Universidade Estadual de Campinas
Instituto de Matemática, Estatística e
Computação Científica - IMECC
Departamento de Matemática

Abordagem Algébrica e Geométrica de Reticulados

Tatiana Bertoldi Carlos

Tese de Doutorado

Orientadora: **Prof**^{a}. **Dr**^{a}. **Sueli Irene Rodrigues Costa**

Maio - 2007

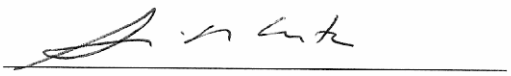
Campinas - SP

[1]Este trabalho contou com apoio financeiro da Fapesp - processos n^o 02/14133 – 8 e 02/07473 – 7

Abordagem Algébrica e Geométrica de Reticulados

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por Tatiana Bertoldi Carlos e aprovada pela comissão julgadora.

Campinas, 09 de Maio de 2007.



Prof^a. Dr^a. Sueli Irene Rodrigues Costa

Orientadora

Banca Examinadora

Prof^a. Dr^a. Sueli Irene Rodrigues Costa (Orientadora)

Prof. Dr. Antonio Aparecido de Andrade (IBILCE/UNESP)

Prof. Dr. Reginaldo Palazzo Júnior (FEEC/UNICAMP)

Prof. Dr. José Plínio de Oliveira Santos (IMECC/UNICAMP)

Prof. Dr. Paulo Roberto Brumatti (IMECC/UNICAMP)

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para obtenção do título de Doutor em Matemática.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP

Bibliotecária: Miriam Cristina Alves - CRB8a / 2116

Carlos, Tatiana Bertoldi

C196a Abordagem algébrica e geométrica de reticulados /Tatiana Bertoldi Carlos – Campinas, [S.P.:s.n.], 2007.

Orientador: Sueli Irene Rodrigues Costa

Tese (doutorado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Teoria dos reticulados 2. Teoria dos grafos. 3. Teoria dos números algébricos. I. Costa, Sueli Irene Rodrigues. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: Algebraic and geometric approaches to lattices

Palavras-chave em inglês (keywords): 1. Lattice theory. 2. Graph theory. 3. Algebraic number theory.

Área de concentração: Geometria discreta

Titulação: Doutora em matemática

Banca examinadora: Prof^a. Dr^a. Sueli Irene Rodrigues Costa (IMECC-UNICAMP)
Prof. Dr. Antonio Aparecido de Andrade (IBILCE-UNESP)
Prof. Dr. Reginaldo Palazzo Júnior (FEEC-UNICAMP)
Prof. Dr. José Plínio de Oliveira Santos (IMECC-UNICAMP)
Prof. Dr. Paulo Roberto Brumatti (IMECC-UNICAMP)

Data da defesa: 09/05/2007

Programa de Pós-Graduação: Doutorado em Matemática

Tese de Doutorado defendida em 09 de maio de 2007 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

Prof. (a). Dr (a). SUELI IRENE RODRIGUES COSTA

Prof. (a). Dr (a). ANTONIO APARECIDO DE ANDRADE

Prof. (a). Dr (a). REGINALDO PALAZZO JÚNIOR

Prof. (a). Dr (a). JOSÉ PLINIO DE OLIVEIRA SANTOS

Prof. (a) Dr. (a). PAULO ROBERTO BRUMATTI

"Feliz aquele que transfere o que sabe e
aprende o que ensina."
Cora Coralina

Ao
Marcos,
dedico.

Agradecimentos

A Deus, por tudo.

À minha orientadora Prof^a. Dr^a. Sueli Irene Rodrigues Costa, sem a qual este trabalho não se realizaria, pela orientação, amizade e motivação nos momentos de dificuldade.

Ao Marcos, pela compreensão, incentivo e apoio nos momentos difíceis.

Aos membros da banca, pelas críticas e sugestões construtivas.

Aos funcionários da secretaria de pós-graduação: Edinaldo, Cidinha e Tânia pela amizade e por todo suporte durante o doutorado.

Aos professores da Universidade Estadual Paulista do Campus de São José do Rio Preto, pela aprendizagem durante a graduação e o mestrado. Em particular, ao Prof. Dr. Antonio Aparecido de Andrade que me orientou no mestrado e também pelas parcerias durante o doutorado.

Ao Prof. Dr. Marcelo Muniz Silva Alves pelas sugestões.

Aos meus pais, minha eterna gratidão, pelo apoio incondicional, pela confiança, por todo amor e incentivo que sempre me deram em tudo que busquei realizar.

À minha grande amiga e irmã de coração, Andréia pela amizade e convivência desde os tempos da graduação.

Aos colegas e amigos João Strapasson e Carina Alves pela interação, discussões e sugestões, que foram fundamentais na conclusão deste trabalho.

Aos amigos, Rogério e Cristiano pela convivência.

Às amigas Flávia, Lidiane e Cristiane pelo apoio e convívio durante esta caminhada que agora se completa.

Ao parecerista FAPESP que acompanhou o desenvolvimento deste trabalho.

À Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) pelo fundamental apoio na iniciação científica, mestrado, doutorado (Processo 02/14133-8) e projeto temático (Processo 02/07473-7) no qual este trabalho se inclui.

Resumo

Neste trabalho abordamos a construção de reticulados usando propriedades da teoria dos números algébricos. Enfocamos particularmente a construção, como reticulado ideal, de rotações do reticulado n-dimensional dos inteiros, usando corpos ciclotômicos. Reticulados desta forma tem se mostrado uma eficiente ferramenta para obtenção de bons esquemas de codificação para canais com desvanecimento, pois permitem estimativas da distância produto e diversidade, parâmetros que controlam a probabilidade de erro no envio de informações por estes canais. Apresentamos uma nova construção de tais reticulados no caso em que n é uma potência de 2, através do subcorpo maximal real do n-ésimo corpo ciclotômico. Estabelecemos também condições para que um reticulado ideal seja rotação do reticulado n-dimensional dos inteiros, usando algoritmos de redução de base, LLL (Lenstra-Lenstra-Lovász) e Minkowski. Outros resultados incluem caracterizações geométricas de grafos circulantes e de alguns reticulados construídos algebricamente.

Abstract

In this work we approach lattice constructions using properties of algebraic number theory. One focus is on the construction of ideal lattices via cyclotomic fields. Those lattices have been used as an efficient tool for designing coding strategies for the Rayleigh fading channels since it is possible to estimate the product distance and the diversity, parameters which control the error probability transmission for those channels. A special case, due to "shaping gain", is when those lattices are rotations of the n-dimensional integer lattice. We present a new construction of such lattices when n is a power of 2, via the maximal sub-field of the n-cyclotomic field. We also establish conditions for an ideal lattice to be a Z^n-lattice using the Minkowski and the LLL (Lenstra-Lenstra-Lovász) reductions. Other results include geometric characterizations of circulant graphs and of some algebraic lattices.

CONTEÚDO

Lista de Símbolos

P_e	probabilidade de erro
$\mathbb{Z}$	conjunto dos números inteiros
$\mathbb{Q}$	conjunto dos números racionais
$\mathbb{R}$	conjunto dos números reais
$\mathbb{C}$	conjunto dos números complexos
L, M, K	corpos de números
L/K	extensão de corpos
$[K : L]$	grau da extensão L/K
$\partial(f(X))$	grau do polinômio f(X)
ζ_n	raiz n-ésima primitiva da unidade
$Gal(L/K)$	grupo de Galois de L sobre K
$\mathcal{O}_K$	anel dos inteiros algébricos de K
r_1	número de mergulhos canônicos reais
r_2	número de mergulhos canônicos complexos
$\mathtt{L}$	diversidade
$N(x)$	norma de x
$Tr(x)$	traço de x
d_{min}	distância mínima
$d_{p,min}$	distância produto mínima
Λ	reticulado no $\mathbb{R}^n$
vol	volume
det	determinante
d_K	discriminante do corpo K
ρ	raio de empacotamente
$\delta(\Lambda)$	densidade de centro de Λ
Δ	densidade de empacotamento esférico
τ	kissing number
$C_n(a_1, \ldots, a_m)$	grafo circulante de n vértices e saltos $a_1, \ldots, a_m$

Introdução

Constelações de sinais tendo estrutura de reticulados são consideradas boas para transmissão de sinais, pois a estrutura linear e altamente simétrica dos reticulados usualmente simplifica a tarefa de decodificação.

O problema de encontrar boas constelações de sinais para um canal de transmissão gaussiano (com distribuição normal de probabilidade de erro) pode ser relacionado ao estudo de empacotamento esférico de reticulados. Constelações com bom desempenho podem ser obtidas de reticulados com alta densidade de empacotamento.

Para a transmissão em um canal com desvanecimento Rayleigh, que modela algumas formas de comunicação sem fio, a idéia básica permanece a mesma. O problema é construir constelações de sinais com energia média mínima para uma desejada taxa de erro, dada a eficiência espectral (número de bits por duas dimensões). Uma interessante abordagem tem sido recentemente proposta, na qual faz-se uso de alguns resultados de teoria dos números algébricos. Usando corpos de números totalmente reais, algumas boas constelações de reticulados casadas a canais com desvanecimento Rayleigh são encontradas. A eficácia dessas constelações está em sua alta diversidade (número de componentes distintas entre dois pontos do reticulado), a qual pode ser obtida como a máxima possível e também na possibilidade de se determinar a distância produto mínima. Diversidade e distância produto mínima são os parâmetros que controlam a probabilidade de erro no envio de informações por estes canais. Constelações de sinais sobre reticulados com estas propriedades e que sejam rotações do reticulado $\mathbb{Z}^n$ são especiais para este tipo de transmissão por terem também "ganho de

forma"(relacionado à energia média).

Constelações de sinais boas para o canal Gaussiano podem ser ruins quando usadas em um canal com desvanecimento Rayleigh, por exemplo se tiverem pequena diversidade. Por outro lado, boas constelações casadas ao canal Rayleigh podem ser ruins quando usadas sobre o canal gaussiano, se a densidade de empacotamento destes reticulados for muito baixa. Assim, um meio para obter constelações eficientes para ambos os canais é buscar reticulados densos com diversidade máxima e distância produto grande.

Com esta motivação, abordamos neste trabalho a construção de reticulados usando propriedades da teoria dos números algébricos. Enfocamos particularmente a construção, como reticulado ideal, de rotações do reticulado n-dimensional dos inteiros, usando corpos ciclotômicos. Apresentamos uma nova construção de tais reticulados no caso em que n é uma potência de 2, através do subcorpo maximal real do n-ésimo corpo ciclotômico. Estabelecemos também condições para que um reticulado ideal seja rotação do reticulado n-dimensional dos inteiros, usando algoritmos de redução de base, LLL (Lenstra-Lenstra-Lovász) e Minkowski. Outros resultados incluem caracterizações geométricas de grafos circulantes e de alguns reticulados construídos algebricamente.

Mais especificamente, este trabalho é organizado como se segue:

No Capítulo 1 são introduzidos conceitos e propriedades que são fundamentais no desenvolvimento e na obtenção dos resultados deste trabalho. São apresentadas as questões relacionadas à busca de constelações de sinais eficientes para transmissão em canais gaussianos e em canais com desvanecimento e uma breve introdução à teoria de reticulados, formas quadráticas, teoria dos números algébricos e construção de reticulados algébricos.

O Capítulo 2 é dedicado ao estudo de uma forma especial de reticulado algébrico, construído a partir de um ideal do anel dos inteiros algébricos de um corpo de números, munido com uma *forma traço*, chamado *reticulado ideal*. Focalizamos duas propriedades: a diversidade e a distância produto mínima. Motivados pelo problema de comunicação descrito no Capítulo 1, para canais com desvanecimento Rayleigh, procuramos por reticulados $\mathbb{Z}^n-$rotacionados com diversidade máxima e distância produto mínima máxima. Apresentamos uma nova construção de tais reticulados no caso em que n é uma potência de 2, através do subcorpo maximal real do n-ésimo corpo ciclotômico. Esta construção é o tema do artigo conjunto "Rotated Lattice via the Cyclotomic Field $\mathbb{Q}(\zeta_{2^r})$"([22]) cujos resultados são

apresentados de forma mais detalhada na Subseção 2.2.2.

O foco do Capítulo 3 é a análise geométrica de reticulados construídos algebricamente. Esta análise parte da redução da base natural obtida da construção de um reticulado algébrico à bases especiais descritas por propriedades da matriz de Gram: reduções de Minkowski e LLL. Estabelecemos condições nestas reduções para que um reticulado seja uma rotação do reticulado de coordenadas inteiras (Teorema 3.1.1) . Através da redução a estas bases especiais foi possível a caracterização geométrica de vários reticulados construídos via corpos ciclotômicos $\mathbb{Q}(\zeta_{p^r})$ e associações com reticulados conhecidos (Seção 3.2). Apresentamos também uma análise comparativa dos parâmetros densidade e distância produto mínima.

No Capítulo 4 abordamos um tema de pesquisa associado a reticulados que é independente dos tratados nos capítulos anteriores, em que também nos envolvemos durante o doutorado. Seu conteúdo é parte integrante do artigo conjunto submetido "Circulant Graphs Viewed as Graphs on Flat Tori"([33]), com alguns detalhamentos. Grafos circulantes têm recebido significativa atenção nas últimas décadas seja teoricamente ou através de suas aplicações na construção de redes de intercomunicação para computação paralela, onde processadores são representados como nós do grafo e os links de comunicação como as arestas conectando-os. A associação que foi feita de grafos circulantes a quocientes de reticulados gerando grafos em toros planares (Proposições 4.1.5 e 4.1.7) permite uma abordagem geométrica para estabelecimento de limitantes para o número de vértices de um grafo circulante com diâmetro d (Seção 4.2). Outros resultados sobre o gênero de grafos circulantes e sobre a associação de grafos circulantes a códigos esféricos também foram obtidos posteriormente a partir desta associação [33], [34] e [35].

CAPÍTULO 1

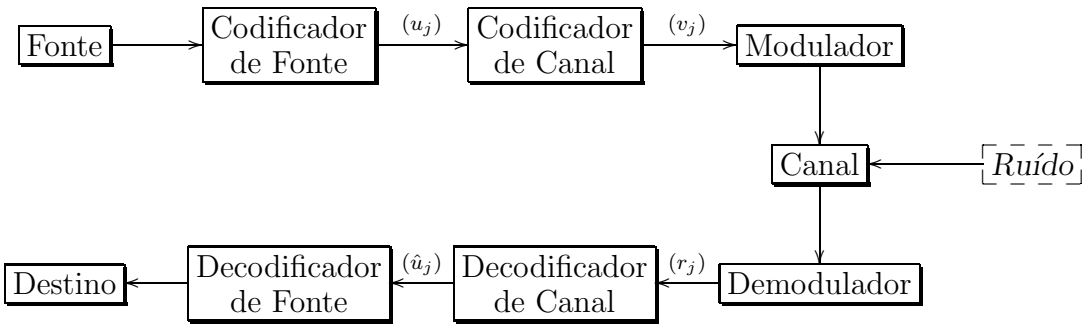
Preliminares

Neste capítulo apresentamos conceitos e resultados relacionados ao conteúdo da tese. Descrevemos o problema da busca de constelações de sinais eficientes para a transmissão em canais gaussianos e com desvanecimento e introduzimos de forma resumida tópicos sobre reticulados, teoria de números algébricos e reticulados algébricos que serão utilizados ao longo deste trabalho. As principais referências utilizadas foram: [1], [2], [3], [4], [5], [6], [8], [10], [11] e [14].

1.1 Sistemas de Comunicação Digital

Apresentamos nesta seção, resumidamente, conceitos básicos sobre sistemas de comunicações. As principais referências foram: [1], [2], [11] e [14].

Descreveremos brevemente o modelo de um típico sistema de transmissão digital (representado por um diagrama de blocos) para depois descrever o que pretendemos analisar neste trabalho.



