Por exemplo, nas dimensões 506, 509 e 510, a família contribui com o mais denso reticulado conhecido, superando inclusive a densidade do reticulado em dimensão 512 citado em [27], pp. 16, Tabela 1.3.

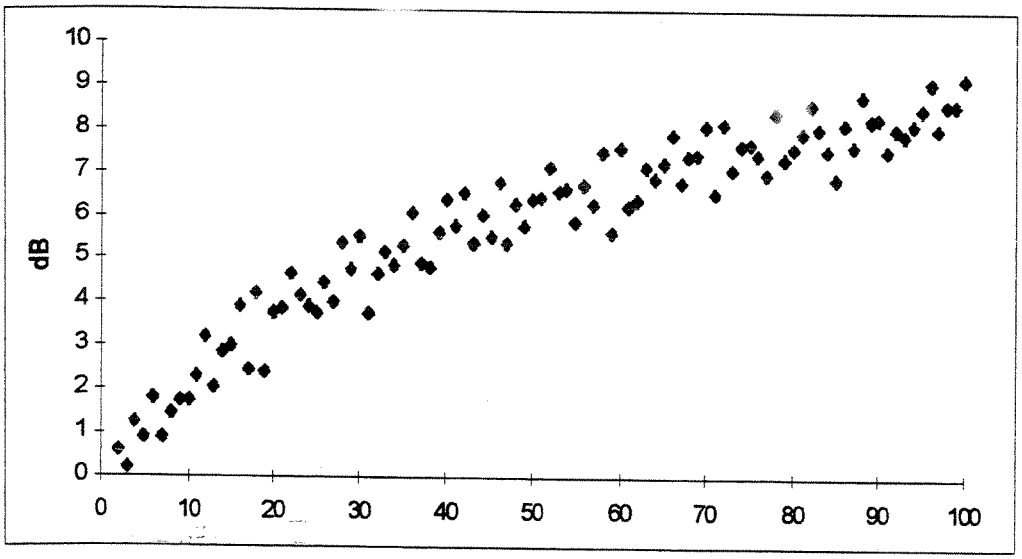


Figure 3-3: Ganho de $\mathcal{A}_n$ (dB)

Na figura 3-4, as densidades máximas conhecidas estão representados pela sequência 2.

Observação: Cálculos computacionais indicam que o ganho fundamental da família $\mathcal{A}_n$ cresce indefinidamente, ou seja,

$$\gamma_n \to \infty, \text{ com } p \to \infty.$$

Para dimensões altas, esta família apresenta ainda um bom desempenho, satisfazendo

$$\tfrac{1}{n}\log_2(\Delta) \geq -\tfrac{1}{2}\log_2\log_2 n,$$

onde Δ é a densidade de empacotamento esférico.

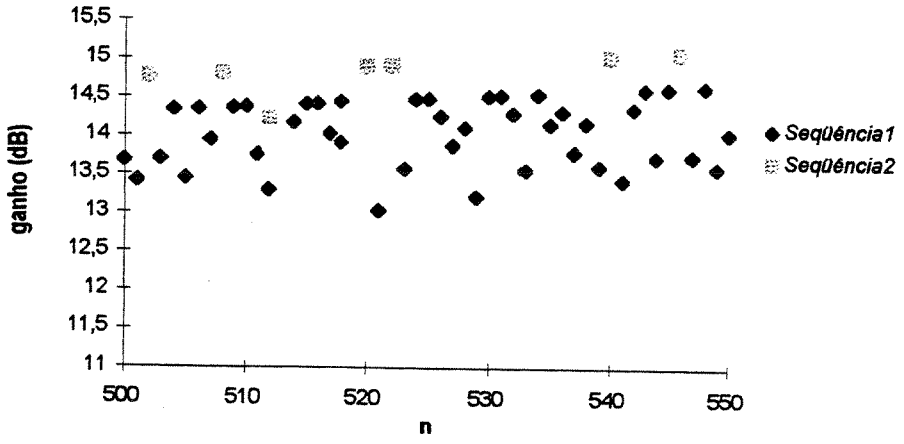


Figure 3-4: Ganho de $\mathcal{A}_n$ (dB)

3.4 Cúbicas Reais Contidas em $\mathbb{Q}(\zeta_p)$

Nesta seção, estudaremos extensões cúbicas reais contidas em $\mathbb{Q}(\zeta_p)$, p primo, bem como propriedades de suas realizações geométricas.

Dado um número primo p, $p \equiv 1 (\mathrm{mod}\, 3)$, existe uma única extensão cúbica K contida em $\mathbb{Q}(\zeta_p)$. Tal extensão é da forma

$$K = \mathbb{Q}(\alpha),$$

onde

$$\alpha = Tr_{\mathbb{Q}(\zeta_p)/K}(\zeta_p)\ .$$

Seja $\mathcal{O}_K$ o anel dos inteiros de K. Aqui, desenvolvemos um método aritmético para calcular o índice $k = [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ e discutimos a representação geométrica de $\mathbb{Z}[\alpha]$ em $\mathbb{R}^3$. Também determinamos um limitante superior para k, usando para isso propriedades de empacotamento esférico.

3.4.1 Propriedades aritméticas

Uma lista é uma sequência não ordenada de elementos em um anel A, onde admite-se repetição de elementos; denotamos por $L = [x_1, ..., x_r]$. Dado $y \in A$, definimos o produto yL como sendo a lista $[yx_1, ..., yx_r]$. O conceito de sublistas e união de listas é intuitivo. Dado $a \in \mathbb{N}$, define-se o produto $a * L$ como a lista formada pela união $L \cup \cdots \cup L$, a vezes.

Sejam p um número primo satisfazendo $p \equiv 1 (\mathrm{mod}\, 3)$ e H o subgrupo de índice 3 em $(\mathbb{Z}/p\mathbb{Z})^*$.

Consideremos as listas com elementos em $\mathbb{Z}/p\mathbb{Z}$,

$$S = [1 + x \ ; \ x \in H, \ x \neq 1]$$

e

$$L_H = [x + y; \ x, y \in H \ e \ x \neq y] = [(1 + x).y, \ x \in H - \{1\} \ e \ y \in H].$$

Seja l um gerador de $(\mathbb{Z}/p\mathbb{Z})^*/H$. Se $1 + h \in S \cap l^i H$, então $(1 + h)h^{-1} = 1 + h^{-1} \in S \cap l^i H$. Logo, se $h \neq \pm 1$, então $1+h$ e $1+h^{-1}$ são distintos. Portanto, $card(S \cap l^i H) = 2n_i$, $i = 0, 1, 2$, e assim $card(S) = 2(n_0 + n_1 + n_2) + 1$. Temos assim

$$L_H = 2n_0 * [H] \cup 2n_1 * [lH] \cup 2n_2 * [l^2 H] \cup T,$$

onde $T = [0, ..., 0]$ tem comprimento $card(H)$.

Dada uma lista L com elementos em $(\mathbb{Z}/p\mathbb{Z})^*$, indicamos

$$\zeta_p^L = \sum_{x \in L} \zeta_p^x \ .$$

Assim, se $2 \in l^i H$, podemos escrever

$$\alpha^2 = \sum_{x\in H} \zeta_p^{2x} + \sum_{\substack{x,y\in H \\ x\neq y}} \zeta_p^{x+y} = \zeta_p^{2[H]} + \zeta_p^{L_H}$$

$$= \zeta_p^{2[H]} + 2n_0.\zeta_p^{[H]} + 2n_1.\zeta_p^{[lH]} + 2n_2.\zeta_p^{[l^2H]} + \zeta_p^T \tag{3.10}$$

Teorema 3.4.1 *Com a notação acima, vale*

$$[\mathcal{O}_K : \mathbb{Z}[\alpha]] = \mid 2(n_1 - n_2) + \delta \mid,$$

onde

$$\delta = \begin{cases} 0\ , & \text{se } 2 \in H; \\ 1\ , & \text{se } 2 \in lH; \\ -1\ , & \text{se } 2 \in l^2H. \end{cases}$$

Demonstração: Reescrendo a equação em (3.10) usando a notação $\alpha = \zeta_p^H$, temos

$$\alpha^2 = \alpha^{\sigma^i} + 2n_0.\alpha + 2n_1.\alpha^\sigma + 2n_2.\alpha^{\sigma^2} + c,$$

onde $c = \zeta_p^T = card(H)$. Como

$$\alpha + \alpha^\sigma + \alpha^{\sigma^2} = -1,$$

pondo

$$\alpha^{\sigma^i} = \delta_{i,0}\alpha + \delta_{i,1}\alpha^\sigma + \delta_{i,2}\alpha^{\sigma^2},$$

onde

$$\delta_{i,j} = \begin{cases} 1, & \text{se } i = j; \\ 0, & \text{se } i \neq j \end{cases},$$

temos

$$\alpha^2 = (2n_0 - c + \delta_{i,0})\alpha + (2n_1 - c + \delta_{i,1})\alpha^\sigma + (2n_2 - c + \delta_{i,2})\alpha^{\sigma^2}.$$

Mas

$$\mathcal{O}_K = \mathbb{Z}\alpha + \mathbb{Z}\alpha^\sigma + \mathbb{Z}\alpha^{\sigma^2}$$

e $\{1, \alpha, \alpha^2\}$ é $\mathbb{Z}$-base para $\mathbb{Z}[\alpha]$. Assim,

$$\begin{array}{rccc} 1 = & -1.\alpha & -1.\alpha^\sigma & -1.\alpha^{\sigma^2} \\ \alpha = & 1.\alpha & 0.\alpha^\sigma & 0.\alpha^{\sigma^2} \\ \alpha^2 = & (2n_0 - c + \delta_{i,0}).\alpha & (2n_1 - c + \delta_{i,1})\alpha^\sigma & (2n_2 - c + \delta_{i,2}).\alpha^{\sigma^2} \end{array}$$

e portanto

$$[\mathcal{O}_K : \mathbb{Z}[\alpha]] = \left| \begin{bmatrix} -1 & -1 & -1 \\ 1 & 0 & 0 \\ 2n_0 - c + \delta_{i,0} & 2n_1 - c + \delta_{i,1} & 2n_2 - c + \delta_{i,2} \end{bmatrix} \right|$$

$$= \mid 2(n_1 - n_2) + \delta_{i,1} - \delta_{i,2} \mid .$$

Temos as seguintes equivalências:

$$2 \in H \Leftrightarrow i = 0 \Leftrightarrow \delta_{i,1} - \delta_{i,2} = 0$$

$$2 \in lH \Leftrightarrow i = 1 \Leftrightarrow \delta_{i,1} - \delta_{i,2} = 1$$

$$2 \in l^2H \Leftrightarrow i = 2 \Leftrightarrow \delta_{i,1} - \delta_{i,2} = -1$$

Logo,

$$[\mathcal{O}_K : \mathbb{Z}[\alpha]] = \mid 2(n_1 - n_2) + \delta \mid,$$

onde δ é como no enunciado. □

Cálculos computacionais simples fornecem os valores n_0, n_1, n_2 e k, dado um primo $p \equiv 1 (\mathrm{mod}\, 3)$:

p	l	$2 \in$:	n_0	n_1	n_2	k
7	3	H	1	0	0	1
13	2	lH	0	0	1	1
19	2	lH	1	0	1	1
31	3	H	1	2	1	2
37	2	lH	1	2	2	1
43	3	H	1	3	2	2
61	2	lH	3	2	4	3
67	2	lH	3	4	3	3
73	5	l^2H	4	3	4	3
79	3	lH	3	4	5	1
97	5	lH	6	4	5	1

Tabela 1: $p \leq 100$

Para $100 \leq p \leq 500$, os números primos p tais que $k = 1$ são 139, 163, 313 e 349.

A referência [9] traz o seguinte resultado:

Teorema 3.4.2 *([9], pp.32) O ideal $2\mathcal{O}_K$ decompõe-se completamente em K se, e somente se, k é par.*

Com os resultados aqui obtidos, completamos o Teorema 3.4.2 com o seguinte

Teorema 3.4.3 *O ideal* $2\mathcal{O}_K$ *decompõe-se completamente em* K *se, e somente se* $2 \in H$.

3.4.2 Representação geométrica

Sejam α_0, α_1 e α_2 elementos de $\mathcal{O}_K$, e suponhamos que o $\mathbb{Z}$-módulo M gerado por estes elementos tenha posto 3. Seja $\{\sigma_1, \sigma_2, \sigma_3\}$ o grupo de Galois de K sobre $\mathbb{Q}$ e $\sigma : M \longrightarrow \mathbb{R}^3$ o homomorfismo de Minkowiski $\sigma : \mathcal{O}_K \longrightarrow \mathbb{R}^3$ restrito a M,

$$\sigma(x) = (\sigma_1(x), \sigma_2(x), \sigma_3(x)) \ .$$

Considere a $\mathbb{Z}$-base $\{\alpha, \alpha^\sigma, \alpha^{\sigma^2}\}$ para $\mathcal{O}_K$. Da expressão

$$(\alpha + \alpha^\sigma + \alpha^{\sigma^2})^2 = \alpha^2 + (\alpha^\sigma)^2 + (\alpha^{\sigma^2})^2 + (\alpha\alpha^\sigma + \alpha\alpha^{\sigma^2} + \alpha^\sigma\alpha^{\sigma^2}),$$

obtemos,

$$Tr_{K/\mathbb{Q}}(\alpha^2) = ((\alpha)^2 + (\alpha^\sigma)^2 + (\alpha^{\sigma^2})^2) = 1 - 2(\alpha\alpha^\sigma + \alpha\alpha^{\sigma^2} + \alpha^\sigma\alpha_p^{\sigma^2}).$$

Por outro lado,

$$\alpha^2 = \zeta_p^{2[H]} + 2(n_0\zeta^{[H]} + n_1\zeta^{l[H]} + n_2\zeta^{l^2[H]}) + \frac{p-1}{3},$$

resultando em

$$Tr_{K/\mathbb{Q}}(\alpha^2) = -2 - 2(n_0 + n_1 + n_2) + p = \frac{2p+1}{3} \ .$$

Substituindo, temos

$$\alpha\alpha^{\sigma} + \alpha\alpha^{\sigma^2} + \alpha^{\sigma}\alpha^{\sigma^2} = -\frac{p-1}{3}.$$

Seja $x = a_0\alpha + a_1\alpha^{\sigma} + a_2\alpha^{\sigma^2} \in \mathcal{O}_K$. Sendo K um corpo totalmente real, para $x \in \mathcal{O}_K$, vale

$$\begin{aligned} \mid \sigma(x) \mid^2 &= Tr_{K/\mathbb{Q}}(x^2) \\ &= \left(Tr_{K/\mathbb{Q}}(\alpha)\right)^2 . \left(\sum_{i=0}^{2} a_i^2\right) - \left(\sum_{i<j} \alpha_i\alpha_j\right)\left(\sum_{i<j}(a_i - a_j)^2\right) \\ &= (a_0^2 + a_1^2 + a_2^2) + \frac{p-1}{3}\left((a_0 - a_1)^2 + (a_0 - a_2)^2 + (a_1 - a_2)^2\right). \end{aligned}$$

Para $a_0 = a_1 = a_2 = 1$, temos $\mid \sigma(x) \mid^2 = 3$, e uma simples verificação mostra que este é o menor valor possível para a forma quadrática.

Para o cálculo da densidade de centro, precisamos conhecer o discriminante $\mathfrak{D}_K$ do corpo K . Usando o Corolário 2.1.18, obtemos

$$\mid \mathfrak{D}_K \mid = p^2.$$

Finalmente, obtem-se a expressão para a densidade de centro do anel $\mathcal{O}_K$:

$$\delta(\sigma(\mathcal{O}_K)) = \frac{\left(\frac{\sqrt{3}}{2}\right)^3}{p} = \frac{3\sqrt{3}}{8p}.$$

Proposição 3.4.4 *O submódulo $\mathbb{Z}[\alpha]$ tem densidade de centro*

$$\delta(\sigma(\mathbb{Z}[\alpha])) = k^2.\delta(\sigma(\mathcal{O}_K))$$

Demonstração: O menor valor assumido pela forma quadrática em $\mathbb{Z}[\alpha]$ é atingido em $\pm(k,k,k)$, com respectivo valor $3k^2$. A densidade de centro é

$$\delta(\sigma(\mathbb{Z}[\alpha])) = \frac{(\rho)^3}{v(\mathbb{Z}[\alpha])} = \frac{3\sqrt{3}k^3}{8pk} = k^2.\delta(\sigma(\mathcal{O}_K)). \ \square$$

O resultado acima nos dá um limitante superior para k, através da densidade de centro máxima em dimensão 3,

$$\delta(\sigma(\mathbb{Z}[\alpha])) = \frac{3\sqrt{3}k^2}{8p} \leq 0.125 = \delta(\Lambda_3),$$

e daí

$$k \leq 0.4387\sqrt{p}.$$

Este limitante está relativamente próximo ao limitante obtido em [9], pp. 32, onde se obteve

$$k \leq (4p/27)^{1/2} \simeq 0.385\sqrt{p},$$

utilizando-se para isso técnicas sofisticadas.

Do último limitante, temos então

$$\delta(\sigma(\mathbb{Z}[\alpha])) = \frac{3\sqrt{3}k^2}{8p} \leq \frac{\sqrt{3}}{18} = 0.096225.$$

3.5 Subcorpos de $\mathbb{Q}(\zeta_{pq})$

Em [4] são construídas versões rotacionadas dos reticulados já conhecidos D_4, K_{12} e Λ_{16} através de ideais de $\mathbb{Q}(\zeta_n)$, para $n = 8$, 21 e 40, respectivamente. Ainda no mesmo trabalho, são utilizadas as construções de Craig, ([7] e [8]), onde são construídos E_6, E_8 e Λ_{24} através de $\mathbb{Q}(\zeta_n)$, para $n = 9$, 20 e 39, respectivamente. As constelações obtidas apresentam bom desempenho para os canais Rayleigh com desvanecimento e gaussiano.

Nesta seção, voltamos nossa atenção para a construção de reticulados a partir de subcorpos de $\mathbb{Q}(\zeta_{pq})$. Desenvolvemos um método que facilita a determinação da distância

mínima nos reticulados $\sigma(\mathfrak{a})$, onde $\mathfrak{a}$ é um ideal de $\mathbb{Z}[\zeta_{pq}]$. O procedimento permitiu obter diversas versões rotacionadas de reticulados apresentando a mesma densidade de centro de E_8, via ideais convenientes em subcorpos de $\mathbb{Q}(\zeta_{pq})$.

3.5.1 A forma quadrática associada a $\mathbb{Q}(\zeta_{pq})$

Ao contrário do que ocorre em $\mathbb{Q}(\zeta_p)$, veremos que a forma quadrática em $\mathbb{Q}(\zeta_{pq})$, p e q primos, não é simétrica.

Lema 3.5.1 *Dados os números primos p e q, temos:*

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

Demonstração: Sejam i, com $(i,pq) = 1$ e u, v inteiros tais que $pu + qv = 1$. Temos

$$\zeta_{pq}^i = \zeta_{pq}^{pui} \cdot \zeta_{pq}^{qvi} = \zeta_q^{ui} . \zeta_p^{vi},$$

onde $(ui, q) = (vi, p) = 1$.

Então

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^i) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_q^{ui} . \zeta_p^{vi})$$

$$= Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta pq)/\mathbb{Q}(\zeta_p)}(\zeta_q^{ui} . \zeta_p^{vi})) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^{vi} . Tr_{\mathbb{Q}(\zeta pq)/\mathbb{Q}(\zeta_p)}(\zeta_q^{ui}))$$

$$= Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^{vi} . Tr_{\mathbb{Q}(\zeta q)/\mathbb{Q}}(\zeta_q^{ui})) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(-\zeta_p^{vi}) = 1.$$

Suponhamos agora $(i,pq) = p$. Então existe $k \in \mathbb{Z}$, com $(k,q) = 1$ tal que $\zeta_{pq}^i = \zeta_q^k$. Logo,

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

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

Para os demais itens, a prova é análoga. □

Corolário 3.5.2 *Para* $0 \leq i \leq pq$, *vale:*

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

Demonstração: No caso $(i, pq) = 1$, 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.

Para $i = 0$, aplicando o Lema 3.5.1, temos:

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

Os demais casos seguem de forma análoga. □

Proposição 3.5.3 *Sejam* p, q *primos,* $m = \phi(pq) = (p-1)(q-1)$ *e* $x = a_0 + a_1\zeta_{pq} + \cdots + a_{m-1}\zeta_{pq}^{m-1}$, $a_i \in \mathbb{Z}$, *um elemento de* $\mathbb{Z}[\zeta_{pq}]$. *Então*

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(x\overline{x}) = (p-1)(q-1)\sum_{i=0}^{m-1} a_i^2 + 2.\sum_{i<j} a_i a_j - 2pC_p - 2qC_q,$$

onde

$$C_i = a_0a_i + a_1a_{i+1} + \cdots + a_{m-1-i}a_{m-1}.$$

Demonstração: Para x como no enunciado acima, vale

$$x\overline{x} = \sum_{i=0}^{m-1} a_i^2 + \sum_{i=1}^{m-1} C_i\alpha_i,$$

onde

$$\alpha_i = \zeta_{pq}^i + \zeta_{pq}^{-i}.$$

Escrevendo

$$x\overline{x} = \sum_{i=0}^{m-1} a_i^2 + \sum_{(i,pq)=1} C_i\alpha_i + \sum_{(i,p)=p} C_i\alpha_i + \sum_{(i,q)=q} C_i\alpha_i \ ;$$

temos

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(x\overline{x}) = (p-1)(q-1)\sum_{i=0}^{m-1} a_i^2 + \sum_{(i,pq)=1} C_iTr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\alpha_i) +$$

$$+ \sum_{(i,p)=p} C_iTr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\alpha_i) + \sum_{(i,q)=q} C_iTr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\alpha_i).$$

Aplicando o Lema anterior, uma simples verificação conclui a demonstração. □

3.5.2 A forma quadrática em subcorpos de $\mathbb{Q}(\zeta_{pq})$

Sejam $K \subseteq L$ corpos de números com $t = [L : K]$, σ_K, σ_L os homomorfismos canônicos de K e L, respectivamente, $x \in K$ e c_K, c_L assumindo os valores no conjunto $\{1/2, 1\}$, conforme o corpo em questão seja real ou complexo. Então

$$| \sigma_L(x) |^2 = c_L Tr_{L/\mathbb{Q}}(x\overline{x}) = tc_L Tr_{K/\mathbb{Q}}(x\overline{x}),$$

o que implica em

$$| \sigma_K(x) |^2 = \frac{c_K}{tc_L} | \sigma_L(x) |^2 .$$

Sejam K um subcorpo de $\mathbb{Q}(\zeta_p)$ de índice t e H o grupo dos K-automorfismos de $\mathbb{Q}(\zeta_p)$. Então $K = \mathbb{Q}(\alpha)$, onde $\alpha = \sum_{\sigma \in H} \sigma(\zeta_p)$.

Observando a simetria de Q, pondo $u = (p-1)/t$ temos:

$$| \sigma_K(x) |^2 = Tr_{K/\mathbb{Q}}(x\overline{x}) = \frac{1}{t} Tr_{L/\mathbb{Q}}(x\overline{x}) = \frac{1}{2t} Q_{p-1}(a_0, ..., a_0, ..., a_u, ..., a_u),$$

onde cada a_i aparece repetido t vezes. Assim chega-se à expressão:

$$| \sigma_K(x) |^2 = \frac{1}{2} \left((a_1^2 + \cdots + a_u^2) + t \sum_{i<j} (a_i - a_j)^2 \right).$$

Sejam $K_1 \subset \mathbb{Q}(\zeta_p)$, $K_2 \subset \mathbb{Q}(\zeta_q)$ e $\{\alpha_1, ..., \alpha_u\}$, $\{\beta_1, ..., \beta_v\}$ bases integrais para $\mathcal{O}_{K_1}$ e $\mathcal{O}_{K_2}$, respectivamente e

$$x = \sum_{j=1}^{v} \sum_{i=1}^{u} a_{ij} \alpha_i \beta_j = \sum_{j=1}^{v} x_j \beta_j \in K_1 K_2,$$

onde

$$x_j = \sum_{i=1}^{u} a_{ij}\alpha_i.$$

Sejam Q' e Q'' as formas quadráticas associadas a K_1 e K_2, respectivamente. Então

$$Tr_{K_1K_2/\mathbb{Q}}(x\overline{x}) = Q''(Q'(x_1), Q'(x_2), ..., Q'(x_v)). \tag{3.11}$$

3.5.3 Decomposição em $\mathbb{Q}(\zeta_{pq})$

Sejam $L = \mathbb{Q}(\zeta_{pq})$ e $\mathfrak{q}$ um ideal primo de $\mathcal{O}_L$ acima de $q\mathbb{Z}$. Conforme vimos na seção 2.2, seu grupo de decomposição depende apenas de q. Sendo assim, dado um subcorpo K de L, denotaremos o grupo de decomposição de um ideal primo de $\mathcal{O}_L$ acima de q por $\mathcal{D}_K(q)$.