Num sistema de comunicação digital o objetivo é transmitir dados de uma fonte até um usuário. Para isso, as seguintes etapas estão envolvidas:

- **Fonte** (de informação): pode ser uma pessoa ou uma máquina que gera uma onda sonora contínua ou uma sequência de símbolos de um alfabeto discreto. 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 $\mathcal{A}$.

- **Codificador de fonte**: associa as saídas da fonte às sequências $(u_j) = (u_1, \ldots, u_k)$ de dígitos (geralmente binários) chamadas de sequências de informação ou palavras-código fonte. Tendo em vista a eliminação de redundâncias, nesta etapa deve-se utilizar o menor número possível de dígitos por unidade de tempo para representar a saída da fonte. Além disso, a saída da fonte deve ser reconstruída a partir da sequência de informação associada sem ambiguidades.

- **Codificador de canal**: transforma a palavra-código fonte (u_j) em uma outra sequência $(v_j) = (v_1, \ldots, v_n)$ chamada de palavra-código de canal. Este estágio tem por objetivo inserir redundância à sequência (u_j) visando minimizar a interferência de ruídos no canal.

- **Modulador**: gera formas de ondas que são apropriadas para a transmissão através do canal. O modulador digital transforma símbolos discretos da saída do codificador de canal em um sinal contínuo com duração de T segundos. Para a transmissão, o modulador então associa a cada palavra-código um símbolo analógico, que é então enviado pelo canal.

- **Canal**: é o meio físico por onde a informação é transmitida/armazenada e 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. Alguns exemplos de canais são:

(i) Canais de transmissão: linhas telefônicas, meios de propagação de sinais entre antenas de rádio, meios de propagação de sinais entre antenas de microondas, meios de propagação de sinais entre estações terrestres e satélites, fibras óticas, cabos coaxiais, etc.

(ii) Canais de armazenagem: fitas cassetes, CD's, memórias de computador, etc.

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

$$r = x + n, \tag{1.1}$$

onde $n = (n_1, \ldots, n_n)$ é uma amostra de um processo aleatório gaussiano com variância σ^2.

Um outro canal bastante presente em sistemas de comunicação digital é o *canal com desvanecimento Rayleigh*, que possui ruído multiplicativo. Quando um sinal x é transmitido através de um canal com tal ruído, o sinal recebido é

$$r = \alpha * x + n, \tag{1.2}$$

onde $n = (n_1, \ldots, n_n)$ é o ruído gaussiano e $\alpha = (\alpha_1, \ldots, \alpha_n)$ são 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 $\mathcal{A}$.

- **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 para o possível símbolo enviado.

- **Decodificador de fonte**: associa a palavra-código obtida do decodificador de canal à 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.

1.2 Conceitos sobre o Problema da Comunicação de Sinais

Constelação de sinais tendo estrutura de reticulados são consideradas boas para transmissão de sinais com alta eficiência espectral (número de bits por duas dimensões). O problema de encontrar boas constelações de sinais para um canal de transmissão gaussiano (com distribuição normal de probabilidade de erro) pode ser relacionado ao estudo de empacotamento esférico de reticulados. Constelações com bom desempenho podem ser obtidas de reticulados com alta densidade de empacotamento. A estrutura linear e altamente simétrica dos reticulados usualmente simplifica a tarefa de decodificação.

Para a transmissão em um canal com desvanecimento Rayleigh, que modela algumas formas de comunicação sem fio, a idéia básica permanece a mesma. O problema é construir constelações de sinais com energia média mínima para uma desejada taxa de erro, dada a eficiência espectral. Uma abordagem de sucesso na construção de boas constelações para esse canal baseia-se em resultados de teoria dos números algébricos. Usando corpos de números totalmente reais, algumas boas constelações de reticulados casadas a canais com desvanecimento Rayleigh são encontradas. A eficácia dessas constelações está em sua alta diversidade, a qual é realmente a máxima possível.

Constelações de sinais boas para o canal Gaussiano podem ser ruins quando usadas em um canal com desvanecimento Rayleigh, por exemplo se tiverem pequena diversidade. Por outro lado, as boas constelações casadas ao canal Rayleigh podem ser ruins quando usadas sobre o canal Gaussiano, se a densidade de empacotamento desses reticulados for muito baixa. Assim, um meio para obter constelações eficientes para ambos os canais é buscar reticulados densos com diversidade máxima e distância produto grande.

1.2.1 O Sistema de Transmissão

Quando consideramos transmissões codificadas, palavras-código são vetores reais n-dimensionais $\mathbf{x} = (x_1, \ldots, x_n)$ tomados de alguma constelação de sinal $S \subseteq \mathbb{R}^n$.

Uma m-upla de bits de entrada é associada a um ponto de sinal $\mathbf{x} = (x_1, \ldots, x_n)$ no espaço Euclidiano n-dimensional $\mathbb{R}^n$. Cada ponto é rotulado por um rótulo m-bit binário.

A *eficiência espectral* mede o número de bits por duas dimensões,

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

e a *relação sinal-ruído* por bit 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 de ruído.

Quando usamos códigos reticulados, $\mathbf{x}$ pertence a uma constelação de sinais n-dimensional S (de cardinalidade 2^m) obtida de um conjunto de pontos do reticulado $\Lambda = \{\mathbf{x} = \mathbf{u}M\}$, onde $\mathbf{u}$ é um vetor com coordenadas inteiras e M é a matriz geradora do reticulado, como veremos nas próximas seções. Os bits de informação podem ser usados para rotular as componentes de $\mathbf{u}$ que são inteiras em relação à base do reticulado.

Os pontos da constelação são transmitidos sobre um canal com desvanecimento Rayleigh independente, como descrito em (1.2), isto é,

$$\mathbf{r} = \mathbf{H}\mathbf{x} + \mathbf{n}.$$

Recordamos que $\mathbf{r} = (r_1, \ldots, r_n)$ é o vetor recebido, $\mathbf{n} = (n_1, \ldots, n_n)$ é o vetor ruído, no qual as componentes reais n_i têm média zero, N_0 é a variância gaussiana distribuída e $\mathbf{H} = diag(\alpha_1, \ldots, \alpha_n)$ é a matriz diagonal de desvanecimento do canal, onde os α_i são variáveis aleatórias reais de Rayleigh independentes com segundo momento unitário (i.e., $E[\alpha_i^2 = 1]$), tal que o ganho de potência de canal é assumido normalizado.

Assumindo um CSI (Channel State Information) perfeito, disponível no receptor, a detecção por *Máxima Verossimilhança* (ML) requer a minimização da seguinte métrica

$$m(\mathbf{x}|\mathbf{r}) = \sum_{i=1}^{n} |r_i - x_i|^2, \tag{1.3}$$

para o canal gaussiano, e

$$m(\mathbf{x}|\mathbf{r}, \alpha) = \sum_{i=1}^{n} |r_i - \alpha_i x_i|^2. \tag{1.4}$$

para o canal Rayleigh com desvanecimento.

A minimização de (1.3) e (1.4) pode ser uma operação muito complexa quando se tem um conjunto de sinais arbitrário com um grande número de pontos.

No caso de códigos reticulados, um decodificador ML mais eficiente pode ser feito aplicando o *Decodificador Esférico*, um decodificador universal de reticulados [12].

1.2.2 A Busca por Constelações de Sinais Eficientes

Com o objetivo de obter critérios para a construção de códigos, estimamos a probabilidade de erro do sistema descrito na Seção 1.2.1.

Denotamos por $P_e(S)$ a probabilidade de erro quando enviamos um ponto da constelação de sinais S, e por $P(\mathbf{x} \to \hat{\mathbf{x}})$ a probabilidade de erro par a par, a probabilidade que, quando $\mathbf{x}$ é transmitido, o ponto recebido está mais próximo de $\hat{\mathbf{x}}$ do que de $\mathbf{x}$ de acordo com as métricas definidas em (1.3) e (1.4).

Para uma constelação de sinais arbitrária S, temos

$$P_e(S) = \frac{1}{|S|} \sum_{\mathbf{x} \in S} P_e(S|\mathbf{x} \text{ transmitido}).$$

Isto pode ser bastante simplificado no caso de códigos reticulados. Como um reticulado infinito é *geometricamente uniforme*, a probabilidade de erro quando enviamos um ponto do reticulado é a mesma, $P_e(\Lambda) = P_e(\Lambda|\mathbf{x})$, para qualquer ponto transmitido $\mathbf{x} \in \mathbf{\Lambda}$. Assumiremos então que S é uma constelação finita obtida de Λ.

Agora aplicamos o limitante da união, o qual nos dá um limite superior para a probabilidade de erro do ponto:

$$P_e(S) \leq P_e(\Lambda) = \bigcup_{\hat{\mathbf{x}} \neq \mathbf{x}} P(\mathbf{x} \to \hat{\mathbf{x}}) \leq \sum_{\hat{\mathbf{x}} \neq \mathbf{x}} P(\mathbf{x} \to \hat{\mathbf{x}}) \tag{1.5}$$

A primeira desigualdade leva em conta os efeitos de bordo da constelação finita S comparada ao reticulado infinito Λ.

Para obtermos um limite superior para a probabilidade de erro condicional $P(\mathbf{x} \to \hat{\mathbf{x}}|\alpha)$, observamos que um erro ocorre quando, usando a decodificação com a regra ML (1.4), o ponto recebido $\mathbf{r}$ está mais próximo de $\hat{\mathbf{x}}$ do que de $\mathbf{x}$, isto é, $m(\hat{\mathbf{x}}|\mathbf{r}, \alpha) \leq m(\mathbf{x}|\mathbf{r}, \alpha)$.

Em cada tipo de canal, a expressão acima possibilita a obtenção de fórmulas explícitas para a probabilidade de erro, conforme veremos a seguir.

Para o canal AWGN, por [11], a probabilidade de erro é limitada superiormente por

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

onde τ é o "kissing number"(número de esferas que tocam uma esfera) e d_{min} é a distância mínima do reticulado.

No caso de um canal com desvanecimento Rayleigh, é demonstrado em [2], que a probabilidade de erro para uma relação sinal-ruído grande, satisfaz:

$$P(\mathbf{x} \to \hat{\mathbf{x}}) \leq \frac{1}{2} \prod_{x_i \neq \hat{x}_i} \frac{1}{\frac{(x_i - \hat{x}_i)^2}{8N_0}} = \frac{1}{2} \frac{(8N_0)^\ell}{d_p^{(\ell)}(\mathbf{x}, \hat{\mathbf{x}})^2} \tag{1.6}$$

onde

$$d_p^{(\ell)}(\mathbf{x}, \hat{\mathbf{x}}) = \prod_{x_i \neq \hat{x}_i} |x_i - \hat{x}_i| \tag{1.7}$$

é a *distância ℓ-produto* de $\mathbf{x}$ a $\hat{\mathbf{x}}$ quando esses dois pontos diferem em ℓ componentes. Rearranjando a equação (1.5), obtemos

$$P_e(S) \leq \sum_{\ell=L}^{n} \frac{1}{2} \frac{(8N_0)^\ell}{d_p^{(\ell)}(\mathbf{x}, \hat{\mathbf{x}})^2} \tag{1.8}$$

onde $\mathtt{L}$ é o número mínimo de componentes distintas entre quaisquer dois pontos da constelação, e é chamado *diversidade de modulação* ou *ordem de diversidade* da constelação de sinais, mas diremos simplesmente *diversidade*. Em outras palavras, $\mathtt{L}$ é a distância mínima de Hamming entre quaisquer dois pontos da constelação.

Observamos que os termos dominantes na soma (1.8) são encontrados para $\mathtt{L} = \min(\ell)$. Entre os termos em (1.8) satisfazendo $\mathtt{L} = min(\ell)$, o termo dominante é encontrado para $d_{p,\min} = \min\, d_p^{(\mathtt{L})}$. Assim, para obtermos uma baixa probabilidade de erro assintoticamente, em ordem de relevância temos que:

1. Maximizar a diversidade $\mathtt{L} = \min(\ell)$.
2. Maximizar $d_{p,\min} = \min(d_p^{(\mathtt{L})}(\mathbf{x}, \hat{\mathbf{x}}))$.

Observação 1.2.1. *A diversidade é obviamente limitada pela dimensão n da constelação, e a diversidade máxima é $\mathtt{L} = n$.*

1.2.3 Constelações de Reticulados $\mathbb{Z}^n$ Rotacionados

Na construção de constelações de sinais, dois aspectos fundamentais devem sempre estar em mente: o *rotulamento de bit* e a *forma da constelação*. Essas questões são críticas para

a complexidade das implementações práticas e são estreitamente relacionadas uma com a outra.

O rotulamento de bit consiste em aplicar os bits da entrada a pontos na constelação de sinais. Se queremos evitar o uso de uma grande tabela de procura, para a eficácia do rotulamento de bit, precisamos de um algoritmo simples que aplica bits a sinais. Quando consideramos uma constelação obtida de um reticulado com a forma

$$\mathcal{C} = \{\mathbf{x} = \mathbf{u}M : \mathbf{u} = (u_1, \ldots, u_n) \in S_0^n\} \subset \Lambda,$$

o mais simples algoritmo para rotulamento que podemos usar é obtido executando o rotulamento de bit sobre as componentes inteiras u_i do vetor $\mathbf{u}$. Estes são usualmente restritos à chamada constelação $2^\eta/2$-PAM, $S_0 = \{\pm 1, \pm 3, \ldots, \pm(2^\eta/2 - 1)\}$, onde η é o número de bits por duas dimensões, como definimos anteriormente. O rotulamento de Gray de cada $2^\eta/2$-PAM componente unidimensional é uma eficiente estratégia para reduzir a probabilidade de erro. Se nos restringirmos ao algoritmo simples de rotulamento acima, observamos que isto induz a uma forma da constelação similar ao paralelepípedo fundamental do reticulado base.

Por outro lado, sabemos que tais constelações limitadas por uma esfera tem o melhor "ganho de forma" (em termos de energia média). Infelizmente, rotular uma constelação de forma esférica não é sempre uma tarefa fácil, sem usar uma tabela de busca. Assim, uma boa alternativa é escolher um reticulado no qual a forma do paralelepípedo fundamental não possa induzir muita perda de energia.

Constelações de reticulados com forma cúbica são boas candidatas: elas são ligeiramente piores em termos do ganho de forma, pois estes reticulados não são os mais densos em suas dimensões, mas são usualmente mais fáceis de rotular e decodificar.

Logo, podemos concluir resumindo algumas razões pelas quais códigos reticulados podem originar bons códigos para o modelo de canal com desvanecimento considerado.

1. O cálculo da probabilidade de erro mostra que a diversidade é o primeiro parâmetro a ser otimizado e o segundo é a distância produto. Precisamos construir constelações em altas dimensões, com máxima diversidade e distância produto e reticulados tendo uma estrutura conveniente para tratar deste problema, mesmo que para n grande.

2. A complexidade do decodificador é outro aspecto importante. O princípio da máxima

verossimilhança pode ser modelado eficientemente para códigos reticulados usando decodificador esférico.

3. Como observado anteriormente, códigos em reticulados isomorfos a $\mathbb{Z}^n$ oferecem um bom equilíbrio entre boa forma e facilidade de rotulamento.

Portanto, nosso objetivo agora é a construção de tais $\mathbb{Z}^n$ reticulados com diversidade máxima e ótima distância produto mínima. Esta construção pode ser feita, como veremos no próximo capítulo, através do conceito de *reticulados ideais*.

1.3 Teoria de Reticulados

Nesta seção revisaremos alguns conceitos e propriedades da teoria de reticulados que serão utilizados também com o objetivo de introduzir a notação adotada. A principal referência usada para este tópico foi [11].

Definição 1.3.1. *Seja $\mathbf{v}_1, \ldots, \mathbf{v}_m$ um conjunto de vetores linearmente independentes em $\mathbb{R}^n$. O conjunto de pontos*

$$\Lambda = \{\mathbf{x} = \sum_{i=1}^{m} \lambda_i \mathbf{v}_i,\ \lambda_i \in \mathbb{Z}\}$$

é chamado um **reticulado** *de dimensão m, e $\mathbf{v}_1, \ldots, \mathbf{v}_m$ é chamado uma base do reticulado.*

Um reticulado é um conjunto discreto de pontos no $\mathbb{R}^n$, pois é formado por combinações lineares inteiras de $\mathbf{v}_1, \ldots, \mathbf{v}_m$, e é um subgrupo de $(\mathbb{R}^n, +)$, pois a soma ou diferença de dois vetores no reticulado ainda estão nele.

Definição 1.3.2. *A região formada pelos pontos*

$$\mathcal{R} = \{x \in \mathbb{R}^n : x = \theta_1 \mathbf{v}_1 + \cdots + \theta_m \mathbf{v}_m,\ 0 \leq \theta_i < 1\}$$

é chamada uma **região** *ou um* **"paralelepípedo" fundamental** *do reticulado.*

Se $m = n$, a região fundamental é um "paralelepípedo" que ladrilha o $\mathbb{R}^n$ por translações de elementos do reticulado. Em cada paralelepípedo transladado haverá um único ponto do reticulado.

Existem muitas maneiras diferentes de escolher uma base para um dado reticulado.

Sejam as coordenadas dos vetores da base

$$\begin{aligned}\mathbf{v}_1 &= (v_{11}, v_{12}, \ldots, v_{1n}),\\ \mathbf{v}_2 &= (v_{21}, v_{22}, \ldots, v_{2n}),\\ &\ldots\\ \mathbf{v}_m &= (v_{m1}, v_{m2}, \ldots, v_{mn})\end{aligned}$$

onde $n \geq m$.

Definição 1.3.3. *A matriz*

$$M = \begin{pmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ & & \ddots & \\ v_{m1} & v_{m2} & \ldots & v_{mn} \end{pmatrix}$$

é chamada uma **matriz geradora** *para o reticulado. Duas matrizes M e $\tilde{M}$ geram o mesmo reticulado se, e somente se, $M = H\tilde{M}$, onde H é uma matriz $m \times m$ com elementos inteiros e determinante ± 1. A matriz $G = MM^T$ é chamada uma* **matriz de Gram** *para o reticulado, onde T denota a transposição.*

Como M contém os vetores da base do reticulado $\{\mathbf{v}_i\}_{i=1}^m$, a (i, j)-ésima entrada da matriz G é o produto interno $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = \mathbf{v}_i \cdot \mathbf{v}_j^T$.

Os pontos do reticulado são formados por

$$\Lambda = \{\mathbf{x} = \lambda M | \lambda \in \mathbb{Z}^m\}.$$

Definição 1.3.4. *O* **determinante** *do reticulado Λ é definido como sendo o determinante da matriz G*

$$det(\Lambda) = det(G).$$

Este é um invariante do reticulado, pois não depende da escolha da base.

Um reticulado é dito ter *posto máximo* se $m = n$, e neste caso M é uma matriz quadrada. Assim,

$$det(\Lambda) = (det(M))^2.$$

A raiz quadrada do determinante de G é o volume de um paralelepípedo fundamental, também chamado *volume do reticulado*, e denotado por $vol(\Lambda)$.

Definição 1.3.5. *Seja B uma matriz $n \times n$ com entradas inteiras. Um* **sub-reticulado** *de Λ é dado por*

$$\Lambda' = \{\mathbf{x} = \lambda BM | \lambda \in \mathbb{Z}^m\}.$$

Como um reticulado tem estrutura de grupo, um sub-reticulado Λ' é então um subgrupo de Λ, e tal que, podemos considerar o grupo quociente Λ/Λ'.

O índice do sub-reticulado Λ' é a cardinalidade do grupo quociente Λ/Λ' e

$$|\Lambda/\Lambda'| = \frac{vol(\Lambda')}{vol(\Lambda)} = |det(B)|.$$

É sempre possível encontrar um sub-reticulado de um dado reticulado considerando sua *versão escalonada* por um fator inteiro.

Dado um reticulado Λ, um *reticulado escalonado* Λ' pode ser obtido multiplicando os vetores do reticulado por uma constante, isto é, $\Lambda' = c\Lambda$ onde $c \in \mathbb{R}$. Assim, Λ' é um sub-reticulado de Λ quando $c \in \mathbb{Z}$.

Mais geralmente, temos a seguinte definição.

Definição 1.3.6. *Se um reticulado pode ser obtido de outro por rotações, reflexões ou multiplicação por um escalar, dizemos que eles são* **equivalentes**.

Mais precisamente, duas matrizes geradoras M e M' definem reticulados equivalentes se, e somente se, eles são descritos por $M' = cUMB$, onde c é uma constante não nula, U é uma matriz com entradas inteiras e determinante ± 1 e B é uma matriz real ortogonal. As correspondentes matrizes de Gram são relacionadas por $G' = c^2 UGU^T$.

Assim, temos que ter em mente que mesmo reticulados equivalentes podem ser representados de diferentes maneiras. Como uma das consequências, dada uma matriz de Gram, não é fácil determinar qual é o reticulado correspondente. Invariantes como a dimensão e o determinante poderão ajudar, mas um dos cuidados que temos que ter é que o mesmo determinante é condição necessária mas não suficiente para garantir que dois reticulados são congruentes por movimento rígido. Essas considerações serão importantes mais tarde, quando construiremos constelações de reticulados algébricos que são rotações de reticulados conhecidos, o que permitirá ganho de diversidade e distância produto.

1.3.1 Empacotamento Reticulado

Um *empacotamento esférico* em $\mathbb{R}^n$ é uma distribuição de esferas de mesmo raio em $\mathbb{R}^n$ de tal forma que estas esferas tenham no máximo um ponto em comum (que chamaremos simplemente de empacotamento). Pode-se descrever um empacotamento indicando o conjunto dos centros das esferas e o raio destas. Um *empacotamento reticulado* é um empacotamento em que o conjunto dos centros formam um reticulado Λ de $\mathbb{R}^n$.

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

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

$$d_{min}^2 = \min\{||v||^2; v \in \Lambda, v \neq 0\}$$

está bem definido.

Podemos observar que $\rho = d_{min}/2$, o *raio de empacotamento*, é o maior raio dentre os quais é possível distribuir esferas centradas nos pontos de Λ e obter um empacotamento. Assim, quando falamos em densidade do reticulado Λ, ficará implícito que estamos falando da densidade do empacotamento com esferas de raio ρ associado a este reticulado, e esta será denotada por $\Delta(\Lambda)$.

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

$$\Delta(\Lambda) = \frac{\text{volume de uma esfera}}{\text{volume da região fundamental}} = \frac{vol(B(\rho))}{vol(\Lambda)} = \frac{vol(B(1))\rho^n}{vol(\Lambda)},$$

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

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

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

1.3.2 Exemplos de Famílias de Reticulados

1) Reticulado n-dimensional cúbico $\mathbb{Z}^n$

$$\mathbb{Z}^n = \{(x_1, \ldots, x_n) : \ x_i \in \mathbb{Z}\}$$

é o reticulado n-dimensional "cúbico"inteiro. Como matriz geradora M pode ser tomada a matriz identidade de ordem n. Então $det(\mathbb{Z}^n) = 1$, e $\mathbb{Z}^n$ tem vetor de norma mínima igual a 1. Seu raio de empacotamento é $\rho = 1/2$, densidade de centro $\delta = 2^{-n}$ e kissing number $\tau = 2n$.

2) O Reticulado n-dimensional A_n

$$A_n = \{(x_0, x_1, \ldots, x_n) \in \mathbb{Z}^{n+1} : \ x_0 + \cdots + x_n = 0\}.$$

Duas possíveis matrizes de Gram são

$$\begin{bmatrix} 2 & -1 & 0 & \cdots & 0 & 0 \\ -1 & 2 & -1 & \cdots & 0 & 0 \\ 0 & -1 & 2 & \cdots & 0 & 0 \\ & & & \ddots & & \\ 0 & 0 & 0 & \cdots & 2 & -1 \\ 0 & 0 & 0 & \cdots & -1 & 2 \end{bmatrix}, \quad \begin{bmatrix} 2 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 1 & \cdots & 1 \\ 1 & 1 & 2 & \cdots & 1 \\ & & \ddots & & \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 1 & \cdots & 2 \end{bmatrix}.$$

Assim, para A_n temos: $det(A_n) = n + 1$, vetor de norma mínima igual a 2, raio de empacotamento $\rho = 1/\sqrt{2}$, densidade de centro $\delta = 2^{n/2}(n+1)^{-1/2}$ e kissing number $\tau = n(n+1)$.

3) O Reticulado n-dimensional D_n

Para $n \geq 3$,

$$D_n = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : \ x_0 + \cdots + x_n \text{ par}\}.$$

Uma matriz de Gram é dada por

$$\begin{bmatrix} 2 & 0 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 2 & -1 & 0 & \cdots & 0 & 0 \\ -1 & -1 & 2 & -1 & \cdots & 0 & 0 \\ & & & \ddots & & & \\ 0 & 0 & 0 & 0 & \cdots & -1 & 2 \end{bmatrix}.$$

Logo, para D_n temos: $det(D_n) = 4$, vetor de norma mínima igual a 4, raio de empacotamento $\rho = 1/\sqrt{2}$, densidade de centro $\delta = 2^{-(n+2)/2}$ e kissing number $\tau = 2n(n-1)$.

1.4 Formas Quadráticas e Reticulados

Definição 1.4.1. *Sejam $\mathbb{K}$ um corpo de característica diferente de 2, e V um espaço $\mathbb{K}$-vetorial. Dizemos que a aplicação q de V em $\mathbb{K}$ é uma* **forma quadrática** *se as seguintes condições são satisfeitas:*
(1) Para todo $\lambda \in \mathbb{K}$ e $x \in V$ temos

$$q(\lambda x) = \lambda^2 q(x).$$

(2) Se $b(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y))$ então b é uma **forma bilinear simétrica**, *isto é, $b(x+x',y) = b(x,y) + b(x',y)$ e $b(\lambda x, y) = \lambda b(x,y)$ para todo $\lambda \in \mathbb{K}$, x, x' e $y \in V$ (as condições são similares sobre a segunda variável, pois $b(y,x) = b(x,y)$).*

A identidade $b(x,x) = q(x)$ nos permite obter q de b.

No caso em que $\mathbb{K} = \mathbb{R}$, dizemos que q é *definida positiva* se para todo $x \in V$, $x \neq 0$, temos $q(x) > 0$.

Seja $(\mathbf{w}_i)_{1 \leq i \leq n}$ uma $\mathbb{Z}$-base de L. Se $\mathbf{x} = \sum_{1 \leq i \leq n} x_i \mathbf{w}_i \in \Lambda$, com $x_i \in \mathbb{Z}$, a definição de forma quadrática implica que

$$q(\mathbf{x}) = \sum_{1 \leq i,j \leq n} q_{i,j} x_i x_j \quad \text{com} \ , \ q_{i,j} = b(\mathbf{w}_i, \mathbf{w}_j)$$

onde b denota a forma bilinear simétrica associada a q.

A matriz $Q = (q_{i,j})_{1 \leq i,j \leq n}$ é então uma matriz simétrica que é definida positiva quando q é definida positiva. Temos que $b(\mathbf{x}, \mathbf{y}) = Y^T Q X$ e em particular $q(\mathbf{x}) = X^T Q X$, onde X e Y

são os vetores colunas dando as coordenadas de $\mathbf{x}$ e $\mathbf{y}$ respectivamente na base $(\mathbf{w}_i)$. Assim, $Q = (q_{i,j})_{1\leq i,j\leq n}$ é a matriz de Gram de L.

Seja Λ um reticulado n-dimensional do espaço $\mathbb{R}^n$, com base $(\mathbf{v}_i)_{1\leq i\leq n}$, formando as linhas da matriz geradora M.

Como vimos na seção (1.3), dado um vetor qualquer do reticulado $\mathbf{x} = (x_1, \ldots, x_n) \in \Lambda$, temos

$$\mathbf{x} = \zeta_1\mathbf{v}_1 + \cdots + \zeta_n\mathbf{v}_n = \zeta M,$$

onde os $\zeta = (\zeta_1, \ldots, \zeta_n),\ \zeta_i \in \mathbb{Z}$.

Quando estudamos reticulados, definimos *norma* de um vetor do reticulado, como seu comprimento ao quadrado. Logo, a norma do vetor $\mathbf{x}$ é

$$||\mathbf{x}||^2 = ||\zeta_1\mathbf{v}_1 + \cdots + \zeta_n\mathbf{v}_n||^2 = \sum_{i=1}^{n}\sum_{j=1}^{n}\zeta_i\zeta_j\mathbf{v}_i\cdot\mathbf{v}_j = \zeta MM^t\zeta^t = \zeta A\zeta^t = f(\zeta),$$

onde $A = MM^T$ é a matriz de Gram de Λ. Considerada como uma função de n variáveis inteiras $\zeta_1, \ldots, \zeta_n$, $f(\zeta)$ é uma forma quadrática associada ao reticulado.

Exemplo 1.4.1. *Uma matriz geradora do reticulado hexagonal é dada por*

$$M = \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}.$$

A matriz de Gram $A = MM^T$ é

$$A = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}.$$

Assim, uma forma quadrática associada ao reticulado hexagonal é

$$\zeta_1^2 + \zeta_1\zeta_2 + \zeta_2^2.$$

Exemplo 1.4.2. *O reticulado cúbico n-dimensional $\mathbb{Z}^n$ tem matriz geradora I_n (matriz identidade de ordem n), e sua correspondente forma quadrática é*

$$\zeta_1^2 + \zeta_2^2 + \cdots + \zeta_n^2.$$

1.5 Teoria dos Números Algébricos

Nesta seção recordaremos alguns conceitos básicos de teoria dos números algébricos. Todos os corpos considerados aqui são subcorpos do corpo dos números complexos $\mathbb{C}$. Omitiremos as demonstrações, que podem ser encontradas nas referências [3], [4], [5] e [6].

1.5.1 Conceitos Básicos

Sejam K e L subcorpos dos números complexos $\mathbb{C}$. Se L é um subcorpo de K, dizemos que o corpo K é uma extensão do corpo L, a qual denotaremos por K/L. A dimensão de K visto como espaço vetorial sobre L é chamado de *grau* de K sobre L, denotado por $[K : L]$. Se $[K : L]$ é finita, dizemos que K é uma extensão finita de L.

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

Sejam K/L uma extensão de corpos, e $\alpha \in K$. Se existe um polinômio mônico irredutível $f(X) \in L[X]\backslash\{0\}$ tal que $f(\alpha) = 0$, dizemos que α é um *número algébrico* sobre L. O polinômio de menor grau com tais propriedades é chamado de *polinômio minimal* de α sobre L.

Todo corpo de números K é da forma $K = \mathbb{Q}(\theta)$ para algum número algébrico $\theta \in K$. Assim, K é um $\mathbb{Q}$-espaço vetorial gerado por potências de θ. Se K tem grau n então $\{1, \theta, \ldots, \theta^{n-1}\}$ é uma base de K e o grau do polinômio minimal de θ sobre $\mathbb{Q}$ é n, isto é, $\partial(f(X)) = n$.

Se o polinômio minimal de θ sobre $\mathbb{Q}$ tem todas as suas raízes em K, dizemos que K é uma *extensão de Galois* de $\mathbb{Q}$. O conjunto dos automorfismos do corpo $Gal(K/\mathbb{Q}) = \{\sigma : K \to K | \sigma(x) = x, \forall x \in \mathbb{Q}\}$ é um grupo, chamado o *grupo de Galois* de K sobre $\mathbb{Q}$.