Quando a conjugação complexa não pertence ao grupo de decomposição $\mathcal{D}_L(q)$, então existe um ideal $\mathfrak{I}$ de $\mathcal{O}_L$ tal que a fatoração de $q\mathcal{O}_L$ em ideais tem a forma

$$q\mathcal{O}_L = (\mathfrak{I}\overline{\mathfrak{I}})^{q-1}. \tag{3.12}$$

Tal propriedade terá consequências que serão estudadas a seguir. Antes disto, daremos a seguinte caracterização:

Teorema 3.5.4 *Com a notação acima, vale:*

$$\theta \in \mathcal{D}_L(q) \Leftrightarrow \theta \in \mathcal{D}_K(q),$$

onde θ é a conjugação complexa.

Demonstração: Seja $\sigma_s \in \mathcal{D}_K(q)$ definido por

$$\sigma_s(\zeta_p) = \zeta_p^s.$$

Para cada $\sigma_s \in \mathcal{D}_K(q)$, existem $q-1$ extensões $\sigma_{s,i}$ de $\mathcal{D}_L(q)$. Cada $\sigma_{s,i}$ é definido por seu valor em ζ_{pq} . Sejam u e v tais que $1 = pu + qv$.

Segue que

$$\sigma_{s,i}(\zeta_{pq}) = \sigma_{s,i}(\zeta_{pq}^{pu+qv}) = \sigma_{s,i}(\zeta_{pq}^{pu})\sigma_{s,i}(\zeta_{pq}^{qv}) =$$

$$= \sigma_{s,i}(\zeta_q^u).\sigma_{s,i}(\zeta_p^v) = \zeta_q^{ui}.\zeta_p^{sv} = \zeta_{pq}^{pui+qsv} .$$

Assim, $\theta \in \mathcal{D}_L(q)$ se, e somente se, existem i, s tais que

$$pui + qsv \equiv -1 \ (mod pq),$$

que equivale a

$$\begin{cases} pui + qsv \equiv -1 (mod p) \\ \text{e} \\ pui + qsv \equiv -1 (mod q). \end{cases}$$

A segunda condição vale sempre, já que i pode assumir qualquer valor não nulo módulo q. Quanto à primeira, esta equivale a $\theta \in \mathcal{D}_K(p)$, o que conclui a prova. □

Corolário 3.5.5 *Com a notação acima, vale*

$$\theta \in \mathcal{D}_L(q) \Leftrightarrow Ord_p(q) \equiv 0 \ (mod\ 2), \tag{3.13}$$

onde $Ord_m(n)$ *é a ordem de* n *módulo* m, *quando* $(m,n) = 1$.

Demonstração: Lembrando que $card(\mathcal{D}_K(q)) = Ord_p(q)$, temos que se $\theta \in \mathcal{D}_K(q)$, então

$$2 \mid card(\mathcal{D}_K(q)) = Ord_p(q).$$

Para a recíproca, suponhamos que $O_p(q) \equiv 0\ (mod 2)$. Como $\mathcal{D}_K(q)$ é cíclico de ordem par, segue que $\{-1, 1\}$ é o único subgrupo de ordem 2 destes grupos. □

Quando p e q satisfazem às condições

$$Ord_p(q) \equiv Ord_q(p) \equiv 1\ (mod\ 2), \tag{3.14}$$

então existem em $\mathbb{Z}[\zeta_{pq}]$ as decomposições em ideais primos

$$p\mathcal{O}_L = (\mathfrak{p}_1 ... \mathfrak{p}_r \overline{\mathfrak{p}_1 ... \mathfrak{p}_r})^{p-1},\ q\mathcal{O}_L = (\mathfrak{q}_1 ... \mathfrak{q}_s \overline{\mathfrak{q}_1 ... \mathfrak{q}_s})^{q-1} \tag{3.15}$$

Teremos particular interesse no ideal

$$\mathfrak{I} = \mathfrak{p}_1 ... \mathfrak{p}_r \mathfrak{q}_1 ... \mathfrak{q}_s. \tag{3.16}$$

3.5.4 Construções algébricas

Construção A - dimensão 24:

Aqui, daremos um tratamento diferenciado para a obtenção do reticulado Λ_{24}, mais simples que o de [7]. Aqui, fazemos uma nova prova para essa construção.

Em $\mathbb{Z}[\zeta_{39}]$ existem 4 ideais primos acima de 3 e dois ideais primos acima de 13, e as decomposições em ideais primos serão, conforme Exemplo 2.2.7,

$$3\mathbb{Z}[\zeta_{39}] = (\mathfrak{p}_1 \mathfrak{p}_2 \overline{\mathfrak{p}_1 \mathfrak{p}_2})^2 \text{ e } 13\mathbb{Z}(\zeta_{39}) = (\mathfrak{q}\overline{\mathfrak{q}})^6.$$

Proposição 3.5.6 *Considerando a decomposição acima, seja o ideal* $\mathfrak{I} = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{q}$ *em* $\mathbb{Z}[\zeta_{39}]$. *Para* $x \in \mathfrak{I}$, *vale*

$$Tr_{\mathbb{Q}(\zeta_{39})/\mathbb{Q}}(x\overline{x}) \geq 4.39.$$

Demonstração: Seja $x \in \mathfrak{I}$, e $x_0, x_1 \in \mathbb{Z}[\zeta_{13}]$ tais que $x = x_0 + x_1\zeta_3$. Sabemos que $Tr_{\mathbb{Q}(\zeta_{39})/\mathbb{Q}}(x\overline{x})$, $x \in \mathfrak{I}$ é par e múltiplo de 39 . Mostraremos que o valor 2.39 não é assumido.

Podemos escrever

$$Tr_{\mathbb{Q}(\zeta_{39})/\mathbb{Q}}(x\overline{x}) = Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(x_0\overline{x_0}) + Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(x_1\overline{x_1}) + Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}((x_0 - x_1)\overline{(x_0 - x_1)})$$

Para que o valor 2.39 seja atingido, as únicas possibilidades são, a menos de ordem,

$$Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(x_0\overline{x_0}) = 12,\ Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(x_1\overline{x_1}) = 30$$

e

$$Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}((x_0 - x_1)\overline{(x_0 - x_1)}) = 36.$$

As possibilidades para x_0 são as potências

$$x_0 = \pm\zeta_{13}^{i_0},\ i_0 = 0, ..., 12.$$

Para x_1, os valores possíveis são:

$$x_1 = \pm(\zeta_{13}^{i_1} + \zeta_{13}^{i_2} + \zeta_{13}^{i_3}).$$

onde os $i_{r's}$ são dois a dois distintos.

Seja

$$x_0 = -\zeta_{13}^{i_0} \text{ e } x_1 = \zeta_{13}^{i_1} + \zeta_{13}^{i_2} + \zeta_{13}^{i_3}.$$

Supondo $i_0 \neq i_k$, $k = 1, 2, 3$, então $Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}((x_0 - x_1)\overline{(x_0 - x_1)}) = 36$.

Se $x \in \mathfrak{I}$, então

$$Tr_{\mathbb{Q}(\zeta_{39})/\mathbb{Q}(\zeta_{13})}(x\overline{x}) = 3(x_0\overline{x_0} + x_1\overline{x_1}) - (x_0 + x_1)\overline{(x_0 + x_1)} \in 3\mathbb{Z}[\zeta_{13}],$$

e portanto

$$(x_0 + x_1)\overline{(x_0 + x_1)} \equiv 0 \ (mod\ 3\mathbb{Z}[\zeta_{13}]).$$

Seja $\gamma : \mathbb{Z}[\zeta_{13}] \to \mathbb{Z}$ o homomorfismo de anéis definido por $\gamma(\sum_{i=0}^{11} a_i\zeta_{13}^i) = \sum_{i=0}^{11} a_i$. Como $(x_0 + x_1)\overline{(x_0 + x_1)} \in 3\mathbb{Z}[\zeta_{13}]$, então $\gamma((x_0 + x_1)\overline{(x_0 + x_1)}) \equiv 0 (\mathrm{mod}\, 3)$.

Reescrevendo, temos

$$(x_0 + x_1)\overline{(x_0 + x_1)} =$$

$$(-\zeta_{13}^{i_0} + \zeta_{13}^{i_1} + \zeta_{13}^{i_2} + \zeta_{13}^{i_3})(-\zeta_{13}^{-i_0} + \zeta_{13}^{-i_1} + \zeta_{13}^{-i_2} + \zeta_{13}^{-i_3}) =$$

$$4 - A + B \equiv 0 \ (mod\ 3\mathbb{Z}[\zeta_{13}]),$$

onde

$$A = \sum_{s=1}^{3} (\zeta_{13}^{i_0 - i_s} + \zeta_{13}^{i_s - i_0}) \text{ e } B = \sum_{r,s=1}^{3} \zeta_{13}^{i_r - i_s}.$$

Sejam n_A (resp. n_B) o número de expoentes tais que $i_0 - i_s = -1$ ou $i_s - i_0 = -1$ (resp. $i_r - i_s = -1$). As possibilidades para n_A são 0 ou 1, já que os $i_{j's}$ são dois a dois distintos. Já n_B pode assumir os valores $0, 1$ ou 2.

Temos $\gamma(\zeta_{13}^{-1}) = \gamma(-1 - \zeta_{13} - \cdots - \zeta_{13}^{11}) = -12 \equiv 0 \ (\mathrm{mod}\, 3)$. Assim,

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

Logo,

$$\gamma((x_0 + x_1)\overline{(x_0 + x_1)}) = 4 - (6 - n_A) + (6 - n_B) \equiv 1 + n_A - n_B \equiv 0 \ (\mathrm{mod}\, 3).$$

As únicas soluções possíveis são portanto

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

ou

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

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

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

Se existem r e s tais que $i_r - i_s = a$, então o coeficiente de ζ_{13}^a na equação acima é nulo, já que $\zeta_{13}^{-1} = -1 - \zeta_{13} - \cdots - \zeta_{13}^{11}$. Assim, ζ_{13}^a aparecerá também com coeficiente nulo na expansão de A na $\mathbb{Z}$-base $\{1, ..., \zeta_{13}^{11}\}$. Se não existem r e s tais que $i_r - i_s = a$, novamente ζ_{13}^a aparecerá com coeficiente nulo na decomposição de $(x_0 + x_1)\overline{(x_0 + x_1)}$.

Assim, a única possibilidade portanto $a = 0$ e $(x_0 + x_1)\overline{(x_0 + x_1)} = 3$. Então

$$Tr_{\mathbb{Q}(\zeta_{39})/\mathbb{Q}(\zeta_{13})}(x\overline{x}) = 3(x_0\overline{x_0} + x_1\overline{x_1}) - (x_0 + x_1)\overline{(x_0 + x_1)},$$

e neste caso temos $Tr_{\mathbb{Q}(\zeta_{39})/\mathbb{Q}}(x\overline{x}) = 90$, o que contradiz a hipótese sobre x.

O caso $n_A = 1$ e $n_B = 2$ se faz analogamente.

Construção B - dimensão 12:

A construção algébrica de K_{12} em [4] é feita via representação geométrica de um ideal primo acima de 7 em $\mathcal{O}_K$, $K = \mathbb{Q}(\zeta_{21})$. Contudo, o resultado foi obtido computacionalmente. Faremos aqui uma prova formal, baseada no seguinte resultado mais geral:

Teorema 3.5.7 *Sejam p, q primos tais que $Ord_p(q) \equiv 1 \ (mod\ 2)$ e $q > 2p - 3$. Seja ainda*

$$q.\mathbb{Z}[\zeta_{pq}] = (\mathfrak{J}\overline{\mathfrak{J}})^{q-1}$$

a decomposição de q em $\mathbb{Q}[\zeta_{pq}]$. Então para $x \in \mathfrak{I}$, vale

$$Tr_{K/\mathbb{Q}}(x\overline{x}) \geq (p-1).2q.$$

Demonstração: Sejam $x_0,...,x_{p-2} \in \mathbb{Z}[\zeta_q]$ tais que $x = \sum_{i=0}^{p-2} x_i\zeta_p^i \in \mathfrak{I}$. Manipulando algebricamente, obtemos

$$Tr_{K/\mathbb{Q}}(x\overline{x}) = \sum_{i=0}^{p-2} Q_{p-1}(x_i) + \sum_{i<j} Q_{p-1}(x_i - x_j).$$

Se $x_0 = \cdots = x_{p-2}$ então

$$x = x_0(1 + \zeta_p + \cdots + \zeta_p^{p-2}),$$

e daí $x_0 \in \mathfrak{I} \cap \mathbb{Z}[\zeta_q]$. Logo,

$$Tr_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(x_i\overline{x_i}) \geq 2q\,,\ i = 0,...,p-2,$$

portanto

$$Tr_{K/\mathbb{Q}}(x\overline{x}) = \sum_{i=0}^{p-2} Q_{p-1}(x_0) \geq (p-1)2q\ .\ \square$$

Se existirem pelo menos dois valores distintos para os $x_{j's}$, e visto que $Q_{p-1}(x_i) \geq p-1$, então a quantidade de $x_i - x_j$ não nulos é pelo menos $p-2$, e daí

$$\sum_{i<j} Q_{p-1}(x_i - x_j) \geq (p-2)(p-1).$$

Logo,

$$Tr_{K/\mathbb{Q}}(x\overline{x}) \geq (2p-3)(q-1),$$

e sendo $q > 2p-3$, então

$$Tr_{K/\mathbb{Q}}(x\overline{x}) > (p-2)2q.$$

Visto que a forma quadrática é par e múltipla de q, então também nesse caso vale

$$Tr_{K/\mathbb{Q}}(x\overline{x}) \geq (p-1)2q.$$

Para a norma de $\mathfrak{I}$ vale

$$N(\mathfrak{I}) = q^{n_1/2}.$$

Cálculos nos mostram que a densidade de centro de $\sigma(\mathfrak{I})$ vale

$$\delta(\sigma(\mathfrak{I})) \geq \frac{((p-1).2q)^{n_1 n_2/2}}{p^{n_2(n_1-1)/2}.q^{n_1(n_2-1)/2}q^{n_1/2}.2^{n_1 n_2}} = \frac{(\frac{p-1}{2})^{n_1 n_2/2}}{p^{n_2(n_1-1)/2}}. \tag{3.17}$$

Em particular, para $p = 3$, o menor primo satisfazendo às condições $q > 2p-3$ e $Ord_p(q) \equiv 1 \ (mod\ 2)$ é $q = 7$. Para estes primos, temos um reticulado $\sigma(\mathfrak{I})$ em dimensão 12, cuja densidade de centro é $\delta = \frac{1}{3^3}$, justamente a densidade de K_{12}.

Construção C - dimensão 8:

Lema 3.5.8 *Sejam L um corpo de números e K um subcorpo de L tais que $[L:K] = h$ seja ímpar. Seja ainda q um número primo e suponhamos que em $\mathcal{O}_L$ a decomposição de $q\mathcal{O}_L$ seja da forma*

$$q\mathcal{O}_L = \mathfrak{q}_1 \ldots \mathfrak{q}_{s/2}\overline{\mathfrak{q}_1 \ldots \mathfrak{q}_{s/2}},$$

para algum $s \in \mathbb{N}$.

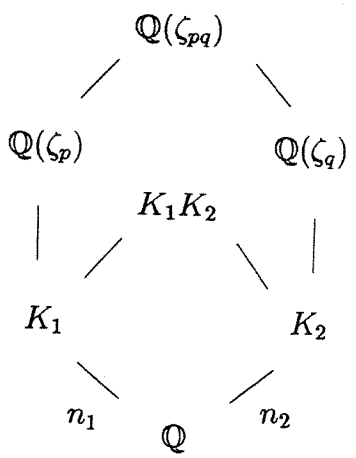
Então a decomposição de $q\mathcal{O}_K$ em ideais primos é da forma

$$q\mathcal{O}_K = \mathfrak{q}_1...\mathfrak{q}_{t/2}\overline{\mathfrak{q}_1...\mathfrak{q}_{t/2}},$$

para algum $t \in \mathbb{N}$.

Demonstração: Consideremos em $\mathcal{O}_K$ um ideal primo $\mathfrak{q}$ que divide $q\mathcal{O}_K$. Temos $\mathfrak{q}\mathcal{O}_L = \mathfrak{b}_1...\mathfrak{b}_t$, onde t divide h, ou seja, t é ímpar. Por outro lado, suponhamos $\overline{\mathfrak{q}} = \mathfrak{q}$. Então $\mathfrak{b}_1...\mathfrak{b}_t = \overline{\mathfrak{b}_1...\mathfrak{b}_t}$, e para cada ideal $\mathfrak{b}_i$, $i = 1, ..., t$, existe $j \neq i$ tal que $\overline{\mathfrak{b}_i} = \mathfrak{b}_j$, ou seja, os ideais acima de $\mathfrak{q}$ aparecem aos pares, o que contraria a hipótese sobre a paridade de t. Logo, $\overline{\mathfrak{q}} \neq \mathfrak{q}$, e portanto vale o resultado enunciado. □

Sejam p e q primos satisfazando às condições $Ord_p(q) \equiv Ord_q(p) \equiv 1 \ (mod\ 2)$ e $K_1 \subseteq \mathbb{Q}(\zeta_p)$, $K_2 \subseteq \mathbb{Q}(\zeta_q)$ tais que $h_p = [\mathbb{Q}(\zeta_p) : K_1]$ e $h_q = [\mathbb{Q}(\zeta_q) : K_2]$ sejam ímpares. Sejam ainda $n_1 = [K_1 : \mathbb{Q}]$ e $n_2 = [K_2 : \mathbb{Q}]$.



O corpo $K = K_1K_2$ tem grau n_1n_2, e sendo K_1 e K_2 corpos linearmente disjuntos, ou seja, têm discriminantes relativamente primos e satisfazem $K_1 \cap K_2 = \mathbb{Q}$, então seu discriminante é dado por

$$\mathfrak{D}_K = p^{n_2(n_1-1)}.q^{n_1(n_2-1)}.$$

Em K, sejam r_p e r_q a quantidade de primos acima de p e q, respectivamente. Sendo h_p e h_q ímpares, vale as decomposições

$$p.\mathcal{O}_K = (\mathfrak{p}_1...\mathfrak{p}_{r_p/2}.\overline{\mathfrak{p}_1...\mathfrak{p}_{r_q/2}})^{n_2}$$

e

$$q.\mathcal{O}_K = (\mathfrak{q}_1...\mathfrak{q}_{r_q/2}.\overline{\mathfrak{q}_1...\mathfrak{q}_{r_q/2}})^{n_1}.$$

Seja

$$\mathfrak{I} = \mathfrak{p}_1...\mathfrak{p}_{r_p/2}.\mathfrak{q}_1...\mathfrak{q}_{r_q/2}.$$

Sua norma é

$$N(\mathfrak{I}) = (p^{h_p})^{r_p/2}(q^{h_q})^{r_q/2} = p^{n_2/2}q^{n_1/2},$$

e para $x \in \mathfrak{I}$, vale

$$Tr_{K/\mathbb{Q}}(x\overline{x}) = \frac{1}{h_p h_q} Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(x\overline{x}).$$

Como h_p e h_q são ímpares e em $\mathbb{Z}[\zeta_{pq}]$ a forma quadrática é par, então

$$Tr_{K/\mathbb{Q}}(x\overline{x}) \geq 2pq.$$

A expressão para a densidade de centro é:

$$\delta = \frac{(2pq)^{n_1 n_2/2}}{p^{n_2(n_1-1)/2}.q^{n_1(n_2-1)/2}p^{n_2/2}q^{n_1/2}.2^{n_1 n_2}} = \frac{1}{2^{n_1 n_2/2}}. \tag{3.18}$$

Para $n_1 n_2 = 4$, temos $\delta = 1/4$, justamente a densidade de centro de D_4 .

Analogamente, para $n_1 n_2 = 8$ a densidade de centro será $\delta = 1/8$, que é a densidade de centro de E_8.

Para obter um reticulado com a mesma densidade de centro de E_8 por este método, basta para isso tomar p, q, n_1 e n_2 convenientes. Assim, potencialmente existem infinitas possibilidades de construção.

Exemplo 3.5.9 *As condições acima, para $n_1 n_2 = 8$, são satisfeitas por exemplo para os seguintes casos:*

Sejam $p = 3$, $q = 13$, $K_1 = \mathbb{Q}(\zeta_3)$ e K_2 o subcorpo de $\mathbb{Q}(\zeta_{13})$ de grau 4.

Para $p = 7$, $q = 29$, sejam $K_1 = \mathbb{Q}(\sqrt{-7})$ a extensão quadrática contida em $\mathbb{Q}(\zeta_7)$ e K_2 o subcorpo de $\mathbb{Q}(\zeta_{29})$ de grau 4.

Em ambos os casos, o corpo $K = K_1 K_2$ tem grau 8 e satisfaz às condições acima.

Exemplo 3.5.10 *Sejam $p = 5$, $q = 31$, $K_1 = \mathbb{Q}(\zeta_5)$ e K_2 o subcorpo de $\mathbb{Q}(\zeta_{31})$ de grau 6. Se todo $x \in \mathfrak{I} \cap K_1 K_2$ satisfizer*

$$Tr_{K_1 K_2/\mathbb{Q}}(x\overline{x}) \geq 4.p.q,$$

então teremos uma versão rotacionada de Λ_{24}.

Uma outra possibilidade é tomar K_2 como sendo a extensão quadrática contida em $\mathbb{Q}(\zeta_{31})$. Novamente, estaremos no caso do Exemplo 3.5.9.

Capítulo 4

Os Canais Gaussiano e Rayleigh com Desvanecimento

A ênfase deste capítulo está na construção de conjuntos de sinais obtidos a partir de corpos de números totalmente reais. Serão usadas propriedades de ideais na construção de conjuntos de sinais com o objetivo de alcançar um bom desempenho em termos da probabilidade de erro em ambos os canais. Para o canal gaussiano, tais constelações têm melhor desempenho que as apresentadas em [15], e para o canal Rayleigh, desempenho similar.

Este capítulo divide-se como segue:

Na seção 4.1 desenvolvemos um algoritmo para o cálculo do número de vizinhos, do qual se obteve a Tabela 2.

Em 4.3, construímos versões rotacionadas do reticulado Λ_3 com diversidade máxima, e através de simulações determinamos a rotação que minimiza a probabilidade de erro para o canal Rayleigh com desvanecimento, com a obtenção da respectiva matriz geradora M_{f_c}.

Na seção 4.4 é desenvolvida uma técnica para a obtenção de reticulados eficientes para ambos os canais, via ideais do anel de inteiros de corpos de números. Os principais

resultados são as Afirmações 1 e 2 contidas nessa referida seção, que se baseiam no limitante superior para a probabilidade de erro.

Finalmente, em 4.5 realizamos simulações para as dimensões 3 e 5, os quais confirmaram os resultados teóricos da seção 4.4. São apresentadas matrizes geradoras e os respectivos ganhos obtidos sobre as constelações de [15], para o canal gaussiano.

4.1 Terminologia

uma constelação n dimensional contendo $M = 2^m$ sinais. A cada m-upla de bits de entrada, é associado um sinal $x = (x_1, ..., x_n) \in M$.