Definição 1.5.1. *Dizemos que α é um* **inteiro algébrico** *se for raiz de um polinômio mônico com coeficientes em $\mathbb{Z}$. O conjunto dos inteiros algébricos de K é um anel chamado o* **anel dos inteiros algébricos** *de K, e denotado por $\mathcal{O}_K$.*

Teorema 1.5.1. *[3] Seja K um corpo de números de grau n. O anel $\mathcal{O}_K$ de K é um $\mathbb{Z}$-módulo livre de posto $[K : \mathbb{Q}]$, isto é, existe uma base livre de n elementos sobre $\mathbb{Z}$.*

Definição 1.5.2. *Seja $\{\omega_1, \ldots, \omega_n\}$ uma base livre do $\mathbb{Z}$-módulo $\mathcal{O}_K$. Assim podemos escrever univocamente qualquer elemento de $\mathcal{O}_K$ como $\sum_{i=1}^{n} a_i\omega_i$, com $a_i \in \mathbb{Z}$. Uma base livre $\{\omega_1, \ldots, \omega_n\}$ do $\mathbb{Z}$-módulo $\mathcal{O}_K$ é chamada de* **base integral** *de K .*

Definição 1.5.3. *Sejam K e L duas extensões de um corpo $\mathbb{F}$. Um homomorfismo de corpos $\varphi : K \to L$ é dito ser um* $\mathbb{F}$**-homomorfismo** *se para todo $a \in \mathbb{F}$ tem-se que $\varphi(a) = a$ (isto é, $\varphi|_{\mathbb{F}}$ é a identidade de $\mathbb{F}$).*

Observação 1.5.1. *Todo homomorfismo $\varphi : K \to L$ de subcorpos de $\mathbb{C}$ é um $\mathbb{Q}$-homomorfismo e como φ é injetivo podemos chamá-lo de* **mergulho**.

O próximo teorema nos diz a respeito de homomorfismo entre tais corpos.

Teorema 1.5.2. *Sejam L, K subcorpos de $\mathbb{C}$ com K sendo extensão de L e $[K : L] = n < \infty$. Então, existe $\theta \in K$ tal que $K = L(\theta)$ e existem exatamente n L-homomorfismos de K em $\mathbb{C}$, $\sigma_i : K \to \mathbb{C}$, $i = 1, \ldots, n$, tal que $\sigma_i(\theta) = \theta_i$, onde θ_i são as raízes distintas em $\mathbb{C}$ do polinômio minimal de θ sobre L.*

Assumindo que $\theta = \theta_1$, note que $\sigma_1(\theta) = \theta_1 = \theta$ e assim σ_1 é a aplicação identidade, $\sigma_1(k) = k$, para todo $k \in K$. Quando aplicamos o mergulho σ_i a um elemento arbitrário $x \in K$, $x = \sum_{k=1}^{n} a_k\theta^k, a_k \in L$, usando as propriedades de L-homomorfismo temos

$$\sigma_i(x) = \sigma_i(\sum_{k=1}^{n} a_k\theta^k) = \sum_{k=1}^{n} \sigma_i(a_k)\sigma(\theta)^k = \sum_{k=1}^{n} a_k\theta_i^k \in \mathbb{C}$$

e temos que a imagem de x sobre σ_i é univocamente identificada por θ_i.

Definição 1.5.4. *Sejam $L \subseteq K$ subcorpos de $\mathbb{C}$, $[K : L] = n$, $\sigma_1, \ldots, \sigma_n$ os n mergulhos de K em $\mathbb{C}$ e $x \in K$. Os elementos $\sigma_1(x), \sigma_2(x), \ldots, \sigma_n(x)$ são chamados os* **L-conjugados** *de x e*

$$N_{K/L}(x) = \prod_{i=1}^{n} \sigma_i(x), \quad Tr_{K/L}(x) = \sum_{i=1}^{n} \sigma_i(x)$$

são chamados, respectivamente, a **norma** *e o* **traço** *de x da extensão L/K.*

Observação 1.5.2. *Quando $L = \mathbb{Q}$, vamos denotar $N_{K/\mathbb{Q}}(x)$ e $Tr_{K/\mathbb{Q}}(x)$ simplesmente por $N(x)$ e $Tr(x)$.*

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

1. $Tr_{K/L}(x)$ e $N_{K/L}(x) \in L$;
2. $Tr_{K/L}(x+y) = Tr_{K/L}(x) + Tr_{K/L}(y)$;
3. $Tr_{K/L}(ax) = aTr_{K/L}(x)$;
4. $Tr_{K/L}(a) = na$;
5. $N_{K/L}(xy) = N_{K/L}(x).N_{K/L}(y)$;
6. $N_{K/L}(a) = a^n$.

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

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

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

Em particular, se $x \in K$, então

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

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

Proposição 1.5.1. *[8] Para qualquer $x \in K$, temos $N(x)$ e $Tr(x) \in \mathbb{Q}$. Se $x \in \mathcal{O}_K$, temos $N(x)$ e $Tr(x) \in \mathbb{Z}$.*

Definição 1.5.5. *Seja $\{\omega_1, \ldots, \omega_n\}$ uma base integral de $\mathcal{O}_K$. O* **discriminante** *de K é definido como $d_K = det[\sigma_j(\omega_i)]^2$.*

O discriminante independe da escolha da base.

Teorema 1.5.3. *[4] O discriminante d_K de um corpo de números pertence a $\mathbb{Z}$.*

Observe que se $K/\mathbb{Q}$ e $\sigma : K \to \mathbb{C}$ é um mergulho então $\bar{\sigma} : K \to \mathbb{C}$, definido por $\bar{\sigma}(x) = \overline{\sigma(x)}$ é também um mergulho, e mais ainda, $\sigma \neq \bar{\sigma}$ se, e somente se, $\sigma(K) \nsubseteq \mathbb{R}$.

Definição 1.5.6. *Sejam $\sigma_1, \sigma_2, \ldots, \sigma_n$ os n mergulhos de K em $\mathbb{C}$. Sejam r_1 o número de mergulhos com imagem em $\mathbb{R}$ e r_2 o número de mergulhos cujas imagens não estão contidas em $\mathbb{R}$, e que, dois a dois, não são conjugados. Assim,*

$$n \ = \ r_1 \ + \ 2r_2.$$

O par (r_1, r_2) é chamado a *assinatura* de K. Se $r_2 = 0$ dizemos que o corpo de números é *totalmente real*. Se $r_1 = 0$ dizemos que o corpo de números é *totalmente complexo*.

Definição 1.5.7. *Consideremos os $\sigma_i's$ tal que, para todo $x \in K$, $\sigma_i(x) \in \mathbb{R}$, $1 \leq i \leq r_1$, e $\bar{\sigma}_i(x)$, é o conjugado complexo de $\sigma_i(x)$ para $r_1 + 1 \leq i \leq r_1 + r_2$. Chamamos de* **mergulho canônico** *$\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ o isomorfismo definido por*

$$\sigma(\alpha) \;=\; (\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), \sigma_{r_1+1}(\alpha), \ldots, \sigma_{r_1+r_2}(\alpha)) \quad \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

Se identificarmos $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ com $\mathbb{R}^n$, o mergulho canônico pode ser reescrito como $\sigma : K \to \mathbb{R}^n$

$$\sigma(\alpha) \;=\; (\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), \Re\sigma_{r_1+1}(\alpha), \Im\sigma_{r_1+1}(\alpha), \ldots, \Re\sigma_{r_1+r_2}(\alpha), \Im\sigma_{r_1+r_2}(\alpha)) \quad \in \mathbb{R}^n,$$

onde $\Re$ é a parte real e $\Im$ é a parte imaginária.

O mergulho canônico nos fornece uma representação geométrica de um corpo de números, que como veremos está associada a um reticulado.

1.5.2 Corpo Ciclotômico

Um elemento $\zeta \in \mathbb{C}$ é chamado uma *raiz n-ésima da unidade* se $\zeta^n = 1$, n inteiro, $n \geq 1$, e é dito *raiz primitiva n-ésima da unidade* se $\zeta^n = 1$ mas $\zeta^d \neq 1$ para qualquer $1 \leq d < n$.

As raízes n-ésimas da unidade são raízes do polinômio $X^n - 1$.

O número complexo ζ^m é uma raiz primitiva n-ésima da unidade se, e somente se, $mdc(m, n) = 1$, isto é, o número de raízes primitivas n-ésimas da unidade é $\varphi(n)$, onde φ é a função de Euler.

Função de Euler: Se $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ então o número de inteiros positivos menores ou iguais a n e coprimos com n é dado por:

$$\varphi(n) = p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r - 1}(p_1 - 1) \cdots (p_r - 1).$$

Dado n um inteiro positivo, definimos $\zeta_n = e^{\frac{2\pi i}{n}}$ e o corpo $L = \mathbb{Q}(\zeta_n)$ é chamado o *n-ésimo corpo ciclotômico*.

O polinômio $\phi_n(X) = \prod_{\substack{j=1,\\ mdc(j,n)=1}}^{n} (X - \zeta_n^j)$ é chamado o *n-ésimo polinômio ciclotômico*, ele é o polinônimo minimal de ζ, isto é, o polinômio com coeficientes inteiros de menor grau, mônico e irredutível, que tem ζ como raiz.

Lema 1.5.1. *Se n é um inteiro positivo, então*

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

Como consequência do Lema 1.5.1 temos que

$$\phi_n(X) = \frac{X^n - 1}{\prod_{d/n,\ d<n} \phi_d(X)}.$$

Quando $n = p$, onde p é um número primo, segue que

$$\phi_p(X) = X^{p-1} + \cdots + X + 1$$

que é chamado de *p-ésimo polinômio ciclotômico.*

Quando $n = p^r$,

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

Teorema 1.5.4. *[5] Se $\zeta_n \in \mathbb{C}$ é uma raiz primitiva n-ésima da unidade, então $L = \mathbb{Q}(\zeta_n)$ é uma extensão de Galois de $\mathbb{Q}$, cujo grupo de Galois, $Gal(L/\mathbb{Q})$ é canonicamente isomorfo a $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$ (grupo das unidades de $\mathbb{Z}/n\mathbb{Z}$) e portanto abeliano de ordem $\varphi(n)$.*

Observamos que o grau da extensão $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ é igual à ordem de $Gal(L/\mathbb{Q})$, e portanto igual a $\varphi(n)$.

Seja $L = \mathbb{Q}(\zeta)$, sendo $\zeta = \zeta_p$ uma raiz primitiva p-ésima da unidade, p um número primo. Então $[L : \mathbb{Q}] = p - 1$ e os números $1, \zeta, \ldots, \zeta^{p-2}$ formam uma base de L sobre $\mathbb{Q}$, sendo que $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ são as raízes do polinômio ciclotômico $\phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$.

O grupo de Galois $Gal(L|\mathbb{Q})$ consiste dos $p - 1$ automorfismos $\sigma_1, \ldots, \sigma_{p-1}$, sendo σ_j univocamente determinado por

$$\sigma_j(\zeta) = \zeta^j \ , \quad j = 1, \ldots, p - 1.$$

Em particular, σ_1 é a identidade de L.

Proposição 1.5.2. *[5] Sejam ζ uma raiz primitiva p-ésima da unidade, e p um número primo. Para $j = 1, \ldots, p-1$, temos:*

$$\begin{aligned} &Tr(\zeta^j) = -1, \quad Tr(\zeta^j - 1) = -p, \quad Tr(1 - \zeta^j) = p, \\ &N(\zeta^j) = 1, \qquad N(\zeta^j - 1) = p, \qquad N(1 - \zeta^j) = p. \end{aligned}$$

Teorema 1.5.5. *[3] Sejam p um número primo e ζ_p uma raiz p-ésima primitiva da unidade em $\mathbb{C}$. Então o anel dos inteiros de $L = \mathbb{Q}(\zeta_p)$ é*

$$\mathcal{O}_L = \mathbb{Z}[\zeta_p] = \{a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2};\ a_i \in \mathbb{Z}\}$$

onde $\{1, \zeta, \ldots, \zeta^{p-2}\}$ é base livre do $\mathbb{Z}$-módulo $\mathbb{Z}[\zeta]$.

Proposição 1.5.3. *Seja $K = \mathbb{Q}(\zeta_p)$, sendo ζ_p uma raiz primitiva p-ésima da unidade, onde p é um número primo ímpar. Então o discriminante, d_K, é dado por*

$$d_K = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

Considere o corpo ciclotômico $\mathbb{Q}(\zeta_{p^r})$, onde p é um primo ímpar e r é um inteiro positivo.

O grupo $\left(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\right)^*$ é cíclico de ordem $\varphi(p^r) = (p-1)p^{r-1}$. O isomorfismo entre $Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ e $\left(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\right)^*$ é dado pela aplicação $\sigma_a \to \bar{a}$, com $0 < a \leq p^r$ e $mdc(a, p^r) = 1$. Daí $Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ também é cíclico de ordem $\varphi(p^r)$.

O teorema fundamental de Galois garante que existe uma correspondência entre os subcorpos de $\mathbb{Q}(\zeta_{p^r})$ e os subgrupos de $\left(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\right)^*$, ela associa a cada subcorpo K de $\mathbb{Q}(\zeta_{p^r})$ ao subgrupo H de $Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ formado pelos automorfismos de $\mathbb{Q}(\zeta_{p^r})$ que fixam K.

Como o $Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ é cíclico, dado um divisor d de $\varphi(p^r)$, existe um único subcorpo K de $\mathbb{Q}(\zeta_{p^r})$ de grau d e tal corpo é fixado pelo único subgrupo H de $Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ de índice d, ou seja, $H = Gal(\mathbb{Q}(\zeta_{p^r})/K)$ e $(Gal(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}) : H) = d$. Logo, $[K : \mathbb{Q}] = d$.

Assim, como o grau de K sobre $\mathbb{Q}$ é um divisor próprio de $\varphi(p^r) = (p-1)p^{r-1}$, podemos escrever $[K : \mathbb{Q}] = up^j$, onde $j = 0, 1, \ldots, r-1$ e u divide $p-1$.

O próximo teorema nos fornece o discriminante absoluto do corpo K, nas condições citadas acima.

Teorema 1.5.6. *[18] Sejam p um primo ímpar, r um inteiro positivo e K um subcorpo de $\mathbb{Q}(\zeta_{p^r})$, com $[K:\mathbb{Q}] = up^j$, onde $u|(p-1)$. Então o discriminante, d_K, é dado por*

$$|d_K| = p^{u[(j+2)p^j - \frac{p^{j+1}-1}{p-1}]-1}.$$

Corolário 1.5.1. *Se p é um primo ímpar e r um inteiro positivo, então o discriminante do corpo ciclotômico $\mathbb{Q}(\zeta_{p^r})$ é dado por*

$$|d_{\mathbb{Q}(\zeta_{p^r})}| = p^{(p-1)[(r+1)p^{r-1} - \frac{p^r-1}{p-1}]-1}.$$

Observação 1.5.3. *A diferença no cálculo do discriminante de subcorpos de $\mathbb{Q}(\zeta_{2^r})$ consiste no fato de que o grupo de Galois de $\mathbb{Q}(\zeta_{2^r})$ sobre $\mathbb{Q}$ não é cíclico, daí não existe a unicidade do caso primo ímpar, podendo haver dois ou mais subcorpos de mesmo grau com diferentes discriminantes. Neste caso, dado um divisor d do grau de $\mathbb{Q}(\zeta_{2^r})$, temos que analisar se o subcorpo K de $\mathbb{Q}(\zeta_{2^r})$ de grau d é ciclotômico ou não.*

Teorema 1.5.7. *[19] Seja K o corpo ciclotômico de $\mathbb{Q}(\zeta_{2^m})$, subcorpo de $\mathbb{Q}(\zeta_{2^r})$, de grau 2^{m-1} e corpo fixo de $H = \langle \bar{5}^{2^{m-2}} \rangle$, onde $|H| = 2^{r-m}$. Então $|d_K| = 2^{(m-1)2^{m-1}}$. No caso em que o corpo intermediário é K, corpo fixo de $H = \langle -\bar{1}, \bar{5}^{2^{m-1}} \rangle$, não ciclotômico, então $|d_K| = 2^{m2^{m-1}-1}$.*

Exemplo 1.5.1. *Sejam $L = \mathbb{Q}(\zeta_{p^r})$ e $K = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$ o subcorpo maximal real de L. O polinômio minimal de ζ_{p^r} sobre K é $f(X) = X^2 + (\zeta_{p^r} + \zeta_{p^r}^{-1})X + 1$, logo ζ_{p^r} e $\zeta_{p^r}^{-1}$ são raízes de $f(X)$ e $\partial(f(X)) = 2$. Assim, $[L:K] = 2$ e $[K:\mathbb{Q}] = \varphi(p^r)/2 = (p-1)p^{r-1}/2$. Pelo Teorema (1.5.6), $u = (p-1)/2$ e $j = r-1$, temos*

$$|d_K| = p^{\frac{1}{2}((p-1)(r+1)p^{r-1} - p^r - 1)}.$$

1.5.3 Reticulados Algébricos

A definição de mergulho canônico estabelece uma correspondência um a um entre os elementos do corpo de números algébricos de grau n e vetores do espaço Euclidiano n-dimensional. O passo final para a construção de um reticulado algébrico é dado pelo resultado a seguir.

Teorema 1.5.8. *[3] Sejam $\{\omega_1, \ldots, \omega_n\}$ uma base integral de K e $\sigma : K \to \mathbb{C}$ o mergulho canônico. Os n vetores $\mathbf{v}_i = \sigma(\omega_i) \in \mathbb{R}^n$, $i = 1, \ldots, n$ são linearmente independentes e definem um reticulado em $\mathbb{R}^n$, denominado* **reticulado algébrico** *de posto máximo, $\Lambda = \sigma(\mathcal{O}_K)$.*

Sabemos que o reticulado $\Lambda = \sigma(\mathcal{O}_K)$ pode ser expresso por meio de sua matriz geradora M.

$$\Lambda = \{\mathbf{x} = \lambda M \in \mathbb{R}^n \mid \lambda \in \mathbb{Z}^n\}$$

A *matriz geradora* do reticulado é dada por

$$M = \begin{pmatrix} \sigma_1(\omega_1) & \ldots & \sigma_{r_1}(\omega_1) & \Im\sigma_{r_1+1}(\omega_1) & \Re\sigma_{r_1+1}(\omega_1) & \ldots & \Re\sigma_{r_1+r_2}(\omega_1) & \Im\sigma_{r_1+r_2}(\omega_1) \\ \sigma_1(\omega_2) & \ldots & \sigma_{r_1}(\omega_2) & \Im\sigma_{r_1+1}(\omega_2) & \Re\sigma_{r_1+1}(\omega_2) & \ldots & \Re\sigma_{r_1+r_2}(\omega_2) & \Im\sigma_{r_1+r_2}(\omega_2) \\ & & & & \vdots & & & \\ \sigma_1(\omega_n) & \ldots & \sigma_{r_1}(\omega_n) & \Im\sigma_{r_1+1}(\omega_n) & \Re\sigma_{r_1+1}(\omega_n) & \ldots & \Re\sigma_{r_1+r_2}(\omega_n) & \Im\sigma_{r_1+r_2}(\omega_n) \end{pmatrix}, \tag{1.9}$$

onde os vetores $\mathbf{v}_i$ são as linhas de M.

Teorema 1.5.9. *[3] O* volume fundamental *do reticulado $\Lambda = \sigma(\mathcal{O}_K)$ é*

$$vol(\Lambda) = |det(\mathbf{M})| = 2^{-r_2}\ \sqrt{|d_K|}$$

onde $d_K = det[\sigma_j(\omega_i)]^2$ é o discriminante absoluto *do corpo.*

Relembramos que a *diversidade* de um reticulado $\Lambda \in \mathbb{R}^n$ é o número de componentes distintas entre quaisquer dois pontos não nulos do reticulado. O teorema a seguir nos fornece a diversidade de um reticulado algébrico, a partir do corpo de número usado para sua construção.

Teorema 1.5.10. *[2] Os reticulados algébricos exibem diversidade*

$$\mathtt{L} \ = \ r_1 + r_2.$$

Demonstração: Seja $\mathbf{x} \neq \mathbf{0}$ um ponto arbitrário de Λ

$$\mathbf{x} = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \ldots, \Im\sigma_{r_1+r_2}(x)),$$

com $x \in \mathcal{O}_K$, isto é, $x = \sum_{i=1}^{n} \lambda_i \omega_i$, para $\lambda_i \in \mathbb{Z}$ e $\{\omega_1, \ldots, \omega_n\}$ uma base integral de $\mathcal{O}_K$.

Como $\mathbf{x} \neq \mathbf{0}$, temos que $x \neq 0$ e os r_1 primeiros coeficientes são não nulos. O número mínimo de coeficientes não nulos entre os $2r_2$ coeficientes que estão a esquerda é r_2, pois as partes real e imaginária de qualquer um dos mergulhos não podem ser nulas ao mesmo tempo. Asssim, temos que a diversidade $\mathtt{L} \geq r_1 + r_2$. Aplicando o mergulho canônico a $x = 1$, temos exatamente $r_1 + r_2$ coeficientes não nulos, pois $\sigma_j(1) = 1, \forall j$, o que conclui a prova. ■

Corolário 1.5.2. *Um reticulado algébrico construído sobre um corpo de números totalmente real, o qual tem assinatura* $(r_1, r_2) = (n, 0)$*, tem diversidade máxima* $\mathtt{L} = n$*. Além disto, sua distância n-produto mínima satisfaz* $d_{p,min} \geq 1$*.*

De fato, sua matriz geradora é dada por

$$M = \begin{pmatrix} \sigma_1(\omega_1) & \sigma_2(\omega_1) & \dots & \sigma_n(\omega_1) \\ \sigma_1(\omega_2) & \sigma_2(\omega_2) & \dots & \sigma_n(\omega_2) \\ \vdots & \vdots & & \vdots \\ \sigma_1(\omega_n) & \sigma_2(\omega_n) & \dots & \sigma_n(\omega_n) \end{pmatrix}.$$

A *distância n-produto* de $\mathbf{x}$ a $\mathbf{0}$ é

$$\begin{aligned} d_p^{(n)}(\mathbf{0}, \mathbf{x}) &= \prod_{j=1}^{n} |x_j| = \prod_{j=1}^{n} \left| \sum_{i=1}^{n} \lambda_i v_{ij} \right| = \prod_{j=1}^{n} \left| \sum_{i=1}^{n} \lambda_i \sigma_j(\omega_i) \right| \\ &= \prod_{j=1}^{n} \left| \sigma_j \left(\sum_{i=1}^{n} \lambda_i \omega_i \right) \right| = \left| N \left(\sum_{i=1}^{n} \lambda_i \omega_i \right) \right| = |N(x)| \geq 1, \end{aligned}$$

onde $x \in \mathcal{O}_K$.

Note que para reticulados algébricos de corpos de números arbitrários com assinatura (r_1, r_2) e com matriz geradora (1.9), a distância produto não pode ser relacionada com a norma algébrica. Como $x \neq 0$, temos pela Proposição 1.5.1,

$$d_p(\mathbf{0}, \mathbf{x}) \geq 1 \ , \quad \forall \ \mathbf{x} \neq \mathbf{0}$$

Assim a *distância produto mínima* do reticulado algébrico $\Lambda = \sigma(\mathcal{O}_K)$ é

$$d_{p,min} = \min_{x \in \Lambda} d_p^{(n)}(\mathbf{0}, \mathbf{x}) = 1.$$

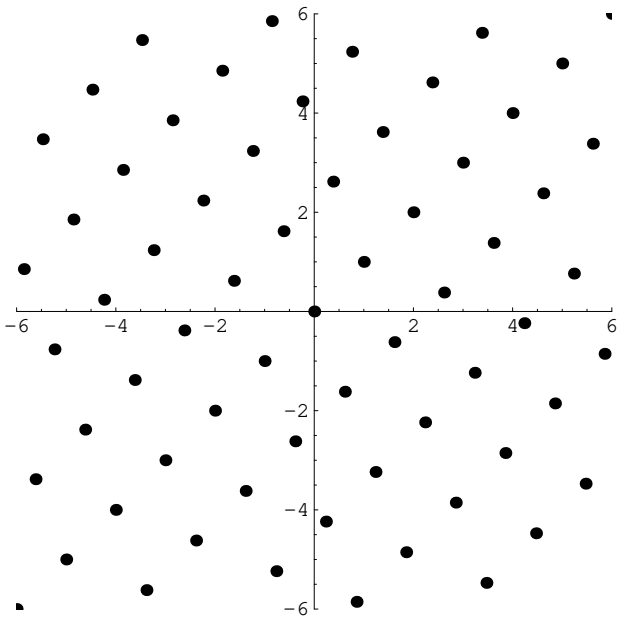


Figura 1.1: Reticulado algébrico obtido de $K = \mathbb{Q}(\sqrt{5})$

Exemplo 1.5.2. *Construiremos o reticulado algébrico obtido de* $K = \mathbb{Q}(\sqrt{5})$*. O anel dos inteiros algébricos de* K *é* $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{5})/2]$*, e uma base integral para* $\mathcal{O}_K$ *é* $\{1, 1+\sqrt{5})/2\}$*. Como* K *é totalmente real então* $r_1 = 2$*, e portanto, a diversidade é máxima, isto é,* $\mathtt{L} = 2$*. Os mergulhos canônicos são* $\sigma_1(\sqrt{5}) = \sqrt{5}$ *e* $\sigma_2(\sqrt{5}) = -\sqrt{5}$ *e a matriz geradora do reticulado é*

$$M = \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1\left(\frac{1+\sqrt{5}}{2}\right) & \sigma_2\left(\frac{1-\sqrt{5}}{2}\right) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \left(\frac{1+\sqrt{5}}{2}\right) & \left(\frac{1-\sqrt{5}}{2}\right) \end{pmatrix}.$$

O volume de $\Lambda(\mathcal{O}_K)$ *é* $\sqrt{5}$*, e a norma mínima, isto é,* d^2_{min} *é* 2*.*

Assim, temos o reticulado gerado pelos vetores $\{(1,1), (\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2})\}$ *em* $\mathbb{R}^2$*, ver Figura 1.1.*

Até aqui, o ingrediente chave para a construção de reticulados algébricos tem sido a existência de uma $\mathbb{Z}$-base livre em K. Como sabemos que $\mathcal{O}_K$ tem tal base, pois $\mathcal{O}_K$ é um $\mathbb{Z}$-módulo livre de posto n, podemos mergulhá-lo em $\mathbb{R}^n$ para obter um reticulado algébrico. Porém, existem outros subconjuntos de $\mathcal{O}_K$ que também têm esta estrutura de $\mathbb{Z}$-módulo livre de posto n, são os ideais de $\mathcal{O}_K$.

Definição 1.5.8. *Um* **ideal** $\mathcal{I}$ *de um anel comutativo* R *é um subgrupo aditivo de* R *o qual*

é estável sob a multiplicação por R, isto é, $a\mathcal{I} \subset \mathcal{I}$ para todo $a \in R$. Um ideal $\mathcal{I}$ é **principal** *se ele é da forma $\mathcal{I} = (x) = xR = \{xy,\ y \in R\},\ x \in \mathcal{I}$.*

Definição 1.5.9. *Dizemos que um ideal $\mathcal{I}$ é* **primo** *se ele satisfaz a seguinte propriedade: se $xy \in \mathcal{I}$ então $x \in \mathcal{I}$ ou $y \in \mathcal{I}$.*

A noção de ideal pode ser estendida como a seguir.

Definição 1.5.10. *Um* **ideal fracionário** *$\mathcal{I}$ é um $\mathcal{O}_K$-submódulo de K tal que existe $d \in \mathcal{O}_K \setminus \{0\}$ com $\mathcal{I} \subseteq d^{-1}\mathcal{O}_K$.*

Teorema 1.5.11. *[4] Todo ideal $\mathcal{I} \neq 0$ de $\mathcal{O}_K$ tem uma $\mathbb{Z}$-base livre, $\{v_1, \ldots, v_n\}$ onde n é o grau de K.*

Definição 1.5.11. *Seja $\mathfrak{a}$ um ideal de $\mathcal{O}_K$. Sua norma é definida por $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$.*

Segue diretamente que se $\mathfrak{a} = a\mathcal{O}_K$ é principal, então $N(\mathfrak{a}) = |N_{K/\mathbb{Q}}(a)|$.

Proposição 1.5.4. *[3] Seja $\mathcal{I}$ um ideal inteiro de $\mathcal{O}_K$. Então $\Lambda = \sigma(\mathcal{O}_K)$ e $\Lambda' = \sigma(\mathcal{I})$ são reticulados, e o volume de Λ' é dado por*

$$vol(\Lambda') = 2^{-r_2} N(\mathcal{I}) \sqrt{d_K}. \tag{1.10}$$

A expressão para *densidade de centro* destes reticulados assume a forma

$$\delta(\sigma(\mathcal{I})) = \frac{2^{r_2}\rho^n}{|d_K|^{1/2} N(\mathcal{I})}, \tag{1.11}$$

onde ρ é o raio de empacotamento do reticulado.

Exemplo 1.5.3. *Como vimos no Exemplo 1.5.2, o reticulado algébrico obtido de $K = \mathbb{Q}(\sqrt{5})$, tem matriz de Gram*

$$G = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}.$$

A distância mínima deste reticulado é $\sqrt{2}$ e portanto $\rho = d_{min}/2 = \sqrt{2}/2$, $r_2 = 0$ e $d_K = |det(M)|^2 = det(G) = 5$. Então sua densidade de centro é $\delta = 1/2\sqrt{5} = 0.223607....$ Observe que a densidade de centro de A_2, o reticulado mais denso em dimensão 2, é $\delta = 0.288675$ e a de $\mathbb{Z}^2$ é $\delta = 0.25$. Logo, este reticulado é menos denso que $\mathbb{Z}^2$, porém sua diversidade $\mathtt{L} = 2$ é maior.

Exemplo 1.5.4. *Sejam $K = \mathbb{Q}(\zeta_3)$ e $x = a + b\zeta_3 \in \mathcal{O}_K$. Temos*

$$N(x) = \sigma_1(x)\sigma_2(x) = (a + b\zeta_3)(a + b\zeta_3^2) = a^2 + b^2 - ab.$$

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

$$|\sigma(x)|^2 = a^2 + b^2 - ab = N(x).$$

Considere $\mathfrak{a} = x\mathcal{O}_K$. Então todo $y \in \mathfrak{a}$ é da forma $y = kx$, com $k \in \mathcal{O}_K$. Assim,

$$|\sigma(y)|^2 = |\sigma(kx)|^2 = N(kx) = N(k)N(x) \geq N(x),$$

pois $|N(k)| \geq 1$. Logo, o menor valor assumido por $|\sigma(y)|^2$, para $y \in \mathfrak{a}$ e $y \neq 0$, é $|N(x)|$. Portanto,

$$\rho = \frac{\sqrt{|N(x)|}}{2},$$

e a densidade de centro é

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

Observe que neste caso particular o anel dos inteiros $\mathbb{Z}[\zeta_3]$ é principal, logo a densidade de centro independe da escolha do ideal. O reticulado obtido é A_2, o mais denso em dimensão 2.

Sabemos que para todo $n \in \mathbb{Z}$, existe uma única fatoração em números primos. Esta noção de fatoração não é verdadeira em geral para anéis de inteiros, mas é substituída de modo análogo para ideais.