Quando x é enviado pelo canal gaussiano, a ação do ruído faz com que o sinal recebido seja

$$r = x + \mu,$$

onde $\mu = (\mu_1, \ldots, \mu_n)$ é um processo aleatório gaussiano.

Quando um sinal x é transmitido através de um canal com ruído Rayleigh com desvanecimento, o sinal recebido é

$$r = \alpha * x + \mu,$$

onde $\mu = (\mu_1, ..., \mu_n)$ é um vetor ruído, cujas componentes são variáveis aleatórias independentes com distribuição gaussiana, média 0 e variância N_0, $\alpha = (\alpha_1, ..., \alpha_n)$ são os coeficientes de desvanecimento com segundo momento unitário e $*$ representa o produto componente a componente.

Os M sinais são escolhidos de uma constelação finita S, que é obtida a partir de um reticulado Λ. Em particular, os pontos da constelação são escolhidos nas primeiras

camadas do reticulado, de forma que o conjunto de sinais se aproxima da forma esférica. A eficiência espectral é medida em número de bits por duas dimensões,

$$\eta = \frac{2m}{n}$$

e a relação sinal ruído é dada por

$$SNR = \frac{E_b}{N_0},$$

onde E_b é a energia média por bit e $N_0/2$ é a densidade espectral de potência.

Um demodulador de máxima verossimilhança deverá minimizar a métrica

$$m(x \mid r) = \sum_{i=1}^{n} \mid r_i - x_i \mid^2$$

para o canal gaussiano, e

$$m(x \mid r, \alpha) = \sum_{i=1}^{n} \mid r_i - \alpha_i x_i \mid^2,$$

para o canal Rayleigh com desvanecimento. Depois disto, é feita uma estimativa $\widehat{x}$ do sinal enviado x e a suposta sequência de bits enviada é obtida.

Dados x e $y \in \Lambda$, denotaremos por $P(x \rightarrow y)$ a probabilidade de que quando x é transmitido, o ponto y seja detectado, ou seja, que o ponto recebido esteja mais próximo de y do que de x, na respectiva métrica. A probabilidade de erro na constelação S tomada a partir de Λ é dada por

$$P_e(S) \leq P_e(\Lambda) \leq \sum_{x \neq y} P(x \rightarrow y).$$

Em cada tipo de canal, a expressão acima possibilita a obtenção de fórmula explícita para a probabilidade de erro, conforme veremos nas seções que se seguem.

4.2 O Canal Gaussiano

Por [27], pp. 71, a probabilidade de erro de símbolo é limitada superiormente por

$$P_e(S) \leq \frac{\tau}{2}\ erfc\left(\frac{d_{min}/2}{\sqrt{2N_0}}\right), \tag{4.1}$$

onde τ é o número de vizinhos e $d_{\min}$ é a menor distância na constelação.

O ganho de codificação é dado por

$$\gamma = \frac{d^2_{\min}}{v(\Lambda)^{2/n}},$$

e representa o ganho de potência com relação a $\mathbb{Z}^n$, podendo ser obtido a partir da densidade de centro por

$$\delta = (\gamma/4)^{n/2}.$$

4.2.1 Número de vizinhos

Uma das maiores dificuldades no cálculo do número de vizinhos é a complexidade computacional para sua contagem. A seguir, propomos um algoritmo com grande redução de custo.

Considere em $\mathbb{Z}[\zeta_{p^r}]$ a relação de equivalência $\equiv$ dada por $x \equiv y$ se, e somente se existe $i \in \mathbb{Z}$ tal que $y = \zeta^i_{p^r}.x$. Denotaremos a classe de equivalência de x por $Cl(x)$. Temos

$$Cl(x) = \{\zeta^i_{p^r}.x,\ x = 0, ..., p^r - 1\}.$$

A cardinalidade de $Cl(x)$ é p^r, já que se $\zeta_{p^r}^i.x = \zeta_{p^r}^j.x$, então $i \equiv j \pmod{p^r}$; além disso, se x e y estão na mesma classe, então $Tr_{K/\mathbb{Q}}(x\overline{x}) = Tr_{K/\mathbb{Q}}(y\overline{y})$. Em particular, para um ideal qualquer $\mathfrak{a}$ em $\mathbb{Z}[\zeta_{p^r}]$, seu número de vizinhos por p^r, já que a cardinalidade de cada classe é divisível por p^r e o conjunto $\{x \in \mathfrak{a}\ ; Tr_{K/\mathbb{Q}}(x\overline{x})$ é mínimo $\}$ é a união disjunta de classes de equivalência.

No que segue, nos fixaremos ao caso particular $r = 1$.

Seja $\lambda : \mathbb{Z}[\zeta_p] \mapsto \mathbb{Z}$ a aplicação definida por $\lambda(\sum_{i=0}^{p-2} a_i\zeta_p^i) = \sum_{i=0}^{p-2} a_i$.

Dado $x = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2} \in \mathbb{Z}[\zeta_p]$, seja k o número de $a_{i's}$ nulos. Como $\lambda(\zeta_p^i x) = \lambda(x) - pa_{p-1-i}$ e os elementos de $Cl(x)$ são da forma $\zeta_p^i.x$, conclui-se que existem exatamente $(k+1).p$ elementos em $\lambda^{-1}\{\lambda(x)\} \cap Cl(x)$. Com isto, vale a seguinte

Proposição 4.2.1 *Para obter o número de vizinhos nos reticulados $\sigma(\mathfrak{p}^i)$, $i = 1, ..., (p-1)/2$, é suficiente pesquisar no conjunto $\lambda^{-1}\{0\}$.*

A partir do Teorema a seguir, é possível restringir o intervalo em $\mathbb{Z}^n$ para a busca da menor distância em $\sigma(\mathfrak{p}^i)$. O algoritmo a seguir faz uso desse resultado.

Teorema 4.2.2 *Dados os números reais $a_1, ..., a_r$, $r < n$, seja*

$$F(X_{r+1}, ..., X_n) = Q_n(a_1, ..., a_r, X_{r+1}, ..., X_n),$$

onde Q_n é a forma quadrática definida em (3.3).

Então F atinge o menor valor, com coordenadas inteiras, no vetor

$$(y, y, ..., y), \text{ onde } y = [\frac{1}{r+1}\sum_{i=1}^{r} a_i]$$

e $[z]$ é o inteiro mais próximo de z. Quando $y + 1/2$ é inteiro, então ambos $(z + 1/2, ..., z + 1/2)$ ou $(z - 1/2, ..., z - 1/2)$ são pontos de mínimo, nas condições do enunciado.

Demonstração: Seja $P = (x, x, ..., x)$, onde $x = (\sum_{i=1}^{r} a_i)/(r+1)$. Os pontos da reta em $\mathbb{R}^{n-r}$ que interceptam P e têm vetor diretor $(b_{r+1}, ..., b_n)$ são da forma

$$X = (x + tb_{r+1}, ..., x + tb_n) .$$

Sobre estas retas, F assume os valores:

$$F(x + tb_{r+1}, ..., x + tb_n) = at^2 + c,$$

onde

$a = (r+1)\sum_{j=r+1}^{n} {b_i}^2 + \sum_{i<j}(b_i - b_j)^2$ e c é uma constante.

A derivada de F com relação a t, em $t = 0$ é 0. Assim, sobre tal reta, o gráfico de F é uma parábola, cujo minimo é assumido em P.

Seja $Y_1 = (y, y, ..., y)$, onde $y = \left[\frac{\sum_{i=1}^{r} a_i}{r+1}\right]$. No que segue, suporemos $y \leq x$, já que caso contrário a prova é análoga.

As parábolas acima descritas têm coeficiente dominante

$$r\sum_{i=r+1}^{n} b_i^2 + d^2(v, 0) + (n-r).d^2(v, \Delta),$$

onde $d^2(v, 0)$ e $d^2(v, \Delta)$ são o quadrado das distâncias de v à origem e de v à diagonal de $\mathbb{R}^{n-r}$, respectivamente.

Para encontrar a direção de crescimento mínimo, consideraremos vetores diretores v de comprimento 1. Na direção de v, o coeficiente líder de uma tal parábola é

$$(r+1) + (n-r).d^2(v, \Delta).$$

Assim, a direção de crescimento mínimo ocorre quando $d^2(v, \Delta)$ é mínimo, ou seja, a direção de Y_1, que coincide com a diagonal. Para outra direção, estas parábolas têm taxa de crescimento maior. Consequentemente, para $Y \in \mathbb{R}^{n-r}$ tal que $F(Y) = F(Y_1)$, vale

$$d(Y, P) \leq d(Y_1, P),$$

com igualdade se, e somente se Y está na diagonal de $\mathbb{R}^{n-r}$.

Consequentemente, para $Y \in \mathbb{Z}^{n-r}$ temos $F(Y) \geq F(Y_1)$, com igualdade se, e somente se Y está na diagonal de $\mathbb{R}^{n-r}$. Quando $x < y + 1/2$, então $d(Y, P) = d(Y_1, P)$ ocorre somente quando $Y = Y_1$. Para $x = y + 1/2$, os únicos pontos da diagonal de $\mathbb{Z}^{n-r}$ satisfazendo $d(Y, P) = d(Y_1, P)$ são Y_1 e $Y_2 = (y + 1, ..., y + 1)$. □

Proposição 4.2.3 *Sejam $k \in \mathbb{N}$ e $M(k) = \min\{Q_n(k, x_2, ..., x_n) \mid x_2, ..., x_n \in \mathbb{Z}\}$. Então M é uma função crescente de k.*

Demonstração: Quando k é par, então

$$M(k) = \frac{k^2(n+1)}{2},$$

e no caso k ímpar,

$$M(k) = \frac{k^2(n+1)}{2} + \frac{(n-1)}{2}.$$

Supondo k par, tem-se

$$M(k+1) = \frac{(k+1)^2(n+1)}{2} + \frac{(n-1)}{2} > M(k).$$

Analogamente, se k é ímpar, mostra-se que

$$M(k+1) > M(k).$$

Assim, M é uma função crescente de k. □

Um algoritmo eficiente para calcular o número de vizinhos é:

(i) Seja $2pk$ o valor mínimo de $Tr(x\overline{x})$, para $x \in \mathfrak{p}^i$;

(ii) Encontre as listas não ordenadas $[a_0, .., a_{r-1}]$ tais que $r \geq i+1$, $\mid a_i \mid \leq \sqrt{k}$, $\sum_{i=0}^{r-1} a_i = 0$ e $\sum_{i=0}^{r-1} a_i^2 = 2k$;

(iii) Para cada multiconjunto obtido em (ii), complete com 0 as $p-r-1$ coordenadas restantes, e permute a $(p-1)$-upla sobre todas as possíveis combinações.

(iv) Para cada sequência obtida, teste se o elemento correspondente de $\mathbb{Z}[\zeta_p]$ está em $\mathfrak{p}^i$;

(v) Seja S a soma dos elementos satisfazendo a condição (iv);

(vi) O número de vizinhos será $\dfrac{S.p}{(p-r)}$.

O algoritmo apresenta uma redução substancial de custo, se comparado com todas as possibilidades de teste, que é aproximadamente $(2\sqrt{k}+1)^{p-1}$.

Tabela 2- Número de vizinhos em $\sigma(\mathfrak{p}^i)$, $i \leq \frac{p-1}{2}$ e $p \leq 13$

i	$p=5$	$p=7$	$p=11$	$p=13$
1	$4.p$	$6.p$	$10.p$	$12.p$
2	$2.p$	$6.p$	$20.p$	$30.p$
3	-	$2.p$	$10.p$	$24.p$
4	-	-	$7.p$	$6.p$
5	-	-	$2.p$	$2.p$
6	-	-	-	$2.p$

4.3 O Canal Rayleigh com Desvanecimento

Para o canal Rayleigh com desvanecimento, a probabilidade de erro de símbolo par a par com alta relação sinal-ruído satisfaz, por [4],

$$P_e(S) \leq \frac{1}{2} \prod_{x_i \neq y_i} \frac{1}{\frac{(x_i - y_i)^2}{8N_0}} = \frac{1}{2} \frac{1}{\left(\frac{\eta}{8} \frac{E_b}{N_0}\right)^l d_p^l(x,y)^2}, \tag{4.2}$$

onde E_b é a energia média por bit, l é a diversidade, $\eta = \frac{2m}{n}$ é a eficiência espectral e $d_p^2(x,y)$ é a distância l-produto normalizada de x a y, dada por

$$d_p^2(x,y) = \frac{\prod_{x_i \neq y_i} (x_i - y_i)^2}{\left(\frac{E}{n}\right)^l}, \tag{4.3}$$

onde E =E($|| \; x \; ||^2$) é a energia média por ponto da constelação.

Como o interesse é pelo caso $l = n$, omitiremos a notação l.

Seja

$$K_S = \sum_{x \in S} \frac{1}{d_p^2(x,0)}. \tag{4.4}$$

De [4], a probabilidade de erro de símbolo satisfaz

$$P_e(S) \leq \frac{1}{2} \frac{K_S}{\left(\frac{\eta}{8}\frac{E_b}{N_0}\right)^n}. \tag{4.5}$$

Para minimizar a probabilidade de erro, precisamos:

- maximizar a diversidade;
- minimizar K_S, que equivale a simultaneamente maximizar a distância produto mínima e minimizar o número de vizinhos produto.

Fixada a probabilidade de erro, devemos minimizar a energia média da constelação.

Para satisfazer a condição de diversidade máxima, as constelações serão construídas a partir de corpos de números totalmente reais, já que se $x \in K$ for não nulo e $\sigma_1, ..., \sigma_n$ são os $\mathbb{Q}$-automorfismos de K em $\mathbb{R}$, então cada coordenada de $\sigma(x) = (\sigma_1(x), ..., \sigma_n(x))$ é também distinta de zero.

Um reticulado Λ é dito crítico para o canal gaussiano quando para pequenas perturbações de seus vetores base a densidade de empacotamento não aumenta.

Analogamente, diremos que um reticulado Λ é crítico para o canal Rayleigh quando pequenas perturbações de vetores de sua base não resultar em aumento de K_Λ (fixada uma constelação com m elementos).

As constelações construídas em [15] são críticas para o canal Rayleigh com desvanecimento, porém apresentam ganho negativo no canal gaussiano, ou seja, têm desempenho inferior ao de $\mathbb{Z}^n$.

Em [4], foram construídas versões rotacionadas dos reticulados mais densos conhecidos em algumas dimensões (portanto críticos para o canal gaussiano) obtendo-se também bom desempenho no canal Rayleigh.

Em [3], foram construídas versões rotacionadas de $\mathbb{Z}^n$ e obtidas constelações críticas para o canal Rayleigh.

O principal problema aqui tratado é construir conjuntos de sinais úteis para ambos os canais. Assim, é de se esperar que estes sejam críticos em ambos os casos. Na próxima seção, apresentaremos a construção de um reticulado satisfazendo estas propriedades.

4.4 Versões Rotacionadas de Λ_3

Quando da procura por conjuntos de sinais úteis para ambos os canais, uma boa estratégia é encontrar uma rotação conveniente de um reticulado denso. Assim, o bom desempenho no canal gaussiano é mantido. Este procedimento é particularmente conveniente quando a prioridade é minimizar a probabilidade de erro para o canal gaussiano.

Nesta seção, construímos versões rotacionada de Λ_3, o reticulado mais denso em dimensão 3, e tomamos aquele com melhor desempenho no canal Rayleigh.

Seja $f(X) = X^3 + aX^2 + bX + c \in \mathbb{Q}[X]$ tal que suas raizes α, β e γ sejam reais.

Considere os vetores em $\mathbb{R}^3$, $v_1 = (\alpha, \beta, \gamma)$, $v_2 = (\beta, \gamma, \alpha)$, $v_3 = (\gamma, \alpha, \beta)$ e seja Λ o $\mathbb{Z}$-reticulado gerado por estes vetores.

Para que Λ tenha posto 3, uma condição necessária e suficiente é que o determinante de sua correspondente matriz geradora

$$M = \begin{bmatrix} \alpha & \beta & \gamma \\ \beta & \gamma & \alpha \\ \gamma & \alpha & \beta \end{bmatrix}$$

seja não nulo.

Para que α, β e γ sejam reais, é necessário e suficiente que a derivada de f se anule em dois números reais distintos, digamos x_1 e x_2, e que $f(x_1)$ e $f(x_2)$ tenham sinais distintos, digamos $f(x_2) < 0 < f(x_1)$, admitindo, sem perda de generalidade, que $x_1 < x_2$. Este comentário pode ser generalizado no seguinte resultado:

Lema 4.4.1 *Sejam $f(X) = X^3 + aX^2 + bX + c$ um polinômio com coeficientes inteiros e α, β e γ sua raizes. Para que tais raizes sejam reais, é necessário e suficiente que $a^2 - 3b > 0$ e que $c(27c + 4a^3 - 18ab) < b^2(a^2 - 4b)$.*

Demonstração: A derivada de $f(X) = X^3 + aX^2 + bX + c$ é $f'(X) = 3X^2 + 2aX + b$, cujas raizes são $x_1 = -(-a - \sqrt{a^2 - 3b})/3$ e $(-a - \sqrt{a^2 - 3b})/3$. Daí $a^2 - 3b > 0$.

Temos

$$f(x_1) = \frac{2a^3 + 2(a^2 - 3b)\sqrt{a^2 - 3b} - 9ab + 27c}{27},$$

e $f(x_1) > 0$ se, e somente se

$$\sqrt{(a^2 - 3b)^3} > \frac{9ab - 2a^3 - 27c}{2}.$$

Analogamente, $f(x_2) < 0$ se, e somente se

$$\sqrt{(a^2 - 3b)^3} > \frac{-(9ab - 2a^3 - 27c)}{2}.$$

Sejam α, β e γ as raizes de $f(X) = X^3 + aX^2 + bX + c$. Então

$$\begin{cases} \alpha + \beta + \gamma = -a; \\ \alpha\beta + \alpha\gamma + \beta\gamma = b; \\ \alpha\beta\gamma = -c. \end{cases}$$

Sejam $f(X) = X^3 + aX^2 + bX + c$ um polinômio satisfazendo às condições do Lema 4.3.1 e α, β e γ suas raizes. Sejam ainda $v_1 = (\alpha, \beta, \gamma)$, $v_2 = (\beta, \gamma, \alpha)$ e $v_3 = (\gamma, \alpha, \beta)$ e Λ o reticulado do $\mathbb{R}^3$ gerado por estes vetores. A densidade de centro de Λ é dada por

$$\delta_M = \frac{\rho^3}{|\det M|},$$

onde

$$M = \begin{bmatrix} \alpha & \beta & \gamma \\ \beta & \gamma & \alpha \\ \gamma & \alpha & \beta \end{bmatrix}$$

é a matriz geradora e ρ é o raio de empacotamento de Λ.

Lema 4.4.2 *O determinante da matriz M vale*

$$\det(M) = -a^3 + 3ab.$$

Demonstração: Com a notação acima, temos

$$|v_i|^2 = \alpha^2 + \beta^2 + \gamma^2 = a^2 - 2b,$$

e

$$v_i v_j = \alpha\beta + \alpha\gamma + \beta\gamma = b,$$

para $i, j = 1, 2, 3$, $i \neq j$. Concluímos o resultado através de manipulações algébricas simples e usando as igualdades acima. □

A seguir, consideraremos $\det(M) \neq 0$, ou seja, o correspondente reticulado tem posto 3.

Seja $v = \sum_{i=1}^{n} X_i v_i \in \Lambda$, $X_i \in \mathbb{Z}$ um vetor genérico de Λ. O quadrado da distância de v até a origem é

$$| v |^2 = v.v = \sum_{i=1}^{3} X_i^2 \mid v_i \mid^2 + 2\sum_{i \neq j} X_i X_j v_i v_j.$$

A expressão acima nas indeterminadas X_i é portanto a forma quadrática $Q(X_1, X_2, X_3)$ associada a Λ.

Assim, encontrar o raio de empacotamento ρ equivale a minimizar a forma quadrática $Q(X_1, X_2, X_3)$, com entradas inteiras não todas nulas.

Seja $K = \mathbb{Q}(\zeta_9)$ e $K^+ = K \cap \mathbb{R}$ seu subcorpo real maximal. Então $K^+ = \mathbb{Q}(\alpha)$, onde $\alpha = \zeta_9 + \zeta_9^{-1} = 2\cos\frac{2\pi}{9}$. O polinômio minimal de α sobre $\mathbb{Q}$ é

$$f(X) = X^3 - 6X^2 + 9X - 1.$$

As raizes de f são reais. Com a notação anterior, Λ é a realização geométrica do submódulo de $\mathcal{O}_{K^+}$ gerado por α, β e γ. O volume é dado por

$$\det(M) = 54,$$

com correspondente forma quadrática

$$Q(X_1, X_2, X_3) = 18(X_1^2 + X_2^2 + X_3^2 + X_1X_2 + X_1X_3 + X_2X_3) .$$

Para a entrada $(1, 0, 0)$, Q atinge o menor valor 18. A densidade de centro é portanto

$$\delta_\Lambda = \frac{1}{4\sqrt{2}},$$

a mesma de Λ_3. Logo, Λ é uma versão rotacionada de Λ_3.

Obtivemos um reticulado denso construído a partir de um submódulo de $\mathcal{O}_K$, onde K é um corpo totalmente real. Logo, este apresenta diversidade máxima $L = 3$ e portanto espera-se um bom desempenho em ambos os canais.

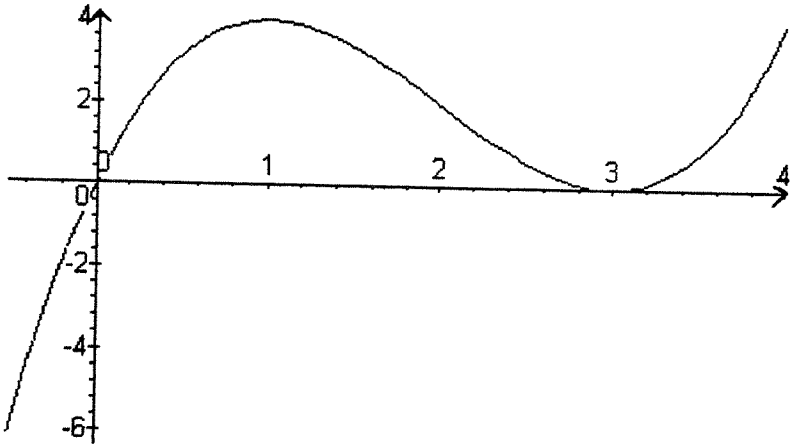


Figure 4-1: Gráfico de $f(X) = X^3 - 6X^2 + 9X$

Note que o volume e o raio de empacotamento independem do termo constante c do polinômio $f(X)$. Assim, para cada c tal que as raizes de

$$f_c(X) = X^3 - 6X^2 + 9X - c$$

sejam reais, uma construção análoga fornece versões rotacionadas Λ_{f_c} de Λ_3.

Para $0 < c < 4$, f_c tem todas suas raizes reais. Para obter bom desempenho no canal Rayleigh, tomamos 100 valores para c no intervalo $0 < c < 4$, e calculamos o parâmetro $K_{\Lambda_{f_c}}$, para uma constelação esférica de 64 sinais. O limitante superior para a probabilidade de erro é minimizada para $K_{\Lambda_{f_c}}$ mínimo. Simulamos este procedimento e o gráfico da função $c \mapsto \log_2(K_{\Lambda_{f_c}})$ é mostrado na figura 4-1:

O menor valor é obtido para $c \simeq 3.848$, com correspondente valor $K_{\Lambda_{f_c}} = 5.243$. A matriz geradora correspondente é

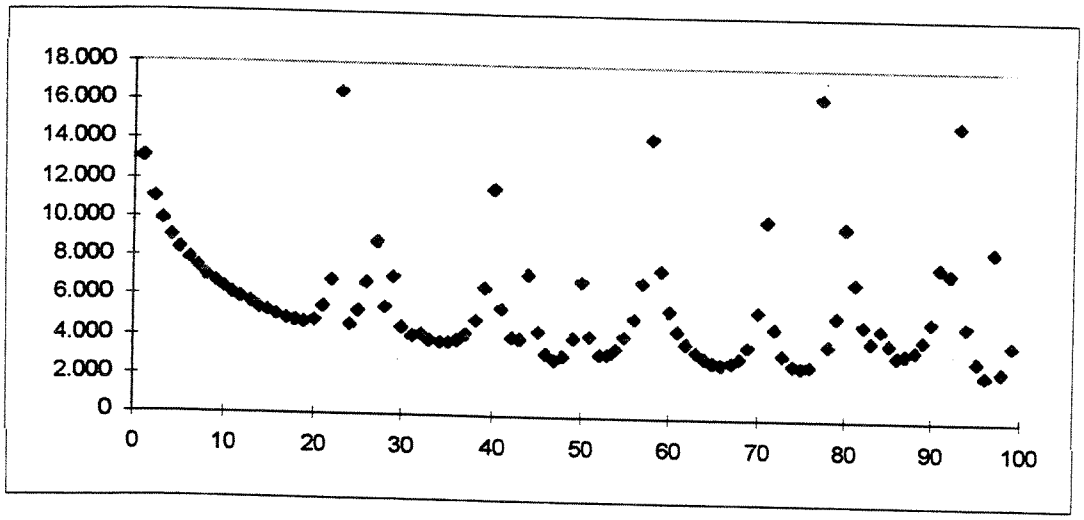


Figure 4-2:

$$M_{f_c} = \begin{bmatrix} 0.7813 & 1.2360 & 3.9827 \\ 1.2360 & 3.9827 & 0.7813 \\ 3.9827 & 0.7813 & 1.2360 \end{bmatrix}.$$

O reticulado Λ_c assim obtido é crítico para ambos os canais.

4.5 Constelações Construídas a partir de Ideais

Como vimos na seção 4.3, a técnica apropriada para a obtenção de conjuntos de sinais eficicientes para ambos os canais é rotacionar reticulados densos. Com isso, são preservadas as propriedades de empacotamento esférico. A idéia básica nesta seção é a sistematização de um procedimento inverso, que permite pesquisar em um conjunto de reticulados apresentando desempenho similar no canal Rayleigh, buscando dentre estes uma boa densidade de empacotamento.

4.5.1 Discriminante mínimo

Nesta subseção, descrevemos as idéias básicas usadas em [15] para obter reticulados ótimos para o canal Rayleigh.

Sejam K um corpo de números totalmente real de grau n, com respectivo grupo de automorfismos $\{\sigma_1, ..., \sigma_n\}$ e S um conjunto de sinais construído via representação geométrica de $\mathcal{O}_K$. Sejam $x \in \mathcal{O}_K$ e $y = \sigma(x) \in S$ o correspondente sinal, isto é,

Vetores x e y estão na :

$$y = (\sigma_1(x), ..., \sigma_n(x)).$$

Para o produto das coordenadas, vale

$$| N_{K|\mathbb{Q}}(x) | = | \sigma_1(x)...\sigma_n(x) | \geq 1. \tag{4.6}$$

Neste caso, a diversidade é máxima, e assim

$$d_p(y,0) = \frac{\prod_{i=1}^{n} \sigma_i(x)^2}{\left(\frac{E}{n}\right)^n} = \frac{N_{K|\mathbb{Q}}(x)^2}{\left(\frac{E}{n}\right)^n} \geq \frac{1}{\left(\frac{E}{n}\right)^n}. \tag{4.7}$$

Para minimizar a probabilidade de erro, é necessário aumentar as distâncias produto. A Propriedade 4.6 assegura um limitante inferior para o produto das coordenadas de $\sigma(x)$, e esta propriedade vale para todo corpo de números K. Logo, a maximização de (4.7) vem com a minimização da energia E da constelação, ou, equivalentemente, tomando K com discriminante mínimo.

Em [4] foram calculados os desempenhos das constelações obtidas desta forma, em dimensões $n \leq 8$.

4.5.2 Ideais no anel de inteiros

Com a notação acima, seja $\mathfrak{a}$ um ideal de $\mathcal{O}_K$. Então para $0 \neq x \in \mathfrak{a}$, o produto das coordenadas de $\sigma(x)$ satisfaz

$$| N_{K|\mathbb{Q}}(x) | \geq N(\mathfrak{a}), \tag{4.8}$$

onde $N(\mathfrak{a})$ é a norma de $\mathfrak{a}$.

O exemplo a seguir mostra que é possível aumentar simultaneamente a energia E e o produto das coordenadas em um conjunto de sinais, e ao mesmo tempo preservar a distância produto. Para $t > 0$, temos

$$d_p(tx, ty) = \frac{\prod\limits_{x_i \neq y_i} (tx_i - ty_i)^2}{\left(\frac{E'}{n}\right)^n} = \frac{t^{2n} \cdot \prod\limits_{x_i \neq y_i} (x_i - y_i)^2}{\left(\frac{t^2 E}{n}\right)^n} = \frac{\prod\limits_{x_i \neq y_i} (x_i - y_i)^2}{\left(\frac{E}{n}\right)^n} = d_p(x, y).$$

Quando comparamos dois sistemas, digamos 1 e 2, com as mesmas dimensões e eficiência espectral, podemos supor a mesma energia, pois como vimos acima, a multiplicação por um escalar t conveniente não altera as distâncias produto. Assim, uma boa medida para o ganho assintótico é dada em [15],

$$G_a = 10 \log_{10}(K_1/K_2).$$

Para canal Rayleigh e baseados no limitante superior para a probabilidade de erro de (4.5), temos as seguintes afirmações:

Afirmação 1 - Assintoticamente, quando o número de sinais tende ao infinito, constelações esféricas construídas a partir de um ideal principal $\mathfrak{a} \in \mathcal{O}_K$ têm desempenho equivalente às constelações construídas a partir de $\mathcal{O}_K$.

Afirmação 2 - Assintoticamente, quando o número de sinais tende ao infinito, constelações esféricas construídas a partir de um ideal não principal $\mathfrak{a} \in \mathcal{O}_K$ têm desempenho melhor que constelações construídas a partir de $\mathcal{O}_K$.

De fato, sejam S_1 uma constelação esférica com m pontos em $\Lambda_{\mathcal{O}_K}$, energia $E(S_1)$ e volume $m.v(\Lambda_{\mathcal{O}_K})$ (por volume de uma constelação esférica entenda-se o volume da bola contendo a constelação), e S_1^* a constelação obtida multiplicando os sinais de S_1 por $N(\mathfrak{a})^{\frac{1}{n}}$. Então S_1^* terá volume $m.N(\mathfrak{a}).v(\Lambda_{\mathcal{O}_K})$ e energia $E(S_1^*) = N(\mathfrak{a})^{\frac{2}{n}}.E(S_1)$.

Consideremos agora uma constelação esférica S_2 de m sinais em $\Lambda_{\mathfrak{a}}$. Seu volume será $m.N(\mathfrak{a}).v(\Lambda_{\mathcal{O}_K})$. Como S_1^* e S_2 são constelações esféricas de m sinais ocupando o mesmo volume, então suas energias são aproximadamente as mesmas, ou seja,

$$E(S_2) \simeq N(\mathfrak{a})^{\frac{2}{n}}.E(S_1).$$

Para $x, y \in \mathfrak{a}$, a distância produto em $\sigma(\mathfrak{a})$ satisfaz

$$d_p(\sigma(x), \sigma(y)) = \frac{\prod_{i=1}^{n}(\sigma_i(x) - \sigma_i(y))^2}{\left(\frac{E(S_2)}{n}\right)^n} = \frac{N_{K|\mathbb{Q}}(x-y)^2}{\left(\frac{E(S_2)}{n}\right)^n} \geq$$

$$\frac{N(\mathfrak{a})^2}{\left(\frac{N(\mathfrak{a})^{\frac{2}{n}}.E(S_1)}{n}\right)^n} = \frac{1}{\left(\frac{E(S_1)}{n}\right)^n}, \tag{4.9}$$

similar ao limitante em (4.7).

Quando $\mathfrak{a}$ é principal, comparando o conjunto das distâncias produto em $\sigma(\mathfrak{a})$ e $\sigma(\mathcal{O}_K)$, observamos uma equivalência "assintótica".

Quando $\mathfrak{a}$ é não principal, então $N(x) > N(\mathfrak{a})$, para todo $x \in \mathfrak{a}$. Neste caso, temos a desigualdade estrita em (4.9). Consequentemente, um ideal não principal apresenta ganho sobre os principais, em particular sobre $\mathcal{O}_K$.

O ganho assintótico de um ideal $\mathfrak{a}$ relativamente a $\mathcal{O}_K$, para o canal gaussiano, é dado por

$$G_a = 10\log_{10}(\gamma_a/\gamma_{\mathcal{O}_K}),$$

onde γ é o correspondente ganho de codificação.

4.6 Reticulados Úteis para os Canais Gaussiano e Rayleigh com Desvanecimento

Nesta seção, construímos constelações de sinais a partir de ideais do anel de inteiros de um corpo de números, a partir de reticulados obtidos no capítulo 3.

É natural partir de um anel $\mathcal{O}_K$ cuja representação geométrica apresente bom desempenho para o canal Rayleigh. As próximas construções são baseadas em ideais de $\mathcal{O}_K$, onde K é o corpo real de discriminante mínimo na respectiva dimensão. (cf. [15]).

Seja $K = \mathbb{Q}(\zeta_p)$ e $K^+ = \mathbb{Q}(\zeta_p) \cap \mathbb{R}$ o subcorpo real maximal de $\mathbb{Q}(\zeta_p)$. Então $K^+ = \mathbb{Q}(\alpha)$, onde $\alpha = \zeta_p + \zeta_p^{-1}$, e respectivo anel de inteiros $\mathbb{Z}[\alpha]$. Seja $\mathfrak{p}$ o ideal principal de $\mathbb{Z}[\zeta_p]$ gerado por $1 - \zeta_p$ e $\mathfrak{p}_{K^+} = \mathfrak{p} \cap K^+ = (2 - \alpha).\mathbb{Z}[\alpha]$.

Visto que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, então $\mathfrak{p}$ é o único ideal primo de $\mathcal{O}_K$ acima de p,

$$p\mathbb{Z}[\zeta_p] = \mathfrak{p}^{p-1}$$

e por propriedades de ramificação,

$$\mathfrak{p}_{K^+}\mathbb{Z}[\zeta_p] = \mathfrak{p}^2.$$

Se $x \in \mathfrak{p}_{K^+}$, então $x \in \mathfrak{p}_K$, e pelo Lema 3.2.5 vale $Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(x\overline{x}) \geq 4p$. Assim,

$$Tr_{K^+/\mathbb{Q}}(x\overline{x}) = \frac{1}{2}Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(x\overline{x}) \geq \frac{1}{2}4p = 2p.$$

O discriminante de K^+ é

$$\mathfrak{D}_{K^+} = p^{\frac{p-3}{2}}.$$

Portanto, a densidade de centro satisfaz

$$\delta(\mathfrak{p}_{K^+}) \geq \frac{\rho^n}{|\mathfrak{D}_K^+|^{1/2} N(\mathfrak{p}_{K^+})} = \frac{1}{2^{(p-1)/4}.p^{1/2}}. \tag{4.10}$$

Dimensão 3: O corpo real de discriminante mínimo é $K^+ = \mathbb{Q}(\zeta_7) \cap \mathbb{R}$. Com a notação acima, a matriz geradora de $\sigma(\mathfrak{p}_{K^+})$ é

$$M_{\mathfrak{p}_{K^+}} = \begin{bmatrix} 3.8019 & 2.4450 & 0.7530 \\ -6.8509 & -1.0881 & 0.9390 \\ 12.3448 & 0.4843 & 1.1709 \end{bmatrix}.$$

O ganho fundamental de codificação é $\gamma = 0.624$ dB.

Para constelações esféricas de 64 sinais, obtem-se $K_{\sigma_L} \simeq K_a \simeq 2.57$. Portanto, neste caso verifica-se a Afirmação 1.

Dimensão 5: Esta construção é análoga à dimensão 3. O corpo real de discriminante mínimo é $K^+ = \mathbb{Q}(\zeta_{11}) \cap \mathbb{R}$, e matriz geradora

$$M_{\mathfrak{p}_{K^+}} = \begin{bmatrix} 3.9190 & 3.3097 & 2.2847 & 1.1692 & 0.3175 \\ -7.5205 & -4.3348 & -0.6503 & 0.9714 & 0.5342 \\ 14.4317 & 5.6774 & 0.1851 & 0.8071 & 0.8988 \\ -27.6942 & -7.4358 & -0.0527 & 0.6705 & 1.5122 \\ 53.1448 & 9.7388 & 0.0150 & 0.5571 & 2.5442 \end{bmatrix}.$$

O ganho fundamental de codificação é $\gamma = 0.927$ dB.

Capítulo 5

Códigos n-ários Via Reticulados Algébricos

Neste capítulo, estudamos as relações entre a teoria desenvolvida no trabalho e outras áreas da Teoria da Comunicação.

A Proposição 5.1.1 mostra que os reticulados $\sigma(\mathfrak{p}^i)$ apresentam densidade de empacotamento cíclica. Portanto, existe certo controle sobre a cadeia de partições (5.1). Destaca-se ainda na seção 5.1 o Teorema 5.1.2.

Na seção 5.2, temos a associação entre códigos, ideais do anel de inteiros e reticulados apresentada em (5.3). Ainda destacam-se o resultado de (5.4), que associa o reticulado $\sigma(\mathfrak{p}^i)$ com códigos BCH primitivos, o Teorema 5.2.2 e o Corolário 5.2.8, que mostra a existência de relação entre a métrica de Lee nos códigos BCH e a distância euclidiana no reticulado correspondente. Simulações mostram ainda uma relação com a distância produto, conforme a Conjectura 3.

A Tabela 5-1 mostra que o mínimo efetivo ultrapassa o limitante em (3.6) para as dimensões 11 e 13.

5.1 Partição de Reticulados Via Potências de Ideais

Sejam Λ um reticulado e $\Lambda' \subseteq \Lambda$ um subreticulado de índice t. O quociente Λ/Λ', chamado de partição de Λ, define t classes de equivalência módulo Λ'. A classe de x é dada por

$$x + \Lambda' = \{x + \lambda' \, ; \lambda' \in \Lambda'\}.$$

Dois pontos estão na mesma classe se, e somente se,

$$x - y \in \Lambda'.$$

A distância intra-classe é definida como sendo a menor distância obtida quando se considera todos os elementos de uma mesma classe. Como cada classe é uma translação de Λ', então a distância intra-classe $d'_{\min}$ é igual a

$$d'_{\min} = \min\{d(x,0) \, ; x \in \Lambda'\}.$$

Dados os reticulados $\Lambda = \Lambda_0, \Lambda_1, ..., \Lambda_m$ tais que $\Lambda_{i+1} \subseteq \Lambda_i$, dá-se o nome de cadeia de partição de reticulados à sequência

$$\Lambda_0/\Lambda_1/\cdots/\Lambda_m.$$

Podemos escrever

$$\Lambda_0 = \Lambda_0/\Lambda_1 + \Lambda_1/\Lambda_2 + \cdots + \Lambda_{m-1}/\Lambda_m + \Lambda_m.$$

A construção de reticulados a partir de um ideal $\mathfrak{a}$ é um meio eficiente para obter subreticulados de índice $N(\mathfrak{a})$. Por exemplo, consideremos os ideais $\mathfrak{p}^i$ acima de p em $\mathbb{Z}[\zeta_p]$. Assim, obtém-se uma cadeia infinita

$$\sigma(\mathcal{O}_K) = \sigma(\mathfrak{p}^0)/\sigma(\mathfrak{p})/\sigma(\mathfrak{p}^2)/\sigma(\mathfrak{p}^3)/\cdots \, , \tag{5.1}$$

onde

$$\sigma(\mathfrak{p}^i)/\sigma(\mathfrak{p}^{i+1}) \simeq \mathbb{Z}/p\mathbb{Z}.$$

Como vimos, numa partição de reticulados, são parâmetros importantes a densidade de centro do reticulado Λ (para minimizar a energia) e a menor distância em Λ', a distância intra-classe.

Para a cadeia acima, conhecemos a densidade dos reticulados $\sigma(\mathfrak{p}^i)$, para $i = 0, ..., \frac{p-1}{2}$. Além disso, a densidade é periódica, como mostra a seguinte

Proposição 5.1.1 *Para os ideais* $\mathfrak{p}^j \in K = \mathbb{Q}(\zeta_{p^r})$, $j \in \mathbb{N}$, *vale*

$$\delta(\sigma(\mathfrak{p}^n)) = \delta(\sigma(\mathfrak{p}^{n+m})),$$

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

Demonstração: Sabe-se que $\mathfrak{p}^m = p\mathcal{O}_K$, pois p se ramifica completamente; logo, $\mathfrak{p}^{n+m} = p.\mathfrak{p}^n$, que implica $N(\mathfrak{p}^{n+m}) = p^{n+m}$. Com isto, $x \in \mathfrak{p}^{n+m}$ se, e somente se, $x = py$, onde $y \in \mathfrak{p}^n$. Segue que

$$| \sigma(x) |^2 = p^2 . | \sigma(y) |^2,$$

valendo assim

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

e

$$\rho(\mathfrak{p}^{n+m}) = min\left\{\frac{| \sigma(x) |}{2}; x \in \mathfrak{p}^{n+m}\right\} = min\left\{\frac{| \sigma(x) |}{2}; x \in p.\mathfrak{p}^n\right\} = p.\rho(\mathfrak{p}^n).$$

Para a densidade de centro, temos:

$$\delta(\sigma(\mathfrak{p}^{n+m})) = \frac{(\rho(\mathfrak{p}^{n+m}))^m}{| \mathfrak{D}_K |^{1/2} .p^{n+m}} = \frac{(\rho(\mathfrak{p}^n))^m}{| \mathfrak{D}_K |^{1/2} .p^n} = \delta(\sigma(\mathfrak{p}^n)). \square$$

5.1.1 Conjunto de sinais e estruturas algébricas

O ganho de potência de uma constelação esférica sobre uma constelação consistindo dos vértices de um cubo foi tratado em [5], e é chamado de ganho de forma (shape gain). Seu valor assintótico, isto é, quando a dimensão tende ao infinito, é $G_a \simeq 1,53\ dB$.

Seja $d(x,y)$ a distância euclidiana de x a y. A região de Voronoi de um reticulado Λ é definida como sendo o conjunto dos pontos $x \in \mathbb{R}^n$ tais que $d(x,0) < d(x,y)$, para todo $y \in \Lambda$. Esta região será indicada por V_Λ.

O volume de V_Λ é igual ao volume da região fundamental de Λ.

Note que a densidade de empacotamento de um reticulado tem relação com a forma de sua região de Voronoi, já que quanto mais denso for o reticulado, maior tende a ser seu número de vizinhos, que por sua vez é igual ao número de faces da região de Voronoi. Note que o número de faces de um hipercubo em dimensão n é $2n$.

Por [27], pp. 24, existem reticulados em dimensão n com número de vizinhos τ (consequentemente número de faces de V_Λ) satisfazendo $\tau > 2^{0.2075...n}$. Visto que $\frac{\tau}{n} \mapsto \infty$, para $n \mapsto \infty$, então o número de faces por dimensão cresce indefinidamente, ou seja, assintoticamente, constelações tomadas na região de Voronoi destes reticulados tendem a ter desempenho igual ao de constelações esféricas.

Uma das vantagens de tomar conjunto de sinais dentro da região de Voronoi é a possibilidade de que estes apresentem estrutura algébrica, como será visto na próxima seção.

Seja Λ um reticulado e $\Lambda' \subset \Lambda$ um subreticulado de índice t. Então o quociente Λ/Λ' tem t elementos. Para cada classe módulo Λ', tomemos um representante x tal que a distância euclidiana até a origem $d(x,0)$ seja mínima. Assim, obtem-se um conjunto de representantes com energia mínima.

Teorema 5.1.2 *Um conjunto completo de representantes do quociente Λ/Λ' com energia mínima pode ser tomado na região de Voronoi de Λ'.*

Demonstração: Sejam x, $y \in V_{\Lambda'}$. Então

$$d(x,y) \leq d(x,0) + d(y,0) = d'_{\min},$$

onde

$$d'_{\min} = \min\{d(x,0)\ ; x \in \Lambda'\}.$$

Por outro lado, estando x e y na mesma classe lateral, então $x - y \in \Lambda'$, e assim

$$d(x,y) = d(x-y,0) \geq d'_{\min}.$$

A única possibilidade para que x, y satisfaçam às condições acima é $y = -x$, ou seja, estão na borda da região $V_{\Lambda'}$ e nesse caso tanto x quanto y podem ser tomados como representantes da classe. □

Quanto à estrutura algébrica, pode-se apenas afirmar que o quociente Λ/Λ' tem a estrutura de grupo. É interessante que o conjunto de sinais esteja associado a uma estrutura algébrica mais rica, como a de anel ou corpo. Quando $\Lambda = \sigma(\mathcal{O}_K)$, para algum corpo de números K e $\Lambda' = \sigma(\mathfrak{a})$, para um ideal $\mathfrak{a} \in \mathcal{O}_K$, então Λ/Λ' herda a estrutura de anel e vale o isomorfismo

$$\Lambda/\Lambda' \simeq \mathcal{O}_K/\mathfrak{a}\ .$$

Observe que quando $\mathfrak{a}$ é um ideal primo, então Λ/Λ' é um corpo. Assim, a teoria desenvolvida nos capítulos anteriores é uma importante ferramenta para a obtenção de conjuntos de sinais com estrutura.

Exemplo 5.1.3 *Para $K = \mathbb{Q}(\zeta_3)$, o anel $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ é principal. Vimos no exemplo 2.3.6 que todo ideal $\mathfrak{a}$ tem a mesma densidade de $\mathcal{O}_K$, ou seja, são "versões rotacionadas" de Λ_2, multiplicados por escalar. Assim, a região de Voronoi dos reticulados $\Lambda' = \sigma(\mathfrak{a})$ são hexágonos, e o conjunto de representantes dentro da região de Voronoi tem a forma hexagonal.*

5.2 Códigos BCH n-ários Via Reticulados Algébricos

Para simplicidade de notação, denotaremos $\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z}$.

Sejam $K = \mathbb{Q}(\zeta_n)$, $m = \phi(n)$, $x = \sum_{i=0}^{m-1} a_i \zeta_n^i \in \mathcal{O}_K$ e

$$\Gamma : \mathcal{O}_K \mapsto \mathbb{Z}_n^m$$

o homomorfismo dado por

$$x \mapsto (\overline{a_1}, \overline{a_2}, ..., \overline{a_{m-1}}),$$

onde $\overline{a}$ significa a redução módulo n.

Para cada ideal $\mathfrak{a} \in \mathcal{O}_K$, o conjunto $\Gamma(\mathfrak{a})$ é um código linear n-ário de comprimento $\phi(n)$ e com $N = \dfrac{n^m}{N(\mathfrak{a})}$ elementos. Logo, sua taxa é

$$r = \frac{\log_n N}{m} = \frac{\log_n \dfrac{n^m}{N(\mathfrak{a})}}{m} = 1 - \frac{\log_n N(\mathfrak{a})}{m}. \tag{5.2}$$

A literatura apresenta algumas construções de reticulados a partir de códigos e vice-versa.

O anel de inteiros $\mathcal{O}_K$ faz uma intermediação natural entre o código $C = \Gamma(\mathfrak{a})$ e o reticulado $\sigma(\mathfrak{a})$, através do seguinte diagrama:

$$\begin{array}{ccccc} \mathbb{Z}_p^m & & \mathcal{O}_K & & \mathbb{R}^m \\ \cup & \Gamma & \cup & \sigma & \cup \\ C = \Gamma(\mathfrak{a}) & \longleftarrow & \mathfrak{a} & \longrightarrow & \sigma(\mathfrak{a}) \end{array} \tag{5.3}$$

Para cada palavra código $x \in C$, seja $\Phi(x)$ o vetor de menor comprimento em $\sigma(\Gamma^{-1}(x))$. Assim, Φ é uma bijeção entre o código C e a constelação $\Phi(C)$ em $\mathbb{R}^m$, que representa uma modulação para o código C.