Teorema 1.5.12. *[3] Todo ideal $\mathcal{I}$ de $\mathcal{O}_K$ pode ser escrito de forma única como um produto de potências de ideais primos:*

$$\mathcal{I} = \prod_{i=1}^{m} \mathcal{B}_i^{e_i}$$

Para ideais fracionários as potências e_i que aparecem na fatoração podem ser negativas. A teoria de ramificação investiga como os ideais primos de $\mathbb{Z}$ comportam-se quando considerados como ideais de $\mathcal{O}_K$.

Definição 1.5.12. *Seja $p \in \mathbb{Z}$. Considere $\mathfrak{p} = p\mathbb{Z}$, um ideal primo de $\mathbb{Z}$. Usando o Teorema 1.5.12, $p\mathcal{O}_K = \prod_{i=1}^{m} \mathcal{B}_i^{e_i}$. O inteiro e_i é chamado* **índice de ramificação** *de $\mathcal{B}_i$. Se $e_i \geq 2$ para algum i, dizemos que $\mathfrak{p}$ se ramifica em $\mathcal{O}_K$. Se $p\mathcal{O}_K = \mathcal{B}^n$, dizemos que $\mathfrak{p}$ é* **totalmente ramificado** *em $\mathcal{O}_K$. No caso especial onde $K/\mathbb{Q}$ é uma extensão de Galois, $e_i = e$ para todo i.*

Exemplo 1.5.5. *Seja $\mathbb{Q}(\zeta)$, onde $\zeta = \zeta_p$, com p um primo ímpar e ζ uma p-ésima raiz da unidade. O polinômio minimal de K é dado por $\phi_p(X) = X^{p-1} + \cdots + X + 1$. Como temos que $\phi_p(X) = \prod_{k=1}^{p-1}(X - \zeta^k)$, avaliando o polinômio em $X = 1$, obtemos que $p = \prod_{k=1}^{p-1}(1 - \zeta^k)$. Usando o fato de que $\mathcal{O}_K = \mathbb{Z}[\zeta]$, temos $p\mathbb{Z}[\zeta] = \prod_{k=1}^{p-1}(X - \zeta^k)$, onde $(1 - \zeta^k)$ é um ideal de $\mathbb{Z}[\zeta]$. Assim, como $1 - \zeta^k | 1 - \zeta$ e reciprocamente $1 - \zeta | 1 - \zeta^k$, a igualdade de ideais $(1 - \zeta^k) = (1 - \zeta)$ é verdadeira para todo k, e portanto a fatoração de $p\mathbb{Z}[\zeta]$ é :*

$$p\mathbb{Z}[\zeta] = (1 - \zeta)^{p-1}.$$

Assim p é totalmente ramificado, e também mostra-se que p é o único primo que se ramifica.

A ramificação de um corpo de números K está ligado a seu discriminante e ao *diferente*.

Definição 1.5.13. *O conjunto $\mathcal{D}_{K/\mathbb{Q}}^{-1} = \{x \in K | \forall \alpha \in \mathcal{O}_K, Tr_{K/\mathbb{Q}}(x\alpha) \in \mathbb{Z}\}$ é um ideal fracionário de $\mathcal{O}_K$ chamado o* **codiferente**. *O seu ideal inverso $\mathcal{D}_{K/\mathbb{Q}}$ é um ideal inteiro de $\mathcal{O}_K$ chamado o* **diferente**.

Proposição 1.5.5. *[6] Um ideal primo $\mathcal{B}$ de $\mathcal{O}_K$ é ramificado em $K/\mathbb{Q}$ se, e somente se, ele divide o diferente $\mathcal{D}_{K/\mathbb{Q}}$, isto é, $\mathcal{B}$ aparece com expoente positivo na sua fatoração em ideais primos de $\mathcal{D}_{K/\mathbb{Q}}$.*

Proposição 1.5.6. *[6] $N(\mathcal{D}_{K/\mathbb{Q}}) = |d_K|$.*

Exemplo 1.5.6. *Seja $K = \mathbb{Q}(\zeta)$, onde $\zeta = \zeta_p$, com p um primo ímpar e ζ uma p-ésima raiz da unidade. O discriminante de K é $(-1)^{(p-1)/2} p^{p-2}$. Existe somente um único fator primo p na fatoração do seu discriminante, o que corresponde ao fato de que somente p se ramifica.*

CAPÍTULO 2

Reticulado Ideal

Este capítulo é dedicado ao estudo de uma forma especial de reticulado algébrico, munido com uma *forma traço*, chamado *reticulado ideal*. Focalizaremos em duas propriedades: sua diversidade e sua distância produto mínima. Motivados pelo problema de comunicação descrito no Capítulo 1, para canais com desvanecimento Rayleigh, procuraremos por diversidade máxima e distância produto mínima máxima. As principais referências para os conceitos e resultados utilizados são [14], [15] e [16]. Os resultados obtidos no artigo conjunto [22] são apresentados de forma mais detalhada na Subseção 2.2.2.

2.1 Definições Básicas

Sejam K um corpo de números de grau n e $\mathcal{O}_K$ seu anel de inteiros algébricos. Considere $- : K \to K$ uma *involução* $\mathbb{Q}$-linear de K, isto é, uma aplicação aditiva e multiplicativa tal que $\bar{\bar{x}} = x$ para todo $x \in K$.

O conjunto $F = \{x \in K | \bar{x} = x\}$ é um corpo, chamado o *corpo fixado* da involução. Temos que $[K : F] \leq 2$. A involução é dita *trivial* se $K = F$, isto é, se ela é igual a identidade, e *não trivial* se $[K : F] = 2$.

Um *reticulado inteiro* é um par (L, b), onde L é um $\mathbb{Z}$-módulo livre de posto finito n, e $b : L \times L \to \mathbb{Z}$ é uma forma $\mathbb{Z}$-bilinear simétrica.

O reticulado (L, b) é dito ser *positivo* (respectivamente *negativo*) *definido* se $b(x, x) > 0$ (respectivamente $b(x, x) < 0$) para todo $0 \neq x \in L$.

Relembramos que $\mathcal{O}_K$ e qualquer ideal não nulo de $\mathcal{O}_K$ são $\mathbb{Z}$-módulos livres de posto finito n. Logo, possuem uma $\mathbb{Z}$-base livre com n elementos, chamada base integral de K.

Definição 2.1.1. *Sejam $\mathcal{I}$ um ideal de $\mathcal{O}_K$ e $\alpha \in F$ tal que $\alpha\mathcal{I}\bar{\mathcal{I}} \subseteq \mathcal{D}_{K/\mathbb{Q}}^{-1}$. Um* **reticulado ideal** *é um reticulado inteiro $(\mathcal{I}, b_\alpha)$, onde*

$$b_\alpha : \mathcal{I} \times \mathcal{I} \to \mathbb{Z}, \quad b_\alpha(x, y) = Tr_{K/\mathbb{Q}}(\alpha x \bar{y}), \quad \forall x, y \in \mathcal{I}.$$

Note que a condição $\mathcal{I}\bar{\mathcal{I}} \subseteq \mathcal{D}_{K/\mathbb{Q}}^{-1}$ garante que o reticulado seja inteiro, e α escolhido para estar em F, garante que a forma traço é simétrica:

$$b_\alpha(x, y) = Tr_{K/\mathbb{Q}}(\alpha x \bar{y}) = \overline{Tr_{K/\mathbb{Q}}(\bar{\alpha}\bar{x}y)} = b_\alpha(y, x).$$

2.1.1 Mergulho e Diversidade

Dado um reticulado ideal (L, b_α), gostaríamos de realizá-lo no $\mathbb{R}^n$. Como a sua matriz de Gram é dada por:

$$G = \left(Tr_{K/\mathbb{Q}}\left(\alpha\omega_i\bar{\omega_j}\right)\right),$$

queremos uma matriz M tal que $G = MM^T$, onde $\{\omega_1, \ldots, \omega_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_K$. Se α é totalmente real e totalmente positivo, ou seja, $\sigma_i(\alpha) \in \mathbb{R}$ e $\sigma_i(\alpha) > 0$, para todo i, então obtemos a matriz M pelo *mergulho canônico torcido ou perturbação do homomorfismo canônico* $\sigma_\alpha : K \to \mathbb{R}^n$, que é construído do seguinte modo:

$$\begin{aligned}\sigma_\alpha(x) \;=\; & (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x)), \\ & \sqrt{2\alpha_{r_1+1}}\Im(\sigma_{r_1+1}(x)), \ldots, \sqrt{2\alpha_{r_2}}\Re(\sigma_{r_2}(x)), \sqrt{2\alpha_{r_2}}\Im(\sigma_{r_2}(x))),\end{aligned}$$

Usando o mergulho canônico torcido, a matriz geradora M do reticulado $\Lambda = \sigma_\alpha(\mathcal{O}_K)$ é dada por

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(w_1) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(w_1) & \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(w_1) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(w_1) \\ \sqrt{\alpha_1}\sigma_1(w_2) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(w_2) & \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(w_2) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(w_2) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \sqrt{\alpha_1}\sigma_1(w_n) & \cdots & \sqrt{\alpha_{r_1}}\sigma_1(w_n) & \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(w_n) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(w_n) \end{pmatrix}$$

$$= (\sigma_i(\omega_j))_{i,j=1}^n diag(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_{r_1}}, \sqrt{2\alpha_{r_1+1}}, \ldots, \sqrt{2\alpha_{r_1+r_2}}). \tag{2.1}$$

A correspondente matriz de Gram G é dada por $G = MM^t = (g_{ij})_{i,j=1}^n$ onde

$$\begin{aligned} g_{ij} &= \sum_{k=1}^{r_1} \alpha_k \sigma_k(\omega_i\omega_j) + \\ &\quad \sum_{k=1}^{r_2} 2\alpha_{r_1+k}[\Re(\sigma_{r_1+k}(\omega_i)\Re(\sigma_{r_1+k}(\omega_j)) + \Im(\sigma_{r_1+k}(\omega_i)\Im(\sigma_{r_1+k}(\omega_j))] \\ &= \sum_{k=1}^{r_1} \alpha_k \sigma_k(\omega_i\omega_j) + \sum_{k=1}^{r_2} 2\alpha_{r_1+k}\Re(\sigma_{r_1+k}(\omega_i)\sigma_{r_1+k}(\overline{\omega_j})) \\ &= \sum_{k=1}^{r_1} \alpha_k \sigma_k(\omega_i\omega_j) + \sum_{k=1}^{r_2} \alpha_{r_1+k}\sigma_{r_1+k}(\omega_i\overline{\omega_j})) + \sum_{k=1}^{r_2} \alpha_{r_1+k}\overline{\sigma_{r_1+k}(\omega_i\overline{\omega_j})} \\ &= Tr_{K/\mathbb{Q}}(\alpha\omega_i\overline{\omega_j}) \end{aligned}$$

Como a matriz de Gram é uma matriz na forma traço, isto mostra que a matriz geradora dada em (2.1) define um reticulado ideal.

A demonstração do Teorema 1.5.8 é facilmente estendida para o caso de mergulhos torcidos, usando o fato de que

$$(\sigma_\alpha(\omega_j))_{j=1}^n = (\sigma_i(\omega_j))_{i,j=1}^n diag(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_{r_1}}, \sqrt{2\alpha_{r_1+1}}, \ldots, \sqrt{2\alpha_{r_1+r_2}}),$$

e que o mergulho torcido de uma base de K também nos dá uma base em $\mathbb{R}^n$.

Observação 2.1.1. *Note as hipóteses sobre α, comparadas com a Definição 2.1.1. Aqui não estamos mais exigindo que $\alpha\mathcal{I}\bar{\mathcal{I}} \subseteq \mathcal{D}_{K/\mathbb{Q}}^{-1}$, e assim, o reticulado não é necessariamente inteiro. Esta condição foi substituída pela condição de que α seja totalmente real e totalmente positivo, de forma que $\sqrt{\alpha_j}$ esteja bem definido para todo j.*

O determinante dos reticulados ideais podem ser relacionados a d_K, o discriminante do corpo de números K. Denotaremos por $det(\Lambda)$ ou $det(b)$ se $\Lambda = (L, b)$.

Proposição 2.1.1. *Seja $(\mathcal{I}, b_\alpha)$ um reticulado ideal. Temos*

$$|det(b_\alpha)| = |d_K| N(\mathcal{I})^2 N(\alpha).$$

Demonstração: Como $\mathcal{I}$ é um $\mathbb{Z}$-submódulo de posto n de $\mathcal{O}_K$, existe uma base $\{v_1, \ldots, v_n\}$ de $\mathcal{O}_K$ e inteiros positivos $q_1, \ldots, q_n$ tal que $\{q_1 v_1, \ldots, q_n v_n\}$ é uma base para $\mathcal{I}$. Expressando-se a matriz geradora de $(\mathcal{I}, b_\alpha)$ nesta base, mostra-se, de forma direta, que $|det(b_\alpha)| = |d_K| N(\mathcal{I}) N(\bar{\mathcal{I}}) N(\alpha)$. ■

2.1.2 Distância Produto Mínima

A distância produto mínima de um reticulado ideal também pode ser obtida de propriedades algébricas do corpo de números.

Teorema 2.1.1. *Seja $\mathcal{I}$ um ideal de $\mathcal{O}_K$. A distância produto mínima de um reticulado ideal $(\mathcal{I}, b_\alpha)$ de determinante $det(b_\alpha)$ é*

$$d_{p,min}(\Lambda) = \sqrt{\frac{det(b_\alpha)}{d_K}} min(\mathcal{I}),$$

onde $min(\mathcal{I}) = \min_{0 \neq x \in \mathcal{I}} \frac{|N(x)|}{N(\mathcal{I})}$.

Demonstração: Seja $\mathbf{x} = \sigma_\alpha(x)$ um ponto do reticulado em $\mathbb{R}^n$, com $x \in \mathcal{I} \subseteq \mathcal{O}_K$ seu correspondente inteiro algébrico. Temos

$$d_{p,min}(\Lambda) = \min_{0 \neq \mathbf{x} \in \Lambda} \prod_{j=1}^{n} |x_j| = \min_{0 \neq x \in \mathcal{I}} \prod_{j=1}^{n} |\sqrt{\sigma_j(\alpha)} \sigma_j(x)| = \sqrt{N(\alpha)} \min_{0 \neq x \in \mathcal{I}} |N(x)|.$$

A demonstração é concluída usando a Proposição 2.1.1. ■

Lema 2.1.1. *Se $\mathcal{I}$ é um ideal principal de $\mathcal{O}_K$, então*

$$\min_{0 \neq x \in \mathcal{I}} N(x) = N(\mathcal{I}).$$

Demonstração: Como $\mathcal{I}$ é principal, $\mathcal{I} = (a)$, para $a \in \mathcal{I}$, e $N(\mathcal{I}) = |N(a)|$. Seja $x \in \mathcal{I}$, então $x = ay$ para algum $y \in \mathcal{O}_K$. Assim, $|N(x)| = |N(a)||N(y)| \geq N(\mathcal{I})$ e a igualdade acontece se, e somente se, $N(y) = \pm 1$. O mínimo é atingido, tomando-se por exemplo $y = 1$.

■

Corolário 2.1.1. *Se $\mathcal{I}$ é principal, então a distância produto mínima de Λ é*

$$d_{p,min}(\Lambda) = \sqrt{\frac{det(b_\alpha)}{d_K}}.$$

Demonstração: A demonstração é imediata do Teorema 2.1.1 e do Lema 2.1.1.

2.2 O Reticulado Ideal $\mathbb{Z}^n$

Nesta seção discutiremos as idéias básicas para construção de reticulados $\mathbb{Z}^n$-rotacionados a partir de reticulados ideais.