5.2.1 Códigos BCH

Uma das vantagens em se trabalhar com reticulados algébricos é que estes podem ser melhor estudados no corpo de números correspondente, através da associação σ^{-1}. Assim, é possível trabalhar em um ambiente mais rico de propriedades algébricas. Analogamente, há vantagens ao estudar códigos gerados através de ideais de corpos de números. Um caso particularmente interessante é $K = \mathbb{Q}(\zeta_p)$ e $\mathfrak{p}$ o ideal primo acima de p. Pela caracterização de 3.2.1, pondo $x = \sum_{i=1}^{p-1} a_i \zeta_p^i \in \mathfrak{p}^j$ e $f(X) = \sum_{i=1}^{p-1} a_i \zeta_p^i$. então

$$x \in \mathfrak{p}^j \Leftrightarrow f(1) \equiv f'(1) \equiv \cdots \equiv f^{j-1}(1) \equiv 0 (\mathrm{mod}\, p).$$

Uma afirmação equivalente é

$$x \in \mathfrak{p}^j \Leftrightarrow \sum_{i=1}^{p-1} a_i \equiv \sum_{i=1}^{p-1} i a_i \equiv \cdots \equiv \sum_{i=1}^{p-1} i^{j-1} a_i \equiv 0 (\mathrm{mod}\, p).$$

Pondo

$$H = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & (p-1) \\ \vdots & & & \vdots \\ 1^{j-1} & 2^{j-1} & \cdots & (p-1)^{j-1} \end{bmatrix},$$

temos

$$x \in \mathfrak{p}^j \Leftrightarrow \Gamma(x) \text{ é ortogonal a } H, \tag{5.4}$$

ou seja, H é a matriz cheque de paridade do código $\Gamma(\mathfrak{p}^j)$. Logo, $\Gamma(\mathfrak{p}^j)$ é um código BCH primitivo módulo p. Assim, um código BCH pode ser interpretado como a "versão discreta" de ideais em $\mathcal{O}_K$.

Por exemplo, a menor distância de Hamming no código é igual ao menor número de coordenadas não nulas em $\mathfrak{p}^j$, que pode ser calculado tanto no código quanto no corpo.

A construção acima pode ser facilmente estendida à $\mathbb{Q}(\zeta_{p^r})$ e seus subcorpos, fornecendo códigos BCH com outros parâmetros. Também pode ser generalizado a $\mathbb{Q}(\zeta_n)$ qualquer.

Teorema 5.2.1 *([23], pg. 1086) Para as palavras código x, y no código BCH $\Gamma(\mathfrak{p}^i)$, vale*

$$d_{Lee}(x,y) \geq \begin{cases} 2i & , \text{ se } i \leq \frac{p-1}{2} \\ p & , \text{ se } \frac{p-1}{2} < i < p \end{cases}$$

Associaremos a métrica de Lee em $\Gamma(\mathfrak{p}^i)$ com a distância euclidiana em $\sigma(\mathfrak{p}^i)$. Para um elemento $x = \sum_{i=1}^{p-1} a_i \zeta_p^i \in \mathfrak{p}^i$, a relação geral entre métrica de Lee em $\Gamma(\mathfrak{p}^i)$ e distância euclidiana em $\sigma(\mathfrak{p}^i)$ pode ser vista na expressão

$$Tr_{K|\mathbb{Q}}(x\overline{x}) = p\sum_{i=1}^{p-1} a_i^2 - \left(\sum_{i=1}^{p-1} a_i\right)^2.$$

Mais precisamente, temos

Teorema 5.2.2 *Sejam $x, y \in \Gamma(\mathfrak{p}^i)$, $i \leq \frac{p-1}{2}$. Então*

$$d_{Lee}(x,y) \text{ é mínima} \Leftrightarrow d_{eucl}(\Phi(x), \Phi(x)) \text{ é mínima,}$$

onde d_{eucl} é a distância euclidiana.

Demonstração: Seja $z = (\overline{a_1}, \overline{a_2}, ..., \overline{a_{p-1}}) \in C$ tal que $d_{Lee}(z, 0) \geq 2r$ seja mínima . Por [23], r dos $a_{i's}$ são iguais a 1, r são iguais a -1 e os demais são nulos, e isto ocorre se, e somente se $d_{eucl}(\Phi(z), 0) = p\sum_{i=1}^{p-1} a_i^2 = 2pr$ é mínimo, já que pelo Proposição 4.1.1, o mínimo em $\sigma(\mathfrak{p}^i)$ ocorre em $\sum_{i=1}^{p-1} a_i = 0$. □

Para que o sistema apresente bom desempenho, é interessante que o reticulado $\sigma(\mathfrak{p}^i)$ apresente boa densidade de empacotamento. Como vimos no capítulo 3, seção 4, a melhor densidade entre os ideais $\mathfrak{p}^i$, $i \leq \frac{p-1}{2}$, ocorre no inteiro i_0 mais próximos de $\frac{p-1}{2.t.\ln(p)}$.

A taxa r de $\Gamma(\mathfrak{p}^{i_0})$ satisfaz $r \to 1$, com $p \to \infty$. De fato, de 5.2 a taxa é dada por

$$r = 1 - \frac{\log_p N(\mathfrak{p}^{i_0})}{p-1}.$$

O resutado vale, visto que

$$\frac{\log_p N(\mathfrak{p}^{i_0})}{p-1} = \frac{\log_p p^{\frac{p-1}{2\ln p}}}{p-1} = \frac{1}{2\ln p}$$

tende a zero, para $p \to \infty$.

5.2.2 O caso $i > \frac{p-1}{2}$

O que faremos a seguir é mostrar a existência de um limitante análogo ao do Teorema 5.2.1 para a distância euclidiana e $i > \frac{p-1}{2}$.

Todo elemento $x \in \mathbb{Z}[\zeta_p]$ pode ser escrito sob a forma

$$x = a_0 + a_1(a - \zeta_p) + a_2(a - \zeta_p)^2 + \cdots + a_{p-2}(a - \zeta_p)^{p-2}, a_i \in \mathbb{Z}, \tag{5.5}$$

e sob esta representação, para $a = 1$, a seguinte relação vale:

$$x \in \mathfrak{p}^i \Leftrightarrow a_j \equiv 0(\mathrm{mod}\, p),\ j = 0, ..., i-1\ .$$

Lema 5.2.3 *Se $i, j \in \mathbb{N}$, tem-se*

$$\sum_{\substack{u+v=k \\ u=0,\ldots,i \\ v=0,\ldots,j}} \binom{i}{u}\binom{j}{v} = \binom{i+j}{k}.$$

Demonstração: Note que ambos os lados da igualdade representam os coeficientes de X^k no polinômio

$$(1+X)^{i+j} = (1+X)^i(1+X)^j \ . \ \square$$

Lema 5.2.4 *Se $i, j \in \mathbb{N}$ e $a \in \mathbb{Z}$, tem-se*

$$Tr_{K/\mathbb{Q}}\left((a-\zeta_p)^i.(a-\zeta_p^{-1})^j\right) = p\sum_{u=0}^{i}\binom{i}{u}\binom{j}{u}a^{i+j-2u} - (a-1)^{i+j},$$

onde $\binom{j}{u} = 0$, se $j < u$.

Demonstração: Temos que

$$Tr_{K/\mathbb{Q}}\left((a-\zeta_p)^i.(a-\zeta_p^{-1})^j\right) = Tr_{K/\mathbb{Q}}\left(\sum_{\substack{u=0,\ldots,i \\ j=0,\ldots,v}}\binom{i}{u}\binom{j}{v}(-\zeta_p)^{u-v}a^{i+j-(u+v)}\right)$$

$$= (p-1)\sum_{u=0}^{i}\binom{i}{u}\binom{j}{u}a^{i+j-2u} - \sum_{\substack{u=0,\ldots,i \\ v=0,\ldots,j \\ u\neq v}}\binom{i}{u}\binom{j}{v}(-1)^{u-v}.a^{i+j-(u+v)}$$

$$= p\sum_{u=0}^{i}\binom{i}{u}\binom{j}{u}a^{i+j-2u} - \sum_{\substack{u=0,\ldots,i \\ v=0,\ldots,j}}\binom{i}{u}\binom{j}{v}(-1)^{u-v}.a^{i+j-(u+v)} \ .$$

Fazendo $u+v=k$ no Lema 5.2.3, obtemos

$$\sum_{\substack{u=0,\ldots,i\\ v=0,\ldots,j}} \binom{i}{u}\binom{j}{v}(-1)^{u+v}.a^{i+j-(u+v)} = \sum_{k=0}^{i+j}\binom{i+j}{k}(-1)^k.a^{i+j-k} = (a-1)^{i+j},$$

que conclui a prova. □

Teorema 5.2.5 *Seja*

$$x = a_0 + a_1(a-\zeta_p) + \cdots + a_{p-2}(a-\zeta_p)^{p-2} \in \mathbb{Z}[\zeta_p]\ .$$

Então

$$Tr_{K/\mathbb{Q}}(x\overline{x}) = -a_0^2 + \sum_{i,j=0}^{p-2} a_i a_j.\left(p\sum_{u=0}^{i}\binom{i}{u}\binom{j}{u}a^{i+j-2u} - (a-1)^{i+j}\right).$$

Demonstração: Temos que

$$x\overline{x} = \left(\sum_{i=0}^{p-2} a_i(a-\zeta_p)^i\right)\left(\sum_{j=0}^{p-2} a_j(a-\zeta_p^{-1})^j\right) = \sum_{i,j=0}^{p-2} a_i a_j(a-\zeta_p)^i(a-\zeta_p^{-1})^j.$$

Assim,

$$Tr_{K/\mathbb{Q}}(x\overline{x}) = Tr_{K/\mathbb{Q}}\left(\sum_{i,j=0}^{p-2} a_i a_j(a-\zeta_p)^i(a-\zeta_p^{-1})^j\right)$$

$$= (p-1).a_0^2 + \sum_{\substack{i,j=0\\(i,j)\neq(0,0)}}^{p-2} a_i a_j Tr_{K/\mathbb{Q}}\left((a-\zeta_p)^i(a-\zeta_p^{-1})^j\right)$$

$$= (p-1).a_0^2 + \sum_{\substack{i,j=0\\(i,j)\neq(0,0)}}^{p-2} a_i a_j\left(p\sum_{u=0}^{i}\binom{i}{u}\binom{j}{u}a^{i+j-2u} - (a-1)^{i+j}\right)$$

$$= -a_0^2 + \sum_{i,j=0}^{p-2} a_i a_j\left(p\sum_{u=0}^{i}\binom{i}{u}\binom{j}{u}a^{i+j-2u} - (a-1)^{i+j}\right).$$

Corolário 5.2.6 *Para* $x = a_0 + a_1(1-\zeta_p) + \cdots + a_{p-2}(1-\zeta_p)^{p-2}$, *vale*

$$Tr_{K/\mathbb{Q}}(x\overline{x}) = -a_0^2 + p\sum_{i,j=0}^{p-2}\binom{i+j}{i}a_i a_j.$$

Demonstração: Para $a = 1$ no Teorema 5.2.5, temos

$$Tr_{K/\mathbb{Q}}(x\overline{x}) = -a_0^2 + \sum_{i,j=0}^{p-2} a_i a_j.\left(p\sum_{u=0}^{i}\binom{i}{u}\binom{j}{u}\right).$$

Pelo Lema 5.2.3 temos as seguintes igualdades:

$$\binom{i+j}{i} = \sum_{u+v=i}\binom{i}{u}\binom{j}{v} = \sum_{u=i-v}\binom{i}{i-v}\binom{j}{v} = \sum_{v=0}^{j}\binom{i}{v}\binom{j}{v} = \sum_{u=0}^{i}\binom{i}{u}\binom{j}{u},$$

o que conclui a prova. □

Corolário 5.2.7 *Para* $x \in \mathfrak{p}^i$, $i \geq \dfrac{p+1}{2}$, *temos:*

$$Tr_{K/\mathbb{Q}}(x\overline{x}) \equiv 0 \pmod{2p^2}.$$

Demonstração: $Tr_{K/\mathbb{Q}}(x\overline{x})$ é obviamente par e múltiplo de p, já que $-a_0^2 \equiv 0(\mathrm{mod}\, p)$. Tal x pode ser escrito como na eq. (5.5), onde $a = 1$ e $a_0 \equiv \cdots \equiv a_{i-1} \equiv 0 \pmod{p}$.

Quando $i + j < p$, então $i < \dfrac{p-1}{2}$ ou $j < \dfrac{p-1}{2}$, que dá $a_i a_j \equiv 0(\mathrm{mod}\, p)$.

Para $i + j \geq p$, o coeficiente binomial $\binom{i+j}{i}$ é um múltiplo de p. Assim, o somatório $\sum_{i,j=1}^{p-2}\binom{i+j}{i}a_i a_j$ é um múltiplo de p. □

Com o corolário acima, podemos enunciar um resultado para distância euclidiana análogo ao apresentado no Teorema 5.2.1. Note a semelhança com a métrica de Lee, a menos de multiplicação por p.

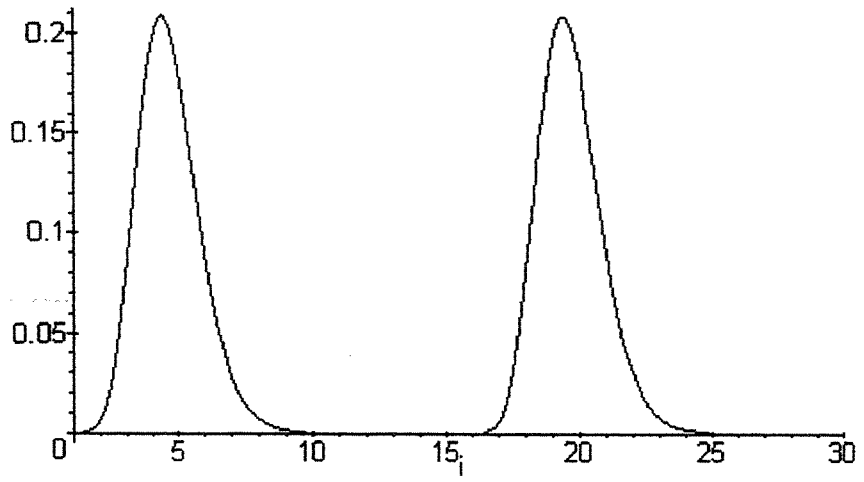


Figure 5-1:

Corolário 5.2.8 *Para as palavras código x, y no código BCH $\Gamma(\mathfrak{p}^i)$, vale*

$$d^2_{eucl}(\Phi(x),\Phi(y)) \geq \begin{cases} 2pi & , \text{ se } i \leq \frac{p-1}{2} \\ 2p^2 & , \text{ se } \frac{p-1}{2} < i < p \end{cases}$$

Temos a seguinte

Conjectura 1: Para o caso $i > \dfrac{p-1}{2}$, se $x \in \mathfrak{p}^{\frac{p-1}{2}+j}$, $j \leq \dfrac{p-1}{2}$, então

$$Tr_{K/\mathbb{Q}}(x\overline{x}) \geq 2p^2 j \ .$$

Caso esta afirmação seja verdadeira, então a densidade de centro satisfaz $\delta(\mathfrak{p}^i) = \delta(\mathfrak{p}^{\frac{p-1}{2}+i})$, ou seja, para i na segunda metade do intervalo $[1..p-1]$ repete-se a densidade de centro da primeira metade.

Como a densidade tem período n, o gráfico de A^i_{30} da figura 4-1 poderia se extender para todas as potências i, com repetições de período $n/2$.

Até agora, para $i \leq \frac{p-1}{2}$, observamos uma estreita relação entre a métrica de Lee e a distância euclidiana. Para $\frac{p-1}{2} < i < p$, observamos ainda uma forte dependência. De fato, neste caso é conhecido um outro limitante superior para a métrica de Lee, dado pelo seguinte

Teorema 5.2.9 *([23], pp. 1089) Para as palavras código x, y no código BCH $\Gamma(\mathfrak{p}^{p-1-k})$, vale*

$$d_{Lee}(x,y) \geq \frac{p^2-k^2}{4k}.$$

Note que para potências próximas de $p-1$, a distância é da ordem de p^2, o que torna o limitante do Teorema 5.2.1, para $i > \frac{p-1}{2}$, muito abaixo do mínimo efetivo. Novamente, há forte semelhança entre o limitante do Teorema 5.2.9 e o conjecturado para a distância euclidiana. Temos a seguinte

Conjectura 2: Para $x, y \in \Gamma(\mathfrak{p}^j)$, $\frac{p-1}{2} < j \leq p-1$, então

$$d_{Lee}(x,y) \text{ é mínima} \Leftrightarrow d_{eucl}(\Phi(x), \Phi(y)) \text{ é mínima.}$$

5.2.3 Mínimo efetivo

Em [23], as tabelas apresentadas mostram que o mínimo efetivo supera o limitante dado no Teorema (5.2.1) em alguns casos.

A Tabela a seguir (obtida por cálculos computacionais) mostra o menor valor de $Tr_{K/\mathbb{Q}}(x\overline{x})$, com $x \in \mathfrak{p}^i$ no corpo $K = \mathbb{Q}(\zeta_p)$. Similarmente, nota-se que o limitante no Corolário 5.2.9 não coincide com o valor mínimo efetivo. Uma consequência é que valores maiores podem ser obtidos para a densidade de centro dos ideais $\mathfrak{p}_K^i$, obtidos no Capítulo 3.

Tabela 5-2

i	$p=5$	$p=7$	$p=11$	$p=13$
1	$2.p.1$	$2.p.1$	$2.p.1$	$2.p.1$
2	$2.p.2$	$2.p.2$	$2.p.2$	$2.p.2$
3		$2.p.3$	$2.p.3$	$2.p.3$
4			$2.p.5$	$2.p.4$
5			$2.p.5$	$2.p.6$
6				$2.p.6$

5.2.4 A métrica de Lee e a distância produto no canal Rayleigh com desvanecimento.

Para o canal Rayleigh com desvanecimento, o sistema de modulação proposto acima ainda apresenta boas propriedades. Para algumas dimensões baixas, simulações mostram que analogamente ao caso gaussiano, em $\sigma(\mathfrak{p}^i)$ os sinais da primeira camada "euclidiana " estão também na primeira camada "produto". Com isto, formulamos a seguinte

Conjectura 3: Para $x, y \in \Gamma(\mathfrak{p}^j)$, $j \leq \frac{p-1}{2}$, vale:

$$Tr_{K|\mathbb{Q}}(x\overline{x}) \text{ é mínimo em } \sigma(\mathfrak{p}^j) \Rightarrow \mid N_{K|\mathbb{Q}}(x) \mid \text{ é mínimo em } \sigma(\mathfrak{p}^i), \tag{5.6}$$

ou, de outra forma,

$$Tr_{K|\mathbb{Q}}(x\overline{x}) = 2pj \Rightarrow \mid N_{K|\mathbb{Q}}(x) \mid = p^j. \tag{5.7}$$

A recíproca não é verdadeira, já que existem infinitas unidades em $\mathcal{O}_K$. Temos então

$d_{Lee}(x,y)$ é mínima$\Leftrightarrow d_{eucl}(\Phi(x),\Phi(y))$ é mínima $\Rightarrow d_{prod}(\Phi(x),\Phi(y))$ é mínima.

Simulações mostram concentração da primeira camada produto em torno da origem.

Capítulo 6

Conclusões e Propostas para Trabalhos Futuros

Este capítulo tem como objetivo ressaltar os pontos relevantes deste trabalho, assim como colocar sugestões para trabalhos futuros.

6.1 Conclusões

Neste trabalho, foram estudados reticulados construídos via ideais de anéis de inteiros de corpos de números abelianos. Motivaram a presente pesquisa algumas construçõs algébricas de reticulados densos, presentes na literatura. Como exemplo, temos os trabalhos de Maurice Craig ([7] e [8]). Mais recentemente, em [4] e [15] são feitas aplicações de reticulados construídos algebricamente em Teoria da Comunicação. Todavia, tais trabalhos apresentam soluções e técnicas restritas ao caso particular tratado, técnicas estas de difícil generalização. Aqui, buscou-se uma sistematização de procedimentos, colocando os vários trabalhos sob o mesmo ponto de vista.

A seguir, listamos os principais resultados obtidos por seção.

Capítulo 3:

Seção 3.1: É voltada para o estudo da representação geométrica do ideal $\mathfrak{p} = (1 - \zeta_{p^r})\mathbb{Z}[\zeta_p^r]$, p primo, e suas potências.

A Proposição 3.1.1 fornece uma caracterização dos elementos $x \in \mathfrak{p}^i$. Na Seção 3.1.2, o Teorema 3.1.3 explicita a forma quadrática asociada a $\mathbb{Q}(\zeta_{p^r})$.

Seção 3.2: A Proposição 3.2.2 e os Teoremas 3.2.3 e 3.2.4 determinam a potência i tal que a densidade de centro de $\sigma(\mathfrak{p}^i)$ seja a maior possível. Através destes resultados, em $\mathbb{Q}(\zeta_9)$ obtém-se o reticulado E_6, o mais denso reticulado em dimensão 6, a partir de $\sigma(\mathfrak{p}^2)$.

A Proposição 3.2.6 mostra que a menor distância nos reticulados $\sigma(\mathfrak{p}^i)$ cresce linearmente com a potência i. A partir desta, é possível generalizar a família de Craig para $\mathbb{Q}(\zeta_{p^r})$, p primo e $r \geq 1$, cuja expressão para a densidade de centro é dada no Teorema 3.2.7.

Seção 3.3: estuda uma outra direção de generalização da família de Craig, que são subcorpos de $\mathbb{Q}(\zeta_p)$. O Teorem 3.3.1 fornece uma expressão para o cálculo da densidade de centro de $\sigma(\mathfrak{p}_K^i)$, onde K é um subcorpo de $\mathbb{Q}(\zeta_p)$ e $\mathfrak{p}_K = \mathfrak{p} \cap K$. Tomando a potência inteira i que maximiza a densidade de centro, obtém-se a família $\mathcal{A}_n$. Esta família contribui com os reticulados mais densos conhecidos em infinitas dimensões e apresenta boa performance assintótica.

Seção 3.4: São estudadas propriedades aritméticas de extensões cúbicas $K = \mathbb{Q}(\alpha)$ contidas em $\mathbb{Q}(\zeta_p)$, p primo, e chega-se a uma expressão para o cálculo do índice $k = [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. É estudada ainda a representação geométrica destas extensões, chegando à obtenção de um limitante superior para k.

Seção 3.5: A Proposição 3.5.3 traz a forma quadrática associada a $\mathbb{Q}(\zeta_{pq})$, p e q primos. A seguir, são desenvolvidas técnicas de construção algébrica de reticulados:

Construção A - É feita uma nova prova para a construção algébrica do reticulado de Leech Λ_{24}, usando técnicas particulares desenvolvidas no trabalho. A prova original é extremamente técnica, e se utiliza de formas unimodulares.

Construção B: É feita uma prova para a construção algébrica do reticulado K_{12}.

Construção C: É desenvolvido um método que permite a construção do reticulado E_8 em subcorpos de diversos corpos ciclotômicos.

Capítulo 4:

Seção 4.1: Nesta seção, desenvolvemos procedimentos teóricos que permitiram a construção de um algoritmo eficiente para o cálculo do número de vizinhos dos reticulados $\sigma(\mathfrak{p}^i)$.

Seção 4.3: É desenvolvido um método algébrico para gerar versões rotacionadas de Λ_3 com diversidade máxima 3. Através de cálculos computacionais, calculamos aquela com melhor desempenho para o canal Rayleigh, gerando a matriz M_{f_c}.

Seção 4.4: Os principais resultados são as Afirmações 1 e 2, mostrando que para o canal Rayleigh, constelações construídas a partir de um ideal principal $\mathfrak{a} \in \mathcal{O}_K$ (resp. não principal) têm desempenho similar (resp. melhor) que constelações construídas a partir de $\mathcal{O}_K$.

Seção 4.5: Aqui, aplicamos os resultados da seção 4.4 para constelações obtidas em [15], que são ótimas para o canal Rayleigh, em dimensões 3 e 5. Assim, obtivemos constelações ótimas para o canal Rayleigh e apresentando ganho, para o canal gaussiano, de $0,624$ dB em dimensão 3 e $0,927$ dB em dimensão 5.

Capítulo 5: Este capítulo mostra ligações entre a teoria desenvolvida no trabalho e alguns tópicos de Teoria da Comunicação.

Traz ainda relações entre a métrica de Lee em códigos BCH e distância euclidiana nos reticulados correspondentes.

Seção 5.1: A Proposição 5.1.1 mostra que os reticulados $\sigma(\mathfrak{p}^i)$ apresentam densidade de empacotamento cíclica. Portanto, existe certo controle sobre a cadeia de partições (5.1). Destaca-se ainda o Teorema 5.1.2, mostrando que um conjunto completo de re-

presentantes do quociente de reticulados Λ/Λ' com energia mínima pode ser tomado na região de Voronoi de Λ'.

Seção 5.2: Aqui, mostramos a existência de estreitas ligações entre códigos BCH, ideais do anel de inteiros de corpos ciclotômicos e reticulados gerados a partir destes ideais. Em particular, mostramos que um código BCH primitivo módulo p pode ser obtido através do ideal $p^i = (1-\zeta_p)^i\mathbb{Z}[\zeta_p]$. Depois de alguns resultados intermediários, chegamos ao Corolário 5.2.8, que é a "versão euclidiana" do Teorema 5.2.1, encontrado em [23], que trata da métrica de Lee em códigos BCH.

A Tabela 5-1 mostra que o mínimo efetivo nos reticulados $\sigma(\ p^i)$ ultrapassa o limitante inferior dado pela Equação (3.6), para as dimensões 11 e 13.

Apêndice: É apresentado um algoritmo implementado no GAP, que calcula discriminantes de subcorpos de $\mathbb{Q}(\zeta_{p^aq^b})$ baseado no Teorema de Hasse.

6.2 Sugestões para Pesquisas Futuras

O leque de linhas de pesquisa que derivam deste trabalho é bastante abrangente. A seguir apresentamos, por capítulo, algumas sugestões.

Capítulo 3 - É natural pensarmos na extensão da família de Craig para subcorpos de $\mathbb{Q}(\zeta_n)$, para n qualquer. Assim, apontamos para a generalização do Teorema 2.1.17, do Lema 3.2.5 e do Teorema 3.3.1 para o caso geral.

Na Seção 3.5 (Cúbicas Reais Contidas em $\mathbb{Q}(\zeta_p)$), dada uma extensão cúbica $K \subseteq \mathbb{Q}(\zeta_p)$, mostramos que a densidade de centro do submódulo $\mathbb{Z}[\alpha]$ é $k^2.\delta(\sigma(\mathcal{O}_K))$, onde $k = [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Isto nos motiva a pesquisar uma classe mais geral de reticulados, os gerados por submódulos do anel de inteiros, para um corpo de números qualquer. Sendo uma classe mais ampla, quando comparada com o conjunto de todos os ideais, a vantagem está na abrangência. Uma desvantagem imediata é a ausência da riqueza de propriedades algébricas quando se trabalha com ideais.

Quanto à Seção 3.6, que traz construções algébricas em subcorpos de $\mathbb{Q}(\zeta_{pq})$, p e q primos, uma primeira alternativa de generalização é estender os conceitos para subcorpos de $\mathbb{Q}(\zeta_{p^a q^b})$, com posterior tratamento do caso geral $\mathbb{Q}(\zeta_n)$. Para a determinação do menor valor assumido pela forma quadrática, sugerimos o uso da expressão 3.9, juntamente com técnica similar à usada nas construções A e B. Contudo, esta apresentará número maior de variáveis, dificultando seu cálculo. Uma alternativa é o uso de algoritmos e cálculos computacionais.

Conjecturamos a construção algébrica de um reticulado em dimensão 28 com densidade de centro igual a 1. O mais denso reticulado conhecido em dimensão 28 tem densidade de centro $2/3$. Convém lembrar que existe um empacotamento não reticulado em dimensão 28 com densidade de centro 1.

Capítulo 4: Na Seção 4.3, construímos versões rotacionadas de Λ_3 com diversidade máxima. Nesta linha, propomos a construção de reticulados densos conhecidos via corpos de números totalmente reais. Assim, tem-se simultaneamente diversidade máxima e máxima densidade de centro conhecida. É natural pensarmos inicialmente na construção de D_4, o mais denso reticulado conhecido em dimensão 4, em um corpo de números totalmente real. Nas construções algébricas existentes, D_4 é construído a partir de corpos de números totalmente complexos, e portanto apresenta diversidade 2.

Ainda neste capítulo, propomos a extensão das simulações de 4.4 para a família $\mathcal{A}_n$, já que as dimensões 3 e 5 estudadas coincidem com os reticulados $\mathcal{A}_3$ e $\mathcal{A}_5$. Para dimensões maiores, conjecturamos bom desempenho para os canais Rayleigh com desvanecimento e gaussiano, já que para algumas dimensões os reticulados $\mathcal{A}_n$ apresentam diversidade máxima n e máxima densidade de centro conhecida .

Capítulo 5: Deste capítulo, derivam diversas possibilidades de pesquisa. Dentre elas, as Conjecturas 1 e 2 aparecem como proposta para pesquisas futuras. Atentamos também para a extensão da Tabela 5-2 para dimensões maiores.

Sugerimos ainda um estudo detalhado de um esquema baseado na família $\mathcal{A}_n$, que resulta em constelações densas, e para uma particular escolha do ideal, podemos consi-

derar eficiência espectral constante. Essas constelações estão "casadas " a códigos BCH, valendo as relações entre as métricas de Lee e euclidiana expostas no capítulo 5. Com a exigência adicional de que estes corpos sejam reais, então a constelação equivalente tem ainda a propriedade de apresentar diversidade máxima, o que torna o esquema útil para ambos os canais. Além disso, está associada uma estrutura algébrica à constelação, e a respectiva matriz geradora do reticulado é circulante.

Apêndice: Uma alternativa para o cálculo do discriminante de subcorpos de $\mathbb{Q}(\zeta_n)$, n qualquer, é generalizar o algoritmo apresentado no apêndice para o caso geral.

Apêndice

A seguir, apresentamos a rotina de um programa que calcula discriminantes de subcorpos de $\mathbb{Q}(\zeta_{p^a q^b})$, com p e q primos. O programa utilizado é o GAP (Groups, Algorithms and Programming).

```
car:=function(p,a,q,b) local l, R, n1, m1, g1, l1, n2, m2, g2, x, l2, marc, i, j, t, t1, t2,
Y, r, s, y, C, S, V, L ,k0, k1, k2, J, T, f, DIV, LL, TT, Aux, mar, G, VV, Y;
l:=[]; R:=[]; n1:=p^a; m1:=Phi(n1); g1:=1; l1:=[]; n2:=q^b; m2:=Phi(n2); g2:=1;
l2:=[];
if p=3 then
g1:=2; fi;
if q=3 then g2:=2; fi;
for i in [1..(n1-1)/2] do marc:=0; for j in [1..m1/2] do
if Mod(i^ j,n1)>1 then marc:=marc+1; fi; od;
if marc=(m1/2) then g1:=i; fi;
od;
for i in [1..(n2-1)/2] do
marc:=0; for j in [1..m2/2] do
if Mod(i^ j,n2)>1 then
marc:=marc+1; fi; od; if marc=(m2/2) then
g2:=i; fi;
od;
```

```
for i in [1..m1] do
if Mod(g1^ i,n1)=Mod(n2,n1) then
t2:=i; fi; od;
for i in [1..m2] do
if Mod(g2^ i,n2)=Mod(n1,n2) then t1:=i; fi;
od;
for i in [1..m1] do
Append(l1,[Mod(g1^ i,n1)]); od;
Append(l,[l1]);
for i in [1..m2] do
Append(l2,[Mod(g2^ i,n2)]); od;
Y:=[1..m1*m2];
for j in [0..m1-1] do for i in [0..m2-1] do
Y[i+m2*j+1]:=[[],1]; for r in [1..m1] do for s in [1..m2] do
y:=E(m1)^ (j*(t2+r))*E(m2)^ (i*(t1+s)); if y<>1 then
y:=0; fi; C:=(n1*n2)/(Gcd(j,n1)*Gcd(i,n2)); if y=1 then Append (Y[i+m2*j+1][1],
[Mod(n1*(g2^s)+n2*(g1^r), n1*n2)]); fi; od; od;
Y[i+m2*j+1][2]:=C; od; od;
S:=[]; V:=[]; for k1 in [1..m1*m2] do
J:=[]; for i in [1..Length(Y[k1][1])] do
Append(J,[true]); od;
if (Y[k1][1] in S)=false then
Append(S,[Y[k1][1]]); T:=[]; for k2 in [1..m1*m2] do
if
List(Y[k1][1],x->x in Y[k2][1] )=J then
Append(T,[Y[k2][2]]); fi; od; f:=Collected(Factors(Product(T)));
Append(V, [[Set(Y[k1][1]), f]]); fi; od;
DIV:=DivisorsInt(m1*m2); LL:=[];
```

```
for k0 in [1..Length(DIV)] do for k1 in [1..n1*n2-1] do
mar:=0; TT:=[]; for k2 in [1..DIV[k0]] do
Append(TT,[Mod(k1^ k2,n1*n2)]);
if (Mod(k1^k2,n1*n2)>1 and (k2<DIV[k0]))
or (Mod(k1^k2,n1*n2)=1 and (k2=DIV[k0])) then
mar:=mar+1; fi; od; if mar=DIV[k0] then
Append(LL,[Set(TT)]); fi;
od; od;
G:=Set(LL);
for k1 in [1..Length(G)] do
J:=[]; for i in [1..Length(G[k1])] do Append(J,[true]); od; T:=[]; for k2 in [1..m1*m2]
do
if List(G[k1],x->x in Y[k2][1])=J then
Append(T,[Y[k2][2]]); fi;
od; f:=Collected(Factors(Product(T))); Append(V,[[Set(G[k1]),f]]); od;
VV:=[]; for k1 in [1..Length(DIV)] do for k2 in [1..Length(V)] do
if Length(V[k2][1])=DIV[k1] then
Append(VV,[V[k2]]); fi; od; od;
for i in [1..Length(VV)] do
Print(VV[i],"\n"); od;
end;
```

Bibliografia

[1] Atiah, M.F. Introduction to Commutative Algebra, Addison-Weslley. 1969.

[2] Borevich, Z.I. and Shafarevich, I.R. Number Theory, Ac. Press. 1966.

[3] Boutros, J. ; Viterbo, E., Signal Space Diversity: A Power- and Bandwidth-Efficient Diversity Technique for the Rayleigh Fading Channel, IEEE Trans. Inform. Theory, V. 44, n.4, july 1998.

[4] Boutros, J. ; Viterbo, E. ; Rastello, C. e Belfiori, J.C. Good Lattice Constellations for Both Rayleigh Fading and Gaussian Channels, IEEE Trans. Inform. Theory, V. 42, n.2, mar. 1996.

[5] Calderbank, A.R. ; Sloane, N.J.A New Trellis Codes based on Lattices and Cosets, IEEE Trans. Inform. Theory, V. IT-33, pp. 177-195, 1987.

[6] Cassels, A. An Introduction to Geometry of Numbers, Springer-Verlag. 1971.

[7] Craig, M. A Cyclotomic Construction for Leech's Lattice, Math. 25. pp. 236-241, 1978.

[8] Craig, M. Extreme Forms and Cyclotomy, Math. 25, pp. 44-56. 1978.

[9] Dumimt, D.S. ; Kisilevski, H.: Indices in Cyclic Cubic Fields, Number Theory and Algebra, (Collected Papers edited by Hans Zassenhaus) Academic Press, New York, 1977, pp. 29-42.

[10] Endler, O. Teoria dos Números Algébricos, IMPA, Projeto Euclides, 1986.

[11] Flores, A.L.. Representação Geométrica de Ideais de Corpos de Números, dissertação de mestrado, UNICAMP, Campinas-SP, 1.996.

[12] Flores, A.L.; Nóbrega, T.P., Lattices in Abelian Fields. Atas do VII ENAL - Encontro em Álgebra USP/UNICAMP, pp. 43-52, junho de 1999.

[13] Forney, G.D.: Coset Codes-Part I: Introduction and Geometrical Classification, IEEE Trans. Inform. Theory, V. 34, n.5, sep. 1988.

[14] Forney, G.D.: Coset Codes-Part II: Binary Lattices and Related Codes, IEEE Trans. Inform. Theory, V. 34, n.5, sep. 1988.

[15] Giraud, X. ; Belfiori, J.C., Constellations Matched to the Rayleigh Fading Channel, IEEE Trans. Inform. Theory, Vol. 42, n.1, jan. 1996.

[16] Gonçalves, A. Introdução à Álgebra. Rio de Janeiro, IMPA - CNPq, 1988.

[17] Herstein, I.N. Tópicos de Álgebra, Ed. da Universidade de São Paulo, 1970.

[18] Kschischang, F.R ; Subbarayan, P.: Some Ternary and Quaternary Codes and Associated Sphere Packings, IEEE Trans. Inform. Theory, Vol. 38, n. 2, mar. 1992.

[19] Lang, Serge: Algebraic Number Theory, Addison-Wesley: Reading, MA, 1970.

[20] Marcus, D.A.: Number Fields, Springer-Verlag, 1977.

[21] Nóbrega, T.P.; Flores, A.L.. Reticulados em Subcorpos de $\mathbb{Q}(\zeta_{pq})$. Atas do VIII ENAL - Encontro em Álgebra USP/UNICAMP, novembro de 1999.

[22] Rosa, E.M., Códigos Treliça baseados em partições de reticulados: propriedades estruturais e determinação de códigos ótimos. Tese de mestrado. FEEC/UNICAMP - junho de 1999.

[23] Roth, R.M., Siegel, P.H.: Lee-Metric BCH Codes and Their Application to Constrained and Partial Response Channels, IEEE Trans. Inform. Theory, V. 40, n.4, july. 1994.

[24] Samuel, P.: Algebraic Theory of Numbers, Hermann, 1970.

[25] Shafarevich, I.R ; Golod, E.S. On Class Field Towers, Amer. Math. Sci. Transl. (2) 48, pp.91-102, 1965.

[26] Shannon, C.E. A Mathematical Theory of Communications, BSTJ 27 (1948), 379-423 and 623-656.

[27] Sloane, N.J.A, Conway, J.H. Sphere Packing, Lattices and Groups, Springer-Verlag, New York, 1999.

[28] Stewart, I.N. and Tall, D.O. Algebraic Number Theory, Chapman&Hall, Second Edition, London, 1.992.

[29] Washington, L.C. Introduction to Cyclotomic Fields, Springer-Verlag, 1982.

Trabalho Publicado: Atas do VII ENAL - junho de 1999

LATTICES IN ABELIAN FIELDS

André Luiz Flores[1] and Trajano Pires da Nóbrega Neto[2]

Abstract

In this paper we develop an efficient tool to construct an asymptotically good family $\mathcal{F}$ of lattices from ideals of subfields of p-cyclotomic fields. The method being proposed furnishes one lattice for every dimension. For each lattice in $\mathcal{F}$, $\frac{1}{n}\log_2(\Delta) \geq -\frac{1}{2}\log_2\log_2 n$, where Δ denotes its sphere packing density. This new family achieves the greatest known density in infinitely many dimensions.

1 Introduction

The classical problem of sphere packing is to find an arrangement of identical spheres in the n-dimensional Euclidean space so the fraction of the space filled with these spheres is the maximum number possible. This can be seen as a version of Hilbert's 18th problem, proposed in 1900. The first conection to the mathematical theory of communication was made by Shannon. More precisely, the proof of Shannon's capacity theorem [13] implies that in the case of high signal to noise ratios, an optimal block code for an ideal band-limited AWGN channel consists of a dense packing of signal points within a sphere in high-dimensional Euclidean space. Further, Leech [9] showed how to use error-correcting codes to construct dense packings in $\mathbf{R}^n$, and Conway and Sloane [4] proved that lattices satisfying the Minkowiski bound (given by equation (1) below) are equivalent to codes achieving channel capacity.

Using different techniques, several works have provided partial solutions to the sphere packing problem. Although quite relevant, these contributions are still far from solving the problem in its most general form. Among the methods for generating lattice packings, Minkowiski's embedding presents interesting characteristics. Using algebraic number theory, Craig reproduced Leech's lattice Λ_{24} from the geometric representation of an ideal in the ring of integers of $\mathbb{Q}(\zeta_{39})$ (for any $n \in \mathrm{N}$, $\zeta_n = e^{\frac{2\pi i}{n}}$). With the same method, he also obtained the family A_n^m in the dimensions $p-1$, from $\mathbb{Q}(\zeta_p)$, where p is a prime number (see [6]).

For each n, Minkowiski proved the existence of lattices in real n-dimensional space with sphere packing density Δ satisfying

$$\frac{1}{n}\log_2\Delta \geq -1. \tag{1}$$

However, his proof is nonconstructive. Constructive families are known only in particular dimensions. For example, the lattices BW_n [4, p. 234] have dimension $n = 2^m$, and asymptotically,

$$\frac{1}{n}\log_2\Delta \simeq -\frac{1}{4}\log_2 n.$$

[1]This work has been supported in part by the Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) under grant No. 143371/1996-7.

[2]This work has been supported in part by Fundação de Amparo à Pesquisa do Estado de São Paulo, FAPESP, under grant No. 95/4720-8.

Lattices from BCH codes in dimensions $n = 2^m$, and Craig's lattices A_n^m in dimensions $n = p-1$, p prime, have asymptotic performance satisfying

$$\frac{1}{n}\log_2 \Delta \simeq -\frac{1}{2}\log_2 \log_2 n.$$

In this paper we develop a method to construct a lattice in any dimension $n \geq 1$. Each lattice is obtained from a subfield of $\mathbb{Q}(\zeta_p)$, with p prime, in the following way. For each subfield K of $\mathbb{Q}(\zeta_p)$, we take the intersection of K with a suitable power of the principal ideal of $\mathbb{Q}(\zeta_p)$ generated by $1-\zeta_p$ and obtain its geometric representation. The family so constructed has the densest known lattices in several high and low dimensions. The sphere packing density Δ satisfies

$$\frac{1}{n}\log_2(\Delta) \geq -\frac{1}{2}\log_2 \log_2(n).$$

The discriminant of subfields K of $\mathbb{Q}(\zeta_n)$ can be obtained using Hasse's Theorem which states that the discriminant of an Abelian field is, up to sign, the product of the conductors of the characters associated to K. If the conductor of the Abelian field K is a prime power, we can compute its discriminant via Theorem 1.

This paper is organized as follows. In Section II we present results from algebraic number theory which are related to the construction of lattices. In Section III we introduce the family $\mathcal{F}$ and present the center density of various lattices in $\mathcal{F}$. In Section IV we draw our conclusions.

2 Preliminaries

Let K be a number field of degree m and $\{\sigma_1, \ldots, \sigma_m\}$ be the embeddings of K into $\mathbb{C}$ (the field of complex numbers) such that σ_i is real for $1 \leq i \leq r_1$, and σ_{j+r_2} is the complex conjugate of σ_j, for $r_1 + 1 \leq j \leq r_1 + r_2$. The canonical embedding $\sigma : K \to \mathbb{R}^m$ is the homomorphism defined by

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \ldots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)),$$

where $\Re z$ and $\Im z$ are the real and imaginary parts of the complex number z, respectively. Let $\mathcal{O}_K$ be the integral ring of K, and M a submodule of index k in $\mathcal{O}_K$. Then the set $\sigma(M)$ is a lattice in $\mathbb{R}^m$ of rank m, with volume

$$V(\sigma(M)) = k \cdot 2^{-r_2} \mid \mathfrak{D}_K \mid^{1/2},$$

where $\mathfrak{D}_K$ is the absolute discriminant of K. The lattice $\sigma(M)$ is called the geometric representation of M. Given $x \in M$, we can calculate distances in $\sigma(M) \subset \mathbb{R}^m$ by

$$\mid \sigma(x) \mid^2 = c_K \mathrm{Tr}_{K/\mathbb{Q}}(x\overline{x}),$$

where $c_K = 1$ if K is totally real, $c_K = 1/2$ if K is totally complex, and $\overline{x}$ denotes the complex conjugate of x. The parameter

$$\rho = \frac{1}{2}\min\{|\ \sigma(x)\ |; x \in M, x \neq 0\}$$

is the packing radius of $\sigma(M)$.

A nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is a submodule of $\mathcal{O}_K$ with finite index $N(\mathfrak{a}) = \text{card}(\mathcal{O}_K/\mathfrak{a})$, the norm of $\mathfrak{a}$. The center density of $\sigma(\mathfrak{a})$ is given by

$$\delta(\sigma(\mathfrak{a})) = \frac{2^{r_2}\rho^n}{|\ \mathfrak{D}_K\ |^{1/2}\ N(\mathfrak{a})}. \tag{2}$$

3 Subfields of $\mathbb{Q}(\zeta_p)$ and Their Associated Lattices

The field $L = \mathbb{Q}(\zeta_n)$ is called the n-cyclotomic field. Its degree is $m = \phi(n)$, its ring of integers is $\mathcal{O}_L = \mathbb{Z}[\zeta_n]$, and its discriminant is

$$\mathfrak{D}_L = \pm\frac{n^{\phi(n)}}{\prod_{p|n,\ p\ \text{prime}} p^{\phi(n)/(p-1)}}.$$

When n is prime, Craig studied the geometric representations of the principal ideals $\mathfrak{p}$ of $\mathcal{O}_L$ generated by $1-\zeta_p$ and its powers (see [4, p. 223]). Such geometric representations are lattices in dimensions $n = p-1$, where p is a prime. For their construction, given a fixed prime number p and $i \geq 1$, let $A_{p-1}^{(i)}$ denote the geometric representation of the ideal $\mathfrak{p}^i$. It is known that its norm is p^i, and from [4, p. 223], if $x \in \mathfrak{p}^i$, $i = 1, \ldots, (p-1)/2$, then

$$\text{Tr}_{L/\mathbb{Q}}(x\overline{x}) \geq 2pi. \tag{3}$$

Having this lower bound in mind, the largest value for $\delta(\sigma(\mathfrak{p}^i))$ is obtained by taking $i = \left[\frac{p-1}{2\ln p}\right]$, where $[x]$ denotes the closest integer to x. $\sigma(\mathfrak{p}^i)$ are the densest known lattices for dimensions between 148 and 3000 (see [4, pp. 16-17]).