Em termos de reticulado ideal, isto significa que dado n, procuramos um corpo de números K de grau n e um ideal $\mathcal{I} \subseteq \mathcal{O}_K$ tal que $\Lambda = (\mathcal{I}, b_\alpha)$ seja equivalente a $\mathbb{Z}^n$, $n \geq 2$. Isto é, este reticulado admite uma matriz ortogonal como geradora e, em relação a esta base, a matriz de Gram é a identidade. Do ponto de vista geométrico, um reticulado $\Lambda' = (\mathcal{I}, b_\alpha)$ sobre $\mathcal{I} \subseteq \mathcal{O}_K$ é um sub-reticulado de $\Lambda = (\mathcal{O}_K, b_\alpha)$. A idéia é que dado um reticulado Λ, procura-se um sub-reticulado que seja $\mathbb{Z}^n$ escalonado.

O determinante do reticulado será um critério útil para nos ajudar a encontrar o $\mathbb{Z}^n$-reticulado. Uma versão escalonada de $\mathbb{Z}^n$ é da forma $(\sqrt{c}\mathbb{Z})^n$ para algum inteiro c, tal que seu determinante é $det(G) = det(M)^2 = c^n$, pois o determinante de $\mathbb{Z}^n$ é 1. Usando a Proposição 2.1.1, deduzimos a seguinte condição necessária (mas não suficiente):

$$N(\mathcal{I})^2 N(\alpha)|d_K| = c^n \tag{2.2}$$

onde c é um inteiro. Podemos supor c o menor inteiro tal que $N(\alpha) \in \mathbb{Z}$. Se assumirmos que $\mathcal{I} = \mathcal{O}_K$, essa expressão é simplificada para

$$N(\alpha)|d_K| = c^n. \tag{2.3}$$

Esta condição necessária será útil para a escolha de um α para a construção de códigos $\mathbb{Z}^n$-reticulados.

Exemplo 2.2.1. *Queremos construir o reticulado $\mathbb{Z}^2$ com diversidade máxima. Tomamos o corpo de números $K = \mathbb{Q}(\sqrt{5})$, no qual seu discriminante é $d_K = 5$. Sabemos que K é totalmente real, pois tem dois mergulhos reais que são:*

$$\sigma_1(a + b\sqrt{5}) = a + b\sqrt{5} \quad e \quad \sigma_2(a + b\sqrt{5}) = a - b\sqrt{5}, \qquad a, b \in \mathbb{Q}.$$

Vimos em (2.2) que uma condição necessária para obter $\mathbb{Z}^2$ é ter um elemento α tal que

$$N(\alpha)|d_K| = N(\alpha) \cdot 5 = c^2, \qquad c \in \mathbb{Z}.$$

É natural escolhermos um elemento α no qual tenha norma 5. Se tomarmos o elemento

$$\alpha = 2 + \frac{1+\sqrt{5}}{2} \tag{2.4}$$

temos que sua norma é:

$$N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = \left(2 + \frac{1+\sqrt{5}}{2}\right)\left(2 + \frac{1-\sqrt{5}}{2}\right) = 5,$$

e α é totalmente real e totalmente positivo.

Uma boa escolha para tentar construir $\mathbb{Z}^2$ consiste em tomar $\mathcal{I} = \mathcal{O}_K$ com α dado por (2.4). A matriz geradora do reticulado M é dada por

$$M = \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & \sqrt{\sigma_2(\alpha)} \\ \sqrt{\sigma_1(\alpha)}\sigma_1(\frac{1+\sqrt{5}}{2}) & \sqrt{\sigma_2(\alpha)}\sigma_2(\frac{1+\sqrt{5}}{2}) \end{pmatrix}.$$

Calculando a matriz de Gram $G = MM^T$:

$$G = \begin{pmatrix} \sigma_1(\alpha) + \sigma_2(\alpha) & \sigma_1(\alpha\frac{1+\sqrt{5}}{2}) + \sigma_2(\alpha\frac{1+\sqrt{5}}{2}) \\ \sigma_1(\alpha\frac{1+\sqrt{5}}{2}) + \sigma_2(\alpha\frac{1+\sqrt{5}}{2}) & \sigma_1(\alpha(\frac{1+\sqrt{5}}{2})^2) + \sigma_2(\alpha(\frac{1+\sqrt{5}}{2})^2) \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}.$$

Isto mostra que temos uma versão escalonada de $\mathbb{Z}^2$. Depois da normalização, temos que $\mathbb{Z}^2$ pode ser construído sobre $\mathcal{O}_K$, com matriz geradora $\frac{1}{\sqrt{5}}M$ e sua distância produto mínima é $1/\sqrt{5}$ (Figura 2.1).

Em [13], foram desenvolvidos métodos para a construção de $\mathbb{Z}^n$ como reticulado ideal em todas as dimensões. A seguir apresentaremos, resumidamente, os três tipos de construções.

(I) *A construção ciclotômica:* usando o anel dos inteiros algébricos do subcorpo maximal real de um corpo ciclotômico $\mathbb{Q}(\zeta_p)$, podemos construir o reticulado $\mathbb{Z}^n$ em dimensão $n = (p-1)/2,\ p \geq 5$ um primo.

(II) *A construção cíclica:* usando o inverso do codiferente de um corpo cíclico, construímos o reticulado $\mathbb{Z}^n$ em dimensões primas.

(III) *A construção mista:* combina construções conhecidas a fim de encontrar reticulados em dimensões não obtidas pelos dois métodos anteriores.

A construção ciclotômica, que abordaremos neste trabalho, foi a primeira a ser encontrada, porém não pode ser obtida em todas as dimensões.

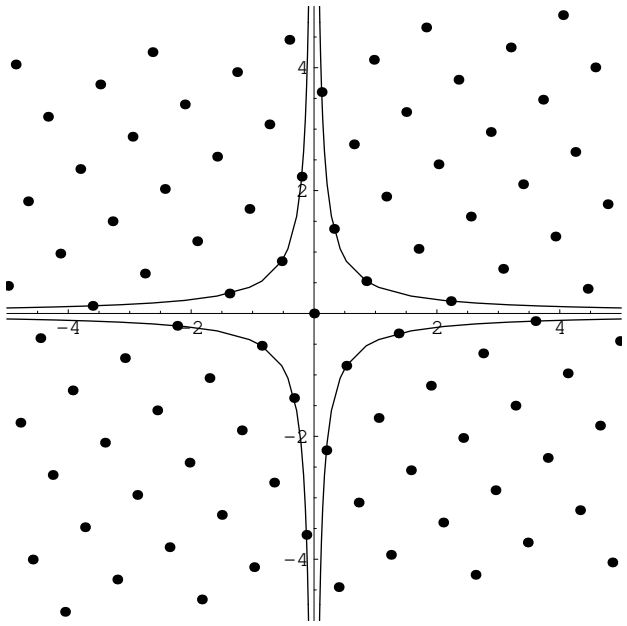


Figura 2.1: Reticulado ideal obtido de $K = \mathbb{Q}(\sqrt{5})$ e $d_{p,min} = 1/\sqrt{5}$.

2.2.1 A Construção Ciclotômica

Consideraremos a construção de reticulados $\mathbb{Z}^n$-rotacionados sobre o anel dos inteiros do subcorpo maximal real de um corpo ciclotômico.

Até o final deste capítulo adotaremos a notação que introduziremos a seguir.

Seja o corpo ciclotômico $L = \mathbb{Q}(\zeta_p)$, onde $p \geq 5$ é um primo e $\zeta = \zeta_p = e^{-2i\pi/p}$ é uma raiz p-ésima da unidade. Os reticulados são construídos via o anel dos inteiros de $K = \mathbb{Q}(\zeta+\zeta^{-1})$, o subcorpo maximal real de $\mathbb{Q}(\zeta)$, o qual tem grau $n = (p-1)/2$ sobre $\mathbb{Q}$. O anel dos inteiros de L é $\mathcal{O}_L = \mathbb{Z}[\zeta]$ e o de K é $\mathcal{O}_K = \mathbb{Z}[\zeta + \zeta^{-1}]$.

Seja $\Lambda = (\mathcal{O}_K, b_\alpha)$ um reticulado ideal. Como vimos em (2.2), uma condição necessária para construirmos uma versão escalonada de $\mathbb{Z}^n$ é

$$N(\alpha)|d_K| = N(\alpha)p^{(p-3)/2} = c^{(p-1)/2}.$$

Um elemento $\alpha \in K$ com norma p é facilmente encontrado em K, pois

$$(p)\mathcal{O}_L = (p)\mathbb{Z}[\zeta] = (1-\zeta)^{p-1}\mathbb{Z}[\zeta]$$

em L e $N_{L/\mathbb{Q}}(1-\zeta) = p$. Usando a transitividade da norma, temos

$$N_{L/\mathbb{Q}}(1-\zeta) = N_{K/\mathbb{Q}}(N_{L/K}(1-\zeta)) = N_{K/\mathbb{Q}}((1-\zeta)(1-\zeta^{-1})).$$

Assim $(1-\zeta)(1-\zeta^{-1})$ é um elemento de $\mathcal{O}_K$ com norma p.

Observação 2.2.1. *Como já destacamos anteriormente essa não é uma condição suficiente para garantir a existência de uma versão escalonada de $\mathbb{Z}^n$. Para mostrar sua existência, temos que construir explicitamente.*

Seja $\{e_j = \zeta^j + \zeta^{-j}\}_{j=1}^n$ a $\mathbb{Z}$-base canônica para $\mathcal{O}_K$. Uma outra base é dada por $\{e'_i\}_{i=1}^n$ onde $e'_n = e_n$ e $e'_j = e_j + e'_{j+1}$, $j = 1, \ldots, n-1$.

Proposição 2.2.1. *Seja $\alpha = (1-\zeta)(1-\zeta^{-1}) = 2 - (\zeta + \zeta^{-1})$. Então*

$$\frac{1}{p} Tr_{K/\mathbb{Q}}(\alpha e'_i e'_j) = \delta_{ij}.$$

Demonstração: Denotamos por $\sigma_j(\zeta) = \zeta^j$ e $\alpha_j = \sigma_j(\alpha)$, $j = 1, \ldots, n$ os conjugados de ζ e α, respectivamente. Temos que

$$Tr_{K/\mathbb{Q}}(\zeta^k + \zeta^{-k}) = \sum_{j=1}^{n} \sigma_j(\zeta^k + \zeta^{-k}) = -1, \ \forall k = 1, \ldots, n, \tag{2.5}$$

Usando (2.5), obtemos

$$\begin{array}{rcl} \sum_{j=1}^n \alpha_j \sigma_j(\zeta^k + \zeta^{-k}) & = & \sum_{j=1}^n (2 - \sigma_j(\zeta + \zeta^{-1}))\sigma_j(\zeta^k + \zeta^{-k}) \\ & = & -2 - \sum_{j=1}^n \sigma_j(\zeta^{k+1} + \zeta^{-k-1} + \zeta^{-k+1} + \zeta^{k-1}) \\ & = & \begin{cases} -p \text{ se } k \equiv \pm 1 (mod\ p) \\ 0 \ \text{ caso contrário} \end{cases} \end{array} \tag{2.6}$$

Agora vamos calcular $Tr_{K/\mathbb{Q}}(\alpha e_i e_j)$, usando (2.5) e (2.6), para todo $i, j = 1, \ldots, n$.

$$\begin{array}{rcl} Tr_{K/\mathbb{Q}}(\alpha e_i^2) & = & \sum_{j=1}^n \sigma_j(\zeta^{2i} + \zeta^{-2i}) + 2\sum_{j=1}^n (2 - \sigma_j(\zeta + \zeta^{-1})) \\ & = & \begin{cases} p \ \text{ se } i = n, \text{ isto é } 2i \equiv -1 (mod\ p) \\ 2p \ \text{ caso contrário} \end{cases} \end{array}$$

$$\begin{array}{rcl} Tr_{K/\mathbb{Q}}(\alpha e_i e_j) & = & \sum_{k=1}^n \alpha_k \sigma_k(\zeta^{i+j} + \zeta^{-(i+j)}) + \sum_{k=1}^n \alpha_k \sigma_k(\zeta^{i-j} + \zeta^{-(i-j)}) \\ & = & \begin{cases} -p \ \text{ se } |i-j| = 1 \\ 0 \ \text{ caso contrário} \end{cases} \end{array}$$

Assim, a matriz de $Tr_{K/\mathbb{Q}}(\alpha xy)$ na base $\{e_1, \ldots, e_n\}$ é dada por

$$\begin{pmatrix} 2 & -1 & 0 & \cdots & 0 \\ -1 & 2 & & & \\ 0 & & \ddots & -1 & 0 \\ & & -1 & 2 & -1 \\ 0 & \cdots & 0 & -1 & 1 \end{pmatrix}.$$

Na nova base $\{e'_i\}_{i=1}^n$ onde $e'_n = e_n$ e $e'_j = e_j + e'_{j+1}$, $j = 1, \ldots, n-1$, a matriz acima é a matriz de Gram do reticulado $\mathbb{Z}^n$.

■

Assim, temos que o reticulado ideal $\Lambda = (\mathcal{O}_K, \frac{1}{p} b_\alpha)$ com $\alpha = (1-\zeta)(1-\zeta^{-1})$ é isomorfo a $\mathbb{Z}^n$.

O correspondente reticulado $\mathbb{Z}^n$-rotacionado é obtido como mostraremos a seguir. Considere os n mergulhos definidos por

$$\sigma_k(e_j) = \zeta^{kj} + \zeta^{-kj} = 2\cos\left(\frac{2\pi kj}{p}\right).$$

O reticulado gerado pelo anel dos inteiros tem a matriz geradora $M_{n\times n}$ com elementos $M_{k,j} = 2\cos\left(\frac{2\pi kj}{p}\right)$ e o elemento torcido pode ser representado pela matriz diagonal

$$A = diag(\sqrt{\sigma_k(\alpha)}).$$

A matriz de transformação de base de $\{e_j\}$ para $\{e'_j\}$ é dada por

$$T = \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ 0 & 1 & 1 & \ldots & 1 \\ \vdots & & \ddots & & \vdots \\ 0 & \ldots & 0 & 1 & 1 \\ 0 & 0 & \ldots & 0 & 1 \end{pmatrix}.$$

Finalmente, a matriz geradora do reticulado $\mathbb{Z}^n$-rotacionado é dada por

$$R = \frac{1}{\sqrt{p}} TMA.$$

Seguindo os passos anteriores construimos reticulados $\mathbb{Z}^n$-rotacionados em dimensão $n = (p-1)/2$, isto é, $n = 2, 3, 5, 6, 8, 9, 11, 14, 15, 18, 20, 21, 23, 26, 29, 30, \ldots$.

Corolário 2.2.1. *A distância produto mínima do reticulado ideal* $\Lambda = (\mathcal{O}_K, \frac{1}{p}b_\alpha)$ *de dimensão* $n = (p-1)/2$ *é*

$$d_{p,min}(\Lambda) = p^{-\frac{n-1}{2}}.$$

Demonstração: Pelo Corolário 2.1.1, a distância produto mínima é dada por $d_{p,min}(\Lambda) = 1/\sqrt{d_K} = p^{-\frac{n-1}{2}}$, pois $d_K = p^{\frac{p-3}{2}} = p^{n-1}$.

■

2.2.2 Reticulados Rotacionados via o Corpo Ciclotômico $\mathbb{Q}(\zeta_{2^r})$

Esta seção contém de forma mais detalhada os resultados do artigo conjunto [22]. A construção dos reticulados $\mathbb{Z}^n$ rotacionados é realizada sobre o anel de inteiros algébricos do subcorpo maximal $\mathbb{Q}(\zeta_{2^r} + \zeta_{2^r}^{-1})$ de $\mathbb{Q}(\zeta_{2^r})$ e calculamos sua distância produto mínima.