When studying lattices constructed from the ring of integers of subfields of cyclotomic fields, again the first problem is to determine its volume, which depends on the discriminant of the respective subfield. This is certainly a tedious work, and the discriminant is only known for some particular cases, e.g., the maximal real subfield of a cyclotomic field and some low degree subfields. These classical results were obtained using an integral basis, which for our purposes is an extremely difficult tool to be used. In order to circumvent that difficulty, we calculate the discriminant of the field K explicitly, using Theorem 1. For the case of subfields of $\mathbb{Q}(\zeta_{p^r})$, p prime and $r \geq 1$, we have the following

Theorem 1. *Let K be a subfield of $\mathbb{Q}(\zeta_{p^r})$, with $[K : \mathbb{Q}] = up^j$, where p does not divide u. Then $|\ \mathfrak{D}_K\ | = p^\alpha$, where*

$$\alpha = u \cdot \left((j+2)p^j - \frac{p^{j+1}-1}{p-1}\right) - 1.$$

Proof: See the Appendix. Note that in the particular case where $K \subset \mathbb{Q}(\zeta_p)$ and $[K : \mathbb{Q}] = u$, one has

$$|\mathfrak{D}(K)| = p^{u-1}.$$

Suppose $L = \mathbb{Q}(\zeta_p)$, and let K be the subfield with degree $(p-1)/t$. Let $\mathfrak{p}_K = \mathfrak{p} \cap K$, and $x \in \mathfrak{p}_K^i$. Since $\mathfrak{p}_K$ ramifies completely in L, then $\mathfrak{p}_K^i \mathcal{O}_L = \mathfrak{p}^{ti}$. From (3), if $x \in \mathfrak{p}_K^i$ then $\mathrm{Tr}_{L/\mathbb{Q}}(x\overline{x}) \geq 2pti$, which implies that

$$\mathrm{Tr}_{K/\mathbb{Q}}(x\overline{x}) = \frac{1}{t}\mathrm{Tr}_{L/\mathbb{Q}}(x\overline{x}) \geq \frac{1}{t}2pti = 2pi.$$

A lower bound on the center density is therefore

$$\delta(\mathfrak{p}_K^i) \geq \frac{2^{r_2} \cdot (\sqrt{c_K . 2pi}/2)^{\frac{p-1}{t}}}{p^{\frac{p-1-t}{2t}} \cdot p^i} = \left(\frac{i}{2}\right)^{\frac{p-1}{2t}} p^{\frac{(1-2i)}{2}}. \tag{4}$$

If t and i are fixed, the above expression is a decreasing function of p. Given $n \in \mathbb{N} - \{0\}$, there are infinitely many prime numbers p such that $p \equiv 1 \pmod{n}$. Let p_n be the smallest of them. We denote by $A_n^{(m)}$ the geometric representation of $\mathfrak{p}_K^m = \mathfrak{p}^m \cap K \subseteq \mathcal{O}_K$, where K is the subfield of $\mathbb{Q}(\zeta_p)$ with degree n.

When p and t are fixed, the largest value of the RHS of (3) is achieved for the integer closest to $\frac{p-1}{2t \ln p}$.

Table 1 shows the center density of the lattices $A_n^{(m)}$, for n from 450 up to 573. Note that the lattices obtained from Craig's construction coincide with this family in the dimensions $n = p - 1$, p prime.

Table 1

n	$\log_2 \delta$	n	$\log_2 \delta$	n	$\log_2 \delta$	n	$\log_2 \delta$
450	560.02	481	600.49	512	619.79	543	775.17
451	545.00	482	633.48	513	679.81	544	697.09
452	546.84	483	655.07	514	695.81	545	779.25
453	596.74	484	637.34	515	718.57	546	821.81
454	523.49	485	658.99	516	720.58	547	702.84
455	600.58	486	697.63	517	687.62	548	785.37
456	637.24	487	629.75	518	678.97	549	691.72
457	496.20	488	664.88	519	726.59	550	732.48
458	557.87	489	586.62	520	767.46	551	791.50
459	608.30	490	705.76	521	606.48	552	771.46
460	645.19	491	670.81	522	771.62	553	758.51
461	563.39	492	621.13	523	657.26	554	797.63
462	649.21	493	641.19	524	736.65	555	762.50
463	539.59	494	656.70	525	738.67	556	842.93
464	617.99	495	678.73	526	719.51	557	746.18
465	588.06	496	660.59	527	687.82	558	805.86
466	657.24	497	595.10	528	709.08	559	770.47
467	574.43	498	722.12	529	632.16	560	761.11
468	625.75	499	652.76	530	748.78	561	812.04
469	595.59	500	636.23	531	750.80	562	855.64
470	629.64	501	616.13	532	731.44	563	718.30
471	569.97	502	730.31	533	668.21	564	818.22
472	601.25	503	641.90	534	756.87	565	761.92
473	635.46	504	696.57	535	722.87	566	799.77
474	618.09	505	623.57	536	739.39	567	786.48
475	606.89	506	700.56	537	693.82	568	868.41
476	641.34	507	668.19	538	728.79	569	736.77
477	558.84	508	742.66	539	679.55	570	872.67
478	681.41	509	706.56	540	809.21	571	749.09
479	584.71	510	708.56	541	665.97	572	784.98
480	592.07	511	657.14	542	751.38	573	798.56

Notice that in dimension $n = 510$, the family contains the densest known lattice. The table in [4, p.17], shows that the best lattice in dimension 512 satisfies $\log_2 \delta = 698$.
For higher dimensions, this family presents a good performance, too, as shown by Table 2.

n	$\log_2 \delta$	n	$\log_2 \delta$	n	$\log_2 \delta$
16374	58776.89	16378	57607.94	16382	56319.26
16375	57595.42	16379	56920.87	16383	57628.82
16376	57599.59	16380	59617.02	16384	58057.07
16377	57090.51	16381	57107.10	16385	58823.55

For fixed t, the constructed family satisfies

$$\frac{1}{n}\log_2(\Delta) \geq -\frac{1}{2}\log_2\log_2(n),$$

where Δ is it sphere packing density. Thus it has good asymptotic performance.

4 Conclusions and Final Remarks

We constructed a family of lattices from subfields of cyclotomic fields. By comparing this family with the densest known lattices, we conclude that these are the lattices with the best known density in infinitely many n. In low dimensions, it also contains lattices having the best known densities so far.

Another aspect is the possibility of strict inequality in the equation in (3). Notice that if this happens, then the density of A_n^m is larger than that obtained by the expression in (3). In fact, we have verified that this occurs for $p = 7$ and $p = 11$. For large p, the algorithm is impracticable.

Potential Applications to Coding and Modulation

Recently Giraud and Belfiore [7] proposed a technique for designing signal sets matched to the Rayleigh fading channel. The idea was to use totally real algebraic number fields to obtain appropriate lattice constellations for those channels. Their constellations are constructed up to dimension 8 and one of their main features of is the maximum diversity, i.e., the number of different signal coordinates. However, the performance of these constellations when used over an AWGN Gaussian channel is not so good.

Later on Boutros *et al.* [2] constructed rotated versions of the known lattices Λ_4, Λ_8, K_{12}, and Λ_{16} from $\mathbb{Q}(\zeta_8)$, $\mathbb{Q}(\zeta_{20})$, $\mathbb{Q}(\zeta_{21})$, and $\mathbb{Q}(\zeta_{40})$, respectively. The probability of error for Rayleigh channels is dominated by $\frac{L}{E_b/N_0}$, where L is the diversity [2]. Therefore, in order to obtain constellations good for both Rayleigh fading and Gaussian channels, the idea is to construct dense lattices with maximum diversity. In [2], the presented lattices have maximum center density, however the diversity is half of the dimension.

The present work completes the results in [2], introducing constellations that have maximum diversity and maximum center density for several dimensions, which makes them suitable for use in both channels. The difference between this work and the previous ones is that our constellations are designed for any dimension, high or low.

Appendix

Here we prove Theorem 1. This will be done with the help of the following lemmas.

Lemma 1. *Let p be an odd prime number, r a positive integer and g an integer such that $\bar{g} = g \bmod p^r$ is a generator of $(\mathbb{Z}_{p^r})^*$. Then $g^k \equiv 1 \pmod{p^j}$ if and only if $k \equiv 0 \pmod{(p-1)p^{j-1})}$, for all j such that $0 < j \leq r$.*

Proof: If $g^k = 1 + p^j t$, then $g^{kp} = 1 + p^{j+1} t_1$, where t and t_1 are integers. Repeating this reasoning, we have $g^{kp^{r-j}} = 1 + p^r t_{r-j}$, where t_{r-j} is an integer. With this, we see that if $g^k \equiv 1 \pmod{p^j})$ then $g^{kp^{r-j}} \equiv 1 \pmod{p^r}$ and therefore $(p-1)p^{r-1}$ divides kp^{r-j}, that is, $k \equiv 0 \pmod{(p-1)p^{j-1}}$. Conversely, suppose that $k \equiv 0 \pmod{(p-1)p^{j-1}}$. Then $(\mathbb{Z}_{p^j})^*$ has order $(p-1)p^{j-1}$ and since g and p are relatively prime, we have $g^k \equiv 1 \pmod{p^j}$ which concludes the proof.

Lemma 2. *Let n and m be positive integers and χ a Dirichlet character defined modulo n. The conductor of χ is m if and only if m is the least integer which divides n and satisfies: for all $a \in \mathbb{Z}$ with $(a,n) = 1$, if $a \equiv 1 \pmod{m}$, then $\chi(\bar{a}) = 1$.*

Proof: Suppose that m is the conductor of χ and $a \in \mathbb{Z}$ is such that $(a,n) = 1$. Since $a \equiv 1 \pmod{m}$, then $(a,m) = 1$ and hence $\chi(\bar{a}) = 1$. Conversely, let a and b be relatively prime to n, and consequently relatively prime to m. If $a \equiv b \pmod{m}$ then $ab^{-1} \equiv 1 \pmod{m}$ and thus $\chi(\overline{ab^{-1}}) = 1$, that is, $\chi(\bar{a}) = \chi(\bar{b})$. Since m is the least divisor of n with the above property, then by definition it is the conductor of χ.

Let p be an odd number, r a positive integer, g an integer such that $\bar{g} = g \bmod p^r$ is a generator of $(\mathbb{Z}_{p^r})^*$ and $\chi : (\mathbb{Z}_{p^r})^* \to \mathbb{C}^*$ a Dirichlet character. Given that there are exactly n characters over an Abelian group of order n, then there exist $(p-1)p^{r-1}$ Dirichlet characters χ defined over $(\mathbb{Z}_{p^r})^*$ and each character is completely determined by its image in $\bar{g}$. On the other hand, $1 = \chi(\bar{1}) = \chi(\overline{g^{(p-1)p^{r-1}}}) = \chi(\bar{g})^{(p-1)p^{r-1}}$, that is, $\chi(\bar{g})$ is a $(p-1)p^{r-1}$-th root of unity. With this, given a character χ defined modulo p^r, there exists an integer number i, $0 \leq i \leq (p-1)p^{r-1}$, tal que $\chi(\bar{g}) = \zeta^i_{(p-1)p^{r-1}}$. the Considering the number of characters and the possibilities for the integer i, we can conclude that all the Dirichlet characters defined modulo p^r are of the form $\chi_i(\bar{g}) = \zeta^i_{(p-1)p^{r-1}}$, $i = 1, \ldots, (p-1)p^{r-1}$.

Lemma 3. *With the above notation, given an integer i, $0 \leq i < (p-1)p^{r-1}$, if $p^j = (i, p^r)$, then the conductor f_{χ_i} of χ_i is p^{r-j} .*

Proof: Given a character χ_i defined modulo p^r, let $f_{\chi_i} = p^u$ be its conductor. By Lemma 1, $g^a \equiv 1 \pmod{p^u}$ if and only if $a \equiv 0 \pmod{(p-1)p^{u-1}}$. The character χ_i takes g in $\zeta^i_{(p-1)p^{r-1}}$ and therefore takes g^a in $\zeta^{ai}_{(p-1)p^{r-1}}$. Hence $\chi_i(g^a) = 1$ if and only if $ia \equiv 0 \pmod{(p-1)p^{r-1}}$. If p^{u-1} is the greatest power of p which divides a, then p^{r-u} is the greatest power of p which divides i, that is, $(i, p^r) = p^{r-u}$. For the converse, we apply the same reasoning.

Given an integer n and the field $L = \mathbb{Q}(\zeta_n)$, we know that L is a Galois extension of the field of rational numbers, with Galois group isomorphic to $(\mathbb{Z}_n)^*$. From Galois Theory, it follows

that there exists a one-to-one correspondence between the groups of $(\mathbb{Z}_n)^*$ and the subfields of L. Now, the isomorphism between the Galois group and $(\mathbb{Z}_n)^*$ is constructed by associating to each integer i relatively prime to n, the automorphism σ_i of L which takes ζ_n in ζ_n^i. So we can define a character χ acting on the automorphisms of L, where $\chi(\sigma_i)$ means $\chi(i)$.

With the above notation, if K is a subfield of L, fixed by the group H, we say that a character χ is associated to K if $\chi(\sigma) = 1$, for all σ in H.

As an example, if $K = L$, the subgroup H that fixes K is the identity σ_1 of L. It is easy to see that $\chi(\sigma_1) = 1$, for all χ defined modulo n and therefore all the characters are associated to L. Also, it is not difficult to see that if K is the field of rational numbers then the only character associated to K is the trivial character.

Theorem 2. *[8]: Let n be a positive integer, $L = \mathbb{Q}(\zeta_n)$, H a subgroup of the group of the automorphisms of L and K the subfield of L fixed by H. Then the discriminat of the field K is, up to sign, the product of the conductors of the characters defined modulo n that are associated to K.*

Let p be an odd prime number, r a positive integer and $L = \mathbb{Q}(\zeta_{p^r})$. Since L is a Galois extension of the rationals with Galois group isomorphic to $(\mathbb{Z}_{p^r})^*$, which is a cyclic group, then there is a one-to-one correspondence between the subfields of L and the divisors of $(p-1)p^{r-1}$, the degree of L. In the next lemma, we calculate the discriminant of a subfield K of L as a function of its degree only. Since the degree of K is a divisor of $(p-1)p^{r-1}$, we can suppose $[K:\mathbb{Q}] = up^j$, where u is a divisor of $p-1$.

Theorem 3. *Let K be a subfield of $\mathbb{Q}(\zeta_{p^r})$, with $[K:\mathbb{Q}] = up^j$, where p does not divide u. Then $Disc(K) = p^{u((j+2)\cdot p^j - \frac{p^{j+1}-1}{p-1})-1}$.*

Proof: First, let us observe that $\Gamma = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ is a cyclic group of order $(p-1)p^{r-1}$. So if K is a subfield of $\mathbb{Q}(\zeta_{p^r})$ of degree up^j, then the subgroup H of G that fixes K is cyclic of order $(p-1)p^{j-1}/u$. If σ_a is a generator of H, we can conclude that the character χ defined modulo p^r is associated to K if and only if $\chi(\sigma_a) = 1$. Since the order of a modulo p^r is equal to the order of H, that is, $(p-1)p^{r-1}/u$, we can suppose without loss of generality, that $a \equiv g^s \pmod{p^r}$, where $s = up^j$. Therefore, given a character χ_i defined modulo p^r, we have $\chi_i(\bar{a}) = 1$ if and only if $si \equiv 0 \pmod{(p-1)p^{r-1}}$ or, equivalently, if and only if $i = (p-1)p^{r-1}t/s$, $t = 1, \ldots, s$. By Lemma 3, the conductor f_{χ_i} of χ_i is $p^{r-(r-j-1+v_p(t))}$, that is, $f_{\chi_i} = p^{j+1-v_p(t)}$, where $v_p(t)$ is the greatest number v such that p^v divides t. Given a number ℓ between 0 and j, we have $v_p(t) = \ell$ if and only if $t = p^\ell t_k$, where t_k is a number that ranges between 1 and up^{j-l}, and is relatively prime to p. There are $u(p-1)p^{j-1}$ t_k in these

conditions.

(t, p^j)	number of such t	f_{X_i}
1	$up^{j-1}(p-1)$	p^{j+1}
p^1	$up^{j-2}(p-1)$	p^{j+1-1}
$\vdots$	$\vdots$	$\vdots$
p^{j-1}	$up^0(p-1)$	p^2
	$u-1$	p
p^j	1	1

By Theorem ??, the discriminant of K' is, up to sign, equal to p^α, where

$$\alpha = u\cdot(p-1)\cdot((j+1)p^{j-1}+jp^{j-2}+\cdots+2p^0)+u-1 = \frac{u(p-1)}{p}\sum_{i=0}^{j+1}(i+1)p^i+u-1-u\frac{(p}{}$$

that is,

$$\alpha = \frac{u(p-1)}{p}\cdot\frac{d}{dp}\left(\frac{p^{j+2}-1}{p-1}\right)+u-1-u\cdot\frac{(p-1)}{p} =$$

$$= \frac{u(p-1)}{p}\left(\frac{(j+2)\cdot p^j\cdot(p-1)-(p^{j+2}-1)}{(p-1)^2}\right)+u-1-u\cdot\frac{(p-1)}{p},$$

which implies that

$$\alpha = u\cdot\left((j+2)\cdot p^j-\frac{p^{j+2}-1}{p\cdot(p-1)}+\frac{1}{p}\right)-1$$

and therefore,

$$\alpha = u\cdot\left((j+2)\cdot p^j-\frac{p^{j+1}-1}{(p-1)}\right)-1.$$

Corollary 1. *Given positive integers p and n, where p is an odd prime, the discriminant of the cyclotomic field $\mathbb{Q}(\zeta_{p^r})$ is, up to sign, equal to $p^{(p-1)((r+1)\cdot p^{r-1}-(p^r-1)/(p-1))-1}$.*

References

[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*. New York: Academic Press, 1966.

[2] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, "Good lattice constellations for both Rayleigh fading and Gaussian channels," *IEEE Trans. Inform. Theory*, vol. 42, No. 2, pp. 502-518, March 1996.

[3] A. Cassels, *An Introduction to Geometry of Numbers.* Springer-Verlag, 1971.

[4] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups.* New York: Springer-Verlag, 1988.

[5] M. Craig, "A cyclotomic construction for Leech's lattice," Mathematika, vol. 25, pp. 236-241, 1978.

[6] M. Craig, "Extreme forms and cyclotomy," Mathematika, vol. 25, pp. 44-56, 1978.

[7] X. Giraud and J. C. Belfiore, "Constellations matched to the Rayleigh fading channel," *IEEE Trans. Inform. Theory,* vol. 42, No. 1, pp. 106-115, Jan. 1996.

[8] Hasse,

[9] J. Leech, "Notes on sphere packings," *Canadian J. Math.*, vol. 19, pp. 251-267, 1967.

[10] D. A. Marcus, *Number Fields.* New York: Springer-Verlag, 1977.

[11] T. P. da Nóbrega Neto, "Real cubics and their applications," (in Portuguese), Proc. 6th Joint Algebra Meeting USP/UNICAMP (Campinas, Brazil, June 1997), pp. 59-66.

[12] P. Samuel, *Algebraic Theory of Numbers.* Paris: Hermann, 1970.

[13] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp. 379-423 and pp. 623-656, July and Oct. 1948.

[14] I. N. Stewart and D. O. Tall, *Algebraic Number Theory*, 2nd. edition. London: Chapman & Hall, 1992.

[15] L. C. Washington, *Introduction to Cyclotomic Fields.* New York: Springer-Verlag, 1982.

André Luiz Flores
Department of Telematics
State University of Campinas - UNICAMP
P.O. Box 6101, 13081-970
Campinas, SP, Brazil
e-mail:alflores@dt.fee.unicamp.br

Trajano Pires da Nóbrega Neto
Departamento de Matemática
Universidade Estadual Paulista (UNESP)
Rua Cristóvão Colombo, 2265
P.O.Box 136, 15054-000
São José do Rio Preto, SP, Brazil
e-mail: trajano@mat.ibilce.unesp.br

Trabalho Publicado: Atas do VIII ENAL - novembro de 1999

Reticulados em Subcorpos de $\mathbb{Q}(\zeta_{pq})$

Trajano Nóbrega Neto e André Luíz Flores

Resumo

Neste trabalho, fornecemos um método para o cálculo da densidade de centro de ideais no anel de inteiros de subcorpos de $\mathbb{Q}(\zeta_{pq})$. O método permite a construção de reticulados densos conhecidos em algumas dimensões, e obtemos o reticulado E_8 via o método para diversos corpos $\mathbb{Q}(\zeta_{pq})$.

1 Introdução

A Teoria de reticulados algébricos tem se mostrado extremamente útil para aplicações em Teoria da Informação. Para um canal com ruído gaussiano aditivo, conjuntos de sinais baseados em reticulados densos apresentam bom desempenho. Além disso, Conway e Sloane provaram que reticulados satisfazendo a cota de Minkowski são equivalentes a códigos atingindo a capacidade do canal. Assim, fica estabelecido um vínculo entre empacotamento esférico e Teoria da Informação.

Recentemente, Giraud e Belfiore propuseram uma técnica para obter conjuntos de sinais eficientes para o canal Rayleigh com desvanecimento, ou seja, no canal com ruído multiplicativo. A idéia básica é a rotação de reticulados. Em [1], são construídas versões rotacionadas dos reticulados já existentes D_4, K_{12} e Λ_{16} através de ideais de $\mathbb{Q}(\zeta_{pq})$, para $n = 8$, 21 e 40, respectivamente. Ainda no mesmo trabalho, são utilizadas as construções de Craig, ([3] e [4]), onde são construídos E_6, E_8 e Λ_{24} através de $\mathbb{Q}(\zeta_n)$, para $n = 9$, 20 e 39, respectivamente. As constelações obtidas apresentam bom desempenho em ambos os canais.

Neste trabalho, a ênfase é a construção de reticulados densos a partir de subcorpos de $\mathbb{Q}(\zeta_{pq})$, fornecendo assim novas versões rotacionadas de reticulados densos. Obtemos E_8 via ideais convenientes em subcorpos de $\mathbb{Q}(\zeta_{pq})$. Conjecturamos a existência de um reticulado em dimensão 28 com densidade de centro igual a 1.

2 Preliminares

Sejam K um corpo de números de grau m e $\{\sigma_1, ..., \sigma_m\}$ os $\mathbb{Q}$-monomorfismos de K em $\mathbb{C}$ ordenados de tal forma que σ_i é real, para $1 \leq i \leq r_1$ e σ_{j+r_2} é o conjugado complexo de σ_j, para $r_1 + 1 \leq j \leq r_1 + r_2$. Denotando por $R(z)$ e $I(z)$ a parte real e imaginária do número complexo z, respectivamente, o homomorfismo canônico $\sigma : K \mapsto \mathbb{R}^m$ é o homomorfismo de grupos dado por

$$\sigma(x) = (\sigma_1(x), ..., \sigma_{r_1}(x), R\sigma_{r_1+1}(x), I\sigma_{r_1+1}(x), ..., R\sigma_{r_1+r_2}(x), I\sigma_{r_1+r_2}(x)).$$

Seja $\mathcal{O}_K$ o anel de inteiros algébricos de K e M um submódulo de índice t em $\mathcal{O}_K$. O conjunto $\sigma(M)$ é um reticulado em $\mathbb{R}^m$ de posto m, cujo volume é

$$v(\sigma(M)) = t.2^{-r_2} \mid \mathfrak{D}_K \mid^{1/2},$$

onde $\mathfrak{D}_K$ é o discriminante de K. O reticulado $\sigma(M)$ é chamado de representação geométrica de M. Dado $x \in M$, podemos calcular distâncias em $\sigma(M) \subseteq \mathbb{R}^m$ por

$$\mid \sigma(x) \mid^2 = c_K Tr_{K|\mathbb{Q}}(x\overline{x}),$$

onde $c_K = 1$ se K for totalmente real, $c_K = 1/2$ se K for totalmente complexo e $\overline{x}$ é o conjugado complexo de x. O parâmetro $\rho = \frac{1}{2}\min\{\mid \sigma(x) \mid ; x \in M,\ x \neq 0\}$ é o raio de empacotamento de $\sigma(M)$.

Um ideal $\mathfrak{a} \neq \{0\}$ de $\mathcal{O}_K$ é um submódulo de $\mathcal{O}_K$ de índice $N(\mathfrak{a}) = card(\mathcal{O}_K/\mathfrak{a})$, a norma de $\mathfrak{a}$. Assim, a densidade de centro de um ideal $\mathfrak{a}$ é dada por

$$\delta(\sigma(\mathfrak{a})) = \frac{2^{r_2}\rho^n}{\mid \mathfrak{D}_K \mid^{1/2} N(\mathfrak{a})}. \tag{1}$$

3 A forma quadrática associada a $\mathbb{Q}(\zeta_{pq})$

Será de fundamental importância a forma quadrática Q em n variáveis dada por

$$Q(X_1, ..., X_n) = \sum_{i=1}^{n} X_i^2 + \sum_{1 \leq i < j \leq n} (X_i - X_j)^2.$$

A seguir, explicitaremos a forma quadrática associada a $\mathbb{Q}(\zeta_{pq})$. Antes, porém, precisamos do seguinte

Lema 1. *Valem:*

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

Demonstração. Sejam i, com $(i,pq) = 1$ e r, s tais que $pr + qs = 1$. Temos $\zeta_{pq}^i = \zeta_{pq}^{pri}$. $\zeta_{pq}^{qsi} = \zeta_q^{ri}.\zeta_p^{si}$, onde $(ri,q) = (si,p) = 1$. Então

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_{pq}^i) = Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\zeta_q^{ri}.\zeta_p^{si}) =$$
$$= Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(Tr_{\mathbb{Q}(\zeta pq)/\mathbb{Q}(\zeta_p)}(\zeta_q^{ri}.\zeta_p^{si})) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^{si}.Tr_{\mathbb{Q}(\zeta pq)/\mathbb{Q}(\zeta_p)}(\zeta_q^{ri})) =$$
$$= Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^{si}.Tr_{\mathbb{Q}(\zeta q)/\mathbb{Q}}(\zeta_q^{ri})) = Tr_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(-\zeta_p^{si}) = 1.$$

Para $(i,pq) = p$, existe $k \in \mathbb{Z}$, com $(k,q) = 1$ tal que $\zeta_{pq}^i = \zeta_q^k$. Logo,

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

Para os demais itens, a prova é análoga. □

Corolário 2. *Para $0 \leq i \leq pq$, vale:*

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

Demonstração. No caso $(i,pq)=1$, 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. Para $i=0$, aplicando o Lema 1, temos:

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

Os demais casos seguem de forma análoga. □

Proposição 3. *Sejam $m=\phi(n)$ e $x = a_0 + a_1\zeta_{pq} + \cdots + a_{m-1}\zeta_{pq}^{m-1}$, $a_i \in \mathbb{Z}$, um elemento de $\mathbb{Z}[\zeta_{pq}]$. Então*

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(x\overline{x}) = (p-1)(q-1)\sum_{i=0}^{m-1} a_i^2 + 2.\sum_{i<j} a_ia_j - 2pC_p - 2qC_q,$$

onde $C_i = a_0a_i + a_1a_{i+1} + \cdots + a_{m-1-i}a_{m-1}$.

Demonstração. Para x como no enunciado acima, vale $x\overline{x} = \sum_{i=0}^{m-1} a_i^2 + \sum_{i=1}^{m-1} C_i\alpha_i$, onde $\alpha_i = \zeta_{pq}^i + \zeta_{pq}^{-i}$. Podemos escrever

$$\sum_{i=0}^{m-1} a_i^2 + \sum_{(i,pq)=1} C_i\alpha_i + \sum_{(i,p)=p} C_i\alpha_i + \sum_{(i,q)=q} C_i\alpha_i.$$

Logo,

$$Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(x\overline{x}) = (p-1)(q-1)\sum_{i=0}^{m-1} a_i^2 + \sum_{(i,pq)=1} C_iTr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\alpha_i) +$$
$$+ \sum_{(i,p)=p} C_iTr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\alpha_i) + \sum_{(i,q)=q} C_iTr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(\alpha_i).$$

Aplicando o Lema anterior, uma simples verificação mostra o resultado enunciado. □

A assimetria da forma quadrática acima dificulta muito sua manipulação, sobretudo em subcorpos de $\mathbb{Q}(\zeta_{pq})$. Apresentamos uma técnica de recorrência que facilita esta manipulação.

Sejam $K \subseteq L$ corpos de números, $t = [L:K]$ e σ_K, σ_L os homomorfismos canônicos de K e L, respectivamente, $x \in K$ e c_K, c_L assumindo os valores no conjunto $\{1/2, 1\}$, conforme o corpo em questão seja real ou complexo. Então

$$| \sigma_K(x) |^2 = \frac{c_K}{tc_L} | \sigma_L(x) |^2 .$$

Seja K um subcorpo de $\mathbb{Q}(\zeta_p)$ de índice t e H o grupo dos K-automorfismos de $\mathbb{Q}(\zeta_p)$. Então $K = \mathbb{Q}(\alpha)$, onde $\alpha = \sum_{\sigma \in H} \sigma(\zeta_p)$. Observando a simetria de Q, pondo $u = (p-1)/t$ temos $| \sigma_K(x) |^2 = Tr_{K/\mathbb{Q}}(x\overline{x}) = \frac{1}{t} Tr_{L/\mathbb{Q}}(x\overline{x}) = \frac{1}{2t} Q(a_0, ..., a_0, ..., a_u, ..., a_u)$, onde cada a_i aparece repetido t vezes. Assim chega-se à expressão:

$$| \sigma_K(x) |^2 = \frac{1}{2} \left((a_0^2 + \cdots + a_u^2) + t \sum_{i<j} (a_i - a_j)^2 \right).$$

3.1 Decomposição em $\mathbb{Q}(\zeta_{pq})$

Sejam $L = \mathbb{Q}(\zeta_{pq})$ e $\mathfrak{q}$ um ideal primo de $\mathcal{O}_L$ acima de $q\mathbb{Z}$. É fato conhecido que seu grupo de decomposição depende apenas de q. Sendo assim, este será denotado simplesmente por $\mathcal{D}_L(q)$. Já em $K = \mathbb{Q}(\zeta_p)$, denotaremos o grupo de decomposição de um ideal primo acima de q por $\mathcal{D}_K(q)$. Quando a conjugação complexa não pertence ao grupo de decomposição $\mathcal{D}_L(q)$, então a fatoração de $q\mathcal{O}_L$ tem a forma $q\mathcal{O}_L = (\mathfrak{J}\overline{\mathfrak{J}})^{p-1}$.

Tal propriedade terá consequências que serão estudadas a seguir. Antes disto, daremos a seguinte caracterização:

Teorema 4. *Com a notação acima, então $\theta \in \mathcal{D}_L(q) \Leftrightarrow \theta \in \mathcal{D}_K(q)$, onde θ é a conjugação complexa.*

Demonstração. Seja $\sigma_s \in \mathcal{D}_K(q)$ definido por $\sigma_s(\zeta_p) = \zeta_p^s$. Para cada $\sigma_s \in \mathcal{D}_K(q)$, existem $q-1$ automorfismos $\sigma_{s,i}$ de $\mathcal{D}_L(p)$, $i = 1, ..., q-1$, tais que suas restrições a $\mathbb{Q}(\zeta_p)$ são exatamente σ_s. Cada $\sigma_{s,i}$ é definido por seu valor em ζ_{pq} . Sejam u e v tais que $1 = pu + qv$. Segue que $\sigma_{s,i}(\zeta_{pq}) = \sigma_{s,i}(\zeta_{pq}^{pu+qv}) = \sigma_{s,i}(\zeta_{pq}^{pu})\sigma_{s,i}(\zeta_{pq}^{qv}) = \sigma_{s,i}(\zeta_q^u).\sigma_{s,i}(\zeta_p^v) = \zeta_q^{ui}.\zeta_p^{sv} = \zeta_{pq}^{pui+qsv}$.

Assim, $\theta \in \mathcal{D}_L(q)$ se, e somente se existirem i, s tais que $pui + qsv \equiv -1 \ (mod\ pq)$, que equivale a $pui + qsv \equiv -1 (mod\ p)$ e $pui + qsv \equiv -1 (mod\ q)$. A segunda condição vale sempre, já que i pode assumir qualquer valor não nulo módulo q. Quanto à primeira, esta equivale a $\theta \in \mathcal{D}_K(p)$, o que conclui a prova. □

Corolário 5. *Com a notação acima, vale $\theta \in \mathcal{D}_L(q) \Leftrightarrow Ord_p(q) \equiv 0 \ (mod\ 2)$, onde $Ord_m(n)$ é a ordem de n módulo m, quando $(m,n) = 1$.*

Demonstração. Lembrando que $card(\mathcal{D}_K(q)) = Ord_p(q)$, temos que se $\theta \in \mathcal{D}_K(q)$, então $2 \mid card(\mathcal{D}_K(q)) = Ord_p(q)$. Para a recíproca, suponhamos que $O_p(q) \equiv 0 \ (mod 2)$. Como $\mathcal{D}_K(q)$ é cíclico de ordem par, segue que $\{-1, 1\}$ é o único subgrupo de ordem 2 destes grupos. □

Sejam $x \in \mathbb{Z}[\zeta_{pq}]$ escrito sob a forma $x = \sum_{j=0}^{q-2} \sum_{i=0}^{p-2} a_{ij} \zeta_p^i \zeta_q^j = \sum_{j=0}^{q-2} x_j \zeta_q^j$, onde $x_j = \sum_{i=0}^{p-2} a_{ij} \zeta_p^i$ e $\gamma_q : \mathbb{Z}[\zeta_{pq}] \mapsto \mathbb{Z}[\zeta_p]$ definida por $\gamma_q(x) = \sum_{j=0}^{q-2} x_j$. Analogamente, define-se γ_p :

$\mathbb{Z}[\zeta_{pq}] \mapsto \mathbb{Z}[\zeta_q]$. Seja ainda $\gamma_{pq} : \mathbb{Z}[\zeta_{pq}] \mapsto \mathbb{Z}$ dada por $\gamma_{pq}(x) = \sum_{i,j=0}^{p-2} a_{ij}$. Se $x, y \in \mathbb{Z}[\zeta_{pq}]$ e $a \in \mathbb{Z}$, valem as propriedades:

(i) $\gamma_q(x+y) = \gamma_q(x) + \gamma_q(y)$; (iii) $\gamma_q(xy) \equiv \gamma_q(x)\gamma_q(y) \pmod{qZ[\zeta_p]}$;
(ii) $\gamma_q(ax) = a\gamma_q(x)$; (iv) $\gamma_q(\overline{x}) \equiv \gamma_q(x) \pmod{q}$.

Se $x \in \mathfrak{I} = \mathfrak{p}_1 ... \mathfrak{p}_r \mathfrak{q}_1 ... \mathfrak{q}_s$, então $x\overline{x} \in (1-\zeta_{pq}^p)(1-\zeta_{pq}^q)\mathcal{O}_K$, e verifica-se que

$$\gamma_q(x\overline{x}) \equiv 0 (\mathrm{mod}\, q\mathbb{Z}[\zeta_p]) \text{ e } \gamma_{pq}(x\overline{x}) = \gamma_q(\gamma_p(x\overline{x})) \equiv 0 \pmod{pq}.$$

3.2 Construções algébricas

Construção A - Λ_{24}. A construção algébrica original de Λ_{24} é de [3]. Aqui, fazemos uma nova prova para essa construção. Em $\mathbb{Z}[\zeta_{39}]$ existem 4 ideais primos acima de 3 e dois ideais primos acima de 13, e as decomposições em ideais primos serão $3\mathbb{Z}[\zeta_{39}] = (\mathfrak{p}_1\mathfrak{p}_2\overline{\mathfrak{p}_1\mathfrak{p}_2})^2$ e $13\mathbb{Z}(\zeta_{39}) = (\mathfrak{q}\overline{\mathfrak{q}})^6$.

Proposição 6. *Considerando a decomposição acima, seja o ideal* $\mathfrak{I}=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{q}$ *em* $\mathbb{Z}[\zeta_{39}]$. *Para* $x \in \mathfrak{I}$, *vale* $Tr_{\mathbb{Q}(\zeta_{39})/\mathbb{Q}}(x\overline{x}) \geq 4.39$.

Demonstração. Seja $x \in \mathfrak{I}$, e $x_0, x_1 \in \mathbb{Z}[\zeta_{13}]$ tais que $x = x_0 + x_1\zeta_3$. Sabemos que $Tr_{\mathbb{Q}(\zeta_{39})/\mathbb{Q}}(x\overline{x})$, $x \in \mathfrak{I}$ é par e múltiplo de 39 . Mostraremos que o valor 2.39 não é assumido. Podemos escrever

$$Tr_{\mathbb{Q}(\zeta_{39})/\mathbb{Q}}(x\overline{x}) = Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(x_0\overline{x_0}) + Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(x_1\overline{x_1}) + Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}((x_0-x_1)\overline{(x_0-x_1)}).$$

Para que o valor 2.39 seja atingido, as únicas possibilidades são, a menos de ordem, $Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(x_0\overline{x_0}) = 12$, $Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(x_1\overline{x_1}) = 30$ e $Tr_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}((x_0-x_1)\overline{(x_0-x_1)}) = 36$. As possibilidades para x_0 são, a menos de sinal, as potências $x_0 = \zeta_{13}^i$, $i = 0, ..., 12$. Para x_1, os valores possíveis são $x_1 = \zeta_{13}^{i_1} + \zeta_{13}^{i_2} + \zeta_{13}^{i_3}$ ou $x_1 = \zeta_{13}^{-1} + \zeta_{13}^{i_2} + \zeta_{13}^{i_3}$, onde os $i_{r's}$ são dois a dois distintos.

Consideremos o caso $x_0 = -\zeta_{13}^{i_0}$ e $x_1 = \zeta_{13}^{i_1} + \zeta_{13}^{i_2} + \zeta_{13}^{i_3}$. Temos $((x_0+x_1)\overline{(x_0+x_1)}) \equiv 0$ $(mod\ 3\mathbb{Z}[\zeta_{13}])$, ou seja,

$$(-\zeta_{13}^{i_0} + \zeta_{13}^{i_1} + \zeta_{13}^{i_2} + \zeta_{13}^{i_3})(-\zeta_{13}^{-i_0} + \zeta_{13}^{-i_1} + \zeta_{13}^{-i_2} + \zeta_{13}^{-i_3}) =$$
$$4 - \sum_{s=1}^{3}(\zeta_{13}^{i_0-i_s} + \zeta_{13}^{i_s-i_0}) + \sum_{r,s=1}^{3}\zeta_{13}^{i_r-i_s} \equiv 0 \ (mod\ 3\mathbb{Z}[\zeta_{13}]).$$

Se não existe uma potência $i_t - i_h = -1$, então a equação acima já é uma representação na $\mathbb{Z}$-base canônica de $\mathbb{Z}[\zeta_{13}]$. Neste caso, uma potência não aparecerá repetida 3 vezes, já que os $i_{r's}$ são dois a dois distintos. Suponhamos $i_0 - i_h = 1$ ou -1. Se existirem $r, s \neq 0$ tal que $i_r - i_s = -1$, então $\gamma_{13}((x_0+x_1)\overline{(x_0+x_1)}) \equiv 1$ $(mod\ 3)$. Se para todo $r, s \neq 0$ valer $i_r - i_s \neq -1$, então $\gamma_{13}((x_0+x_1)\overline{(x_0+x_1)}) \equiv 2$ $(mod\ 3)$. Note que o resultado acima vale inclusive para $i_0 = -1$, que é o caso tratado.

Construção B - K_{12}: A construção algébrica de K_{12} em [1] é feita via representação geométrica de um ideal primo acima de 7 em $\mathcal{O}_K$, $K = \mathbb{Q}(\zeta_{21})$. Contudo, o resultado foi obtido computacionalmente. Faremos aqui uma prova formal, baseado sobretudo no seguinte resultado mais geral:

Teorema 7. *Sejam p, q primos tais que $Ord_p(q) \equiv 1 \ (mod\ 2)$ e $q > 2p-3$. Seja ainda $q.\mathbb{Z}[\zeta_{pq}] = (\mathfrak{J}\overline{\mathfrak{J}})^{q-1}$ a decomposição de q em $\mathbb{Q}[\zeta_{pq}]$. Então para $x \in \mathfrak{J}$, vale $Tr_{K/\mathbb{Q}}(x\overline{x}) \geq (p-1).2q$.*

Demonstração. Sejam $x_0,...,x_{p-2} \in \mathbb{Z}[\zeta_q]$ tais que $x = \sum_{i=0}^{p-2} x_i\zeta_p^i \in \mathfrak{J}$. Manipulando algebricamente, obtemos

$$Tr_{K/\mathbb{Q}}(x\overline{x}) = \sum_{i=0}^{p-2} Q_{p-1}(x_i) + \sum_{i<j} Q_{p-1}(x_i - x_j).$$

Se $x_0 = \cdots = x_{p-2}$, então $x = x_0(1 + \zeta_p + \cdots + \zeta_p^{p-2})$, e daí $x_0 \in \mathfrak{J} \cap \mathbb{Z}[\zeta_q]$. Logo, $Tr_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(x_i\overline{x_i}) \geq 2q$, $i = 0, ..., p-2$, e portanto $Tr_{K/\mathbb{Q}}(x\overline{x}) = \sum_{i=0}^{p-2} Q_{p-1}(x_0) \geq (p-1)2q$. Se existirem pelo menos dois valores distintos para os $x_{j's}$, e visto que $Q_{p-1}(x_i) \geq p-1$, então a quantidade de $x_i - x_j$ não nulos é pelo menos $p-2$, e daí $\sum_{i<j} Q_{p-1}(x_i - x_j) \geq (p-2)(p-1)$. Logo, $Tr_{K/\mathbb{Q}}(x\overline{x}) \geq (2p-3)(q-1)$, e sendo $q > 2p-3$, então $Tr_{K/\mathbb{Q}}(x\overline{x}) > (p-2)2q$. Visto que a forma quadrática é par e múltipla de q, então também nesse caso vale $Tr_{K/\mathbb{Q}}(x\overline{x}) \geq (p-1)2q$. □

A norma de $\mathfrak{J}$ vale $N(\mathfrak{J}) = q^{n_1/2}$. A densidade de centro de $\sigma(\mathfrak{J})$ é dada por

$$\delta \geq \frac{((p-1).2q)^{n_1n_2/2}}{p^{n_2(n_1-1)/2}.q^{n_1(n_2-1)/2}q^{n_1/2}.2^{n_1n_2}} = \frac{(\frac{p-1}{2})^{n_1n_2/2}}{p^{n_2(n_1-1)/2}}.$$

Em particular, para $p = 3$, o menor primo satisfazendo às condições $q > 2p-3$ e $Ord_p(q) \equiv 1 \ (mod\ 2)$ é $q = 7$. Para estes primos, temos um reticulado $\sigma(\mathfrak{J})$ em dimensão 12, cuja densidade de centro é $\delta = \frac{1}{3^3}$, justamente a densidade de K_{12}.

Construção C - E_8. Aqui, mostraremos que E_8 está contido em diversos corpos de números. Sejam p e q primos satisfazando às condições $Ord_p(q) \equiv Ord_q(p) \equiv 1 \ (mod\ 2)$ e $K_1 \subseteq \mathbb{Q}(\zeta_p)$, $K_2 \subseteq \mathbb{Q}(\zeta_q)$ tais que $h_p = [\mathbb{Q}(\zeta_p) : K_1]$ e $h_q = [\mathbb{Q}(\zeta_q) : K_2]$ sejam ímpares. Sejam ainda $n_1 = [K_1 : \mathbb{Q}]$ e $n_2 = [K_2 : \mathbb{Q}]$. O corpo K formado pela adjunção $K = K_1K_2$ tem grau n_1n_2, e sendo corpos linearmente disjuntos, seu discriminante é $\mathfrak{D}_K = p^{n_2(n_1-1)}.q^{n_1(n_2-1)}$. Em K, sejam r_p e r_q a quantidade de primos acima de p e q, respectivamente. Vale as decomposições

$$p.\mathcal{O}_K = (\mathfrak{p}_1...\mathfrak{p}_{r_p/2}\overline{\mathfrak{p}_1...\mathfrak{p}_{r_q/2}})^{n_2} \text{ e } q.\mathcal{O}_K = (\mathfrak{q}_1...\mathfrak{q}_{r_q/2}\overline{\mathfrak{q}_1...\mathfrak{q}_{r_q/2}})^{n_1}.$$

Seja $\mathfrak{J} = \mathfrak{p}_1...\mathfrak{p}_{r_p/2}\mathfrak{q}_1...\mathfrak{q}_{r_q/2}$. Sua norma é $N(\mathfrak{J}) = (p^{h_p})^{r_p/2}(q^{h_q})^{r_q/2} = p^{n_2/2}q^{n_1/2}$, e para $x \in \mathfrak{J}$, vale $Tr_{K/\mathbb{Q}}(x\overline{x}) = (\frac{1}{h_ph_q})Tr_{\mathbb{Q}(\zeta_{pq})/\mathbb{Q}}(x\overline{x})$. Como h_p e h_q são ímpares e em $\mathbb{Z}[\zeta_{pq}]$ a forma quadrática é par, então $Tr_{K/\mathbb{Q}}(x\overline{x}) \geq 2pq$.

A expressão para a densidade de centro é

$$\delta = \frac{(2pq)^{n_1n_2/2}}{p^{n_2(n_1-1)/2}.q^{n_1(n_2-1)/2}p^{n_2/2}q^{n_1/2}.2^{n_1n_2}} = \frac{1}{2^{n_1n_2/2}}.$$

Para $n_1n_2 = 8$ a densidade de centro será $\delta = 1/8$, que é a densidade de E_8. Podemos construir E_8 por este método, bastando para isso tomar p, q, n_1 e n_2 convenientes. Assim, descrevemos um método que potencialmente fornece infinitas "versões rotacionadas " de E_8.

Exemplo 8. *Em* $\mathbb{Q}(\zeta_{39})$, *sejam* $K_1 = \mathbb{Q}(\zeta_3)$ *e* K_2 *o subcorpo de* $\mathbb{Q}(\zeta_{13})$ *de grau* 4. *A construção acima no corpo* $K = K_1K_2$ *fornece o reticulado* E_8.

Sejam $p = 7$, $q = 29$, $K_1 = \mathbb{Q}(\sqrt{-7})$ *a extensão quadrática contida em* $\mathbb{Q}(\zeta_7)$ *e* K_2 *o subcorpo de* $\mathbb{Q}(\zeta_{29})$ *de grau* 4. *Novamente temos a construção de* E_8.

Sejam $p = 5$, $q = 31$, $K_1 = \mathbb{Q}(\zeta_5)$ *e* K_2 *o subcorpo de* $\mathbb{Q}(\zeta_{31})$ *de grau* 6. *Se para* $x \in \mathfrak{I} \cap K_1K_2$ *valer* $Tr_{K_1K_2/\mathbb{Q}}(x\overline{x}) \geq 4.p.q$,*então teremos uma versão rotacionada de* Λ_{24}. *Uma outra possibilidade é tomar* K_2 *como sendo a extensão quadrática contida em* $\mathbb{Q}(\zeta_{31})$. *Neste caso, pela Construção 3 obtemos* E_8.

Conjecturamos a construção algébrica de um reticulado em dimensão 28 com densidade de centro igual a 1. O mais denso reticulado conhecido em dimensão 28 tem densidade de centro 2/3 . Convém lembrar que existe um empacotamento não reticulado em dimensão 28 com densidade de centro 1. Uma possível construção é encontrar p e q satisfazendo a condições adequadas.

Referências

[1] Boutros, J. ; Viterbo, E. ; Rastello, C. e Belfiori, J.C. *Good Lattice Constellations for Both Rayleigh Fading and Gaussian Channels*, IEEE Trans. Inform. Theory, V. 42, n.2, mar. 1996.

[2] Borevich, Z.I. and Shafarevich, I.R. *Number Theory*, Ac. Press, 1966.

[3] Craig, M. *A Cyclotomic Construction for Leech's Lattice*, Math. 25, pp. 236-241, 1978.

[4] Craig, M. *Extreme Forms and Cyclotomy*, Math. 25, pp. 44-56, 1978.

[5] Giraud, X. ; Belfiori, J.C., *Constellations Matched to the Rayleigh Fading Channel*, IEEE Trans. Inform. Theory, Vol. 42, n.1, jan. 1996.

[6] Marcus, D.A.: *Number Fields*, Springer-Verlag, 1977.

[7] Samuel, P.: *Algebraic Theory of Numbers*, Hermann, 1970.

[8] Sloane, N.J.A, Conway, J.H. *Sphere Packing, Lattices and Groups*, Springer-Verlag, 1988.

[9] Washington, L.C. *Introduction to Cyclotomic Fields*, Springer-Verlag, 1982.

Trajano Pires da Nóbrega Neto
Departamento de Matemática
Universidade Estadual Paulista (UNESP)
Rua Cristóvão Colombo, 2265
P.O. Box 136, 15054-000
São José do Rio Preto, SP, Brasil
e-mail: trajano@mat.ibilce.unesp.br

André Luíz Flores
Departamento de Telemática
Universidade Estadual de Campinas-UNICAMP
P.O. Box 6101, 13081-970
Campinas, SP, Brasil
e-mail: alflores@dt.fee.unicamp.br