Seja $\zeta = \zeta_{2^r}$ uma 2^r-ésima raiz da unidade, onde r é um inteiro positivo. Seja $L = \mathbb{Q}(\zeta)$ e $K = \mathbb{Q}(\zeta + \zeta^{-1})$. Sabemos que $[L : \mathbb{Q}] = \varphi(2^r) = 2^{r-1}$ e $n = [K : \mathbb{Q}] = \varphi(2^r)/2 = 2^{r-2} = n$, pois $[L : K]$ é uma extensão quadrática. Uma base integral para $\mathcal{O}_K$ é dada por $\{1, \zeta + \zeta^{-1}, \cdots, \zeta^{n-1} + \zeta^{-(n-1)}\}$.

Proposição 2.2.2. *[19] O discriminante de* K *é dado por*

$$d_K = 2^\beta, \quad \textit{onde} \quad \beta = (r-1)n - 1.$$

Seja $\Lambda = (\mathcal{O}_K, b_\alpha)$ um reticulado ideal. Como vimos na seção anterior, uma condição necessária (mas não suficiente) para Λ ser isomorfo a $(\sqrt{c}\mathbb{Z})^n$, uma versão escalonada de $\mathbb{Z}^n$, é que $det(\Lambda) = c^n$. Logo, precisamos encontrar $\alpha \in \mathcal{O}_K$ tal que

$$N_{K/\mathbb{Q}}(\alpha) d_K = N_{K/\mathbb{Q}}(\alpha) 2^\beta = c^n,$$

onde $\beta = (r-1)n - 1$. Neste caso, temos $c = 2^{r-1}$.

Um elemento $\alpha \in \mathcal{O}_K$ com norma 2 é facilmente encontrado. Temos

$$2\mathbb{Z}[\zeta] = (1-\zeta)^{\phi(2^r)}\mathbb{Z}[\zeta]$$

em $\mathbb{Q}(\zeta)$, onde $N_{L/\mathbb{Q}}(1-\zeta) = 2$. Usando a transitividade da norma, obtemos

$$N_{L/\mathbb{Q}}(1-\zeta) = N_{K/\mathbb{Q}}(N_{L/K}(1-\zeta)) = N_{K/\mathbb{Q}}((1-\zeta)(1-\zeta^{-1})).$$

Assim $\alpha = (1-\zeta)(1-\zeta^{-1}) = 2-(\zeta+\zeta^{-1})$ é um elemento de $\mathcal{O}_K$ cuja norma é 2. Esta condição não é suficiente para garantir a existência de uma versão escalonada de $\mathbb{Z}^n$. Para mostrar esta existência, temos que construir explicitamente.

Proposição 2.2.3. *[21] Se $L = \mathbb{Q}(\zeta)$ então*

$$Tr_{L/\mathbb{Q}}(\zeta^k) = \begin{cases} 0 \quad se \quad mdc(k,\, 2^r) < 2^{r-1}; \\ -2^{r-1} \quad se \quad mdc(k,\, 2^r) = 2^{r-1}; \\ 2^{r-1} \quad se \quad mdc(k,\, 2^r) > 2^{r-1}. \end{cases}$$

Corolário 2.2.2. *Se $K = \mathbb{Q}(\zeta+\zeta^{-1})$ então*

$$Tr_{K/\mathbb{Q}}(\zeta^k+\zeta^{-k}) = \begin{cases} 0 \quad se \quad mdc(k,\, 2^r) < 2^{r-1}; \\ -2^{r-1} \quad se \quad mdc(k,\, 2^r) = 2^{r-1}; \\ 2^{r-1} \quad se \quad mdc(k,\, 2^r) > 2^{r-1}. \end{cases}$$

Demonstração: Pela transitividade do traço temos $Tr_{L/\mathbb{Q}}(\zeta^k) + Tr_{L/\mathbb{Q}}(\zeta^{-k}) = Tr_{L/\mathbb{Q}}(\zeta^k+\zeta^{-k}) = Tr_{K/\mathbb{Q}}(Tr_{L/K}(\zeta^k+\zeta^{-k})) = 2Tr_{K/\mathbb{Q}}(\zeta^k+\zeta^{-k})$, de onde segue o resultado. ■

Proposição 2.2.4. *Considere $e_0 = 1$ e $e_i = \zeta^i + \zeta^{-i}$, para $i = 1, 2, \cdots, n-1$.*

1. *Se $i = 0, 1, \cdots, n-1$ então* $b_\alpha(e_i, e_i) = \begin{cases} 2n & se \;\; i = 0 \\ 4n & se \;\; i \neq 0. \end{cases}$

2. *Se $i \neq 0$ então* $b_\alpha(e_i, e_0) = \begin{cases} -2n & se \;\; i = 1 \\ 0 & se \;\; i \neq 1. \end{cases}$

3. *Se $i \neq 0$, $j \neq 0$ e $i \neq j$ então* $b_\alpha(e_i, e_j) = \begin{cases} -2n & se \quad \mid i-j \mid = 1 \\ 0 & caso\ contrário. \end{cases}$

Demonstração: Pelo Corolário 2.2.2 temos que $Tr_{K/\mathbb{Q}}(\alpha e_0) = Tr(\alpha) = 2^{r-1}$, pois $mdc(1, 2^r) < 2^{r-1}$, e assim $b_\alpha(e_0, e_0) = Tr_{K/\mathbb{Q}}(\alpha) = 2n$. Agora, como $mdc(i, 2^r) < 2^{r-1}$, para todo

$i = 1, 2, \cdots, n$, segue que

$$\begin{aligned} b_\alpha(e_i, e_0) &= Tr_{K/\mathbb{Q}}(\alpha e_i) = Tr_{K/\mathbb{Q}}((2 - (\zeta + \zeta^{-1}))(\zeta^i + \zeta^{-i})) \\ &= 2Tr_{K/\mathbb{Q}}(\zeta + \zeta^{-1}) - Tr_{K/\mathbb{Q}}(\zeta^{i+1} + \zeta^{-(i+1)}) - Tr_{K/\mathbb{Q}}(\zeta^{i-1} + \zeta^{-(i-1)}) \\ &= Tr_{K/\mathbb{Q}}(\zeta^{i-1} + \zeta^{-(i-1)}) \\ &= \begin{cases} -2n & \text{se} \quad i = 1 \\ 0 & \text{caso contrário.} \end{cases} \end{aligned}$$

Também, como $mdc(2i, 2^r), mdc(2i \pm 1, 2^r) < 2^{r-1}$, para todo $i = 1, 2, \cdots, n-1$, segue que

$$\begin{aligned} b_\alpha(e_i, e_i) &= Tr_{K/\mathbb{Q}}(\alpha e_i^2) = Tr_{K/\mathbb{Q}}((2 - (\zeta + \zeta^{-1}))(\zeta^{2i} + \zeta^{-2i} + 2)) \\ &= 2Tr_{K/\mathbb{Q}}(\zeta^{2i} + \zeta^{-2i}) + Tr_{K/\mathbb{Q}}(4) - Tr_{K/\mathbb{Q}}(\zeta^{2i+1} + \zeta^{-(2i+1)}) \\ &-Tr_{K/\mathbb{Q}}(\zeta^{2i-1} + \zeta^{-(2i-1)}) - 2Tr_{K/\mathbb{Q}}(\zeta + \zeta^{-1}) \\ &= 4n. \end{aligned}$$

Finalmente, para todo $i \neq 0$, $j \neq 0$ e $i \neq j$, como $mdc(i \pm j, 2^r), mdc(i + j \pm 1, 2^r) < 2^{r-1}$ segue que

$$\begin{aligned} b_\alpha(e_i, e_j) &= Tr_{K/\mathbb{Q}}(\alpha e_i e_j) = Tr_{K/\mathbb{Q}}((2 - (\zeta + \zeta^{-1}))(\zeta^i + \zeta^{-i})(\zeta^j + \zeta^{-j})) \\ &= 2Tr_{K/\mathbb{Q}}(\zeta^{i+j} + \zeta^{-(i+j)}) + 2Tr_{K/\mathbb{Q}}(\zeta^{i-j} + \zeta^{-(i-j)}) \\ &-Tr_{K/\mathbb{Q}}(\zeta^{i+j+1} + \zeta^{-(i+j+1)}) - Tr_{K/\mathbb{Q}}(\zeta^{i-j+1} + \zeta^{-(i-j+1)}) \\ &-Tr_{K/\mathbb{Q}}(\zeta^{-i+j+1} + \zeta^{-(-i+j+1)}) - Tr_{K/\mathbb{Q}}(\zeta^{i+j-1} + \zeta^{-(i+j-1)}) \\ &= \begin{cases} -2n & \text{se} \quad \mid i - j \mid = 1 \\ 0 & \text{caso contrário,} \end{cases} \end{aligned}$$

o que conclui a demonstração. ■

Corolário 2.2.3. *Se $Q(x, y) = \frac{1}{2^{r-1}} Tr_{K/\mathbb{Q}}(\alpha xy)$ então a matriz de Q na base $\{e_0, e_1, \cdots, e_{n-1}\}$ é dada por*

$$G = \begin{pmatrix} 1 & -1 & 0 & \cdots & & & \\ -1 & 2 & -1 & 0 & \cdots & & \\ 0 & -1 & 2 & \cdots & & & \\ & & & & \vdots & & \\ & & & & 2 & -1 & 0 \\ & & & \vdots & -1 & 2 & -1 \\ & & & \vdots & 0 & -1 & 2 \end{pmatrix}.$$

Demonstração: Segue da aplicação direta da Proposição 2.2.4. ■

Note que a matriz G do Corolário 2.2.3 é a matriz de Gram do reticulado $\mathbb{Z}^n$ dada pela base $\{w_0, w_2, \cdots, w_{n-1}\}$ definida como a seguir: $w_0 = -E_0$, $w_i = E_{i-1} - E_i$, $i = 1, 2, \cdots, n-1$, onde $\{E_j\}_{j=0}^{n-1}$ é a base canônica de $\mathbb{Z}^n$.

Isto implica que $\varphi(e_i) = w_i$, para $i = 0, 1, \cdots, n-1$, é um isomorfismo sobre o reticulado $\mathbb{Z}^n$. A base na qual corresponde a base canônica de $\mathbb{Z}^n$ através deste isomorfismo é dada por $f_i = \varphi^{-1}(E_i) = -\sum_{j=0}^{i} e_j$.

Assim, temos o seguinte resultado:

Proposição 2.2.5. *Considere a base de $\mathcal{O}_K$ dada por $\{f_0, f_1, \cdots, f_{n-1}\}$, com $f_i = -\sum_{j=0}^{i} e_j$, para todo $i = 0, 1, \cdots, n-1$. Então*

$$\frac{1}{2^{r-1}} Tr_{K/\mathbb{Q}}(\alpha f_i f_j) = \delta_{ij},$$

isto é, o reticulado $(\mathcal{O}_K, \frac{1}{2^{r-1}} b_\alpha)$ é isomorfo a $\mathbb{Z}^n$.

Seja $Gal(K, \mathbb{Q}) = \{\sigma_1, \cdots, \sigma_n\}$ o grupo de Galois de K sobre $\mathbb{Q}$. Assim, o reticulado gerado pelo anel de inteiros algébricos tem a matriz geradora $M_{n\times n}$ dada por

$$M = \begin{pmatrix} \sigma_1(e_0) & \cdots & \sigma_n(e_0) \\ \vdots & \ddots & \vdots \\ \sigma_1(e_{n-1}) & \cdots & \sigma_n(e_{n-1}) \end{pmatrix}.$$

Seja A a matriz diagonal dada por

$$A = diag(\sqrt{\sigma_k(\alpha)})_{k=1}^{n}.$$

Seja T a seguinte matriz

$$T = \begin{pmatrix} -1 & -1 & \cdots & -1 & -1 \\ -1 & -1 & \cdots & -1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -1 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

A matriz geradora do reticulado $\mathbb{Z}^n$ rotacionado é dada por

$$R = \frac{1}{\sqrt{2^{r-1}}} TMA.$$

Exemplo 2.2.2. *Seja $L = \mathbb{Q}(\zeta)$ um corpo ciclotômico e $K = \mathbb{Q}(\zeta + \zeta^{-1})$ seu subcorpo maximal real, onde $\zeta = \zeta_{2^3}$. Considerando a base $\{e_0 = 1, e_1 = \zeta + \zeta^{-1}\}$ de $\mathcal{O}_K$ e $b_\alpha(x, y) = \frac{1}{4}Tr_{K/\mathbb{Q}}(\alpha xy)$, onde $\alpha = 2 - (\zeta + \zeta^{-1})$, temos que a matriz de b_α é dada por*

$$G = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}.$$

Por outro lado, temos que

$$\begin{aligned} R = & \frac{1}{2}\begin{pmatrix} -1 & -1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ \sqrt{2} & -\sqrt{2} \end{pmatrix}\begin{pmatrix} \sqrt{2-\sqrt{2}} & 0 \\ 0 & \sqrt{2+\sqrt{2}} \end{pmatrix} \\ = & \begin{pmatrix} (-1-\sqrt{2})\sqrt{2-\sqrt{2}} & (-1+\sqrt{2})\sqrt{2+\sqrt{2}} \\ -\sqrt{2-\sqrt{2}} & -\sqrt{2+\sqrt{2}} \end{pmatrix}. \end{aligned}$$

Assim $RR^T = I$.

Por [13] temos que a distância produto mínima de Λ é dada por $d_{p,min}(\Lambda) = \frac{1}{\sqrt{d_K}} = \frac{1}{\sqrt{2^\beta}}$, onde $\beta = (r-1)n - 1$, mas é também útil considerar $\sqrt[n]{d_{p,min}(\Lambda)}$ com objetivo de comparar reticulados de diferentes dimensões.

r	n	$d_{p,min}(\Lambda)$
3	2	$0,594604$
4	4	$0,385553$
5	8	$0,261068$
6	16	$0,180648$
7	32	$0,126361$
8	64	$0,0888683$
9	128	$0,0626695$
10	256	$0,044254$
11	512	$0,0312712$
12	1024	$0,0221046$

Tabela 2.1: Distância produto mínima

CAPÍTULO 3

Análise Algébrica e Geométrica de Reticulados obtidos via Corpos Ciclotômicos

Um reticulado Λ pode ser gerado por muitas bases diferentes, porém entre todas elas, algumas são especiais. Aquelas cujos elementos são, de certa forma, os menores possíveis, são chamadas *reduzidas*.

Estas bases especiais são, em geral, descritas por propriedades requeridas da matriz de Gram. Destacaremos duas formas de bases reduzidas: a redução de Minkowski e a associada ao algoritmo LLL.

Através da redução a estas bases especiais foi possível associar às propriedades algébricas uma análise mais geométrica dos reticulados obtidos via corpos ciclotômicos que é o objeto deste capítulo.

Esta análise permitiu a caracterização de reticulados construídos via corpos ciclotômicos $\mathbb{Q}(\zeta_{p^r})$ fazendo possíveis associações com reticulados conhecidos. Destacaremos alguns dos parâmetros fazendo comparações entre os resultados obtidos e os que seriam ótimos.

Para a verificação dos resultados e elaboração dos exemplos utilizamos o algoritmo LLL, rotinas do Programa Mathematica, e para a redução de Minkowski usamos o algoritmo [34].

3.1 Redução de Base de Reticulados

3.1.1 Redução de Minkowski

Seja f uma forma quadrática positiva definida n-dimensional sobre $\mathbb{R}$. Dizemos que f é uma forma *reduzida de Minkowski* se ela pode ser expressa em termos de uma base $e_1, \ldots, e_n$ tal que para cada t, $1 \leq t \leq n$,

$$f(e_t) \leq f(v) \quad \text{para todos os vetores inteiros } v \text{ para o qual } e_1, \ldots, e_{t-1}, v \text{ podem ser estendidos a uma base de } \Lambda. \tag{3.1}$$

Em outras palavras, cada e_t sucessivo é escolhido tal que $f(e_t)$ seja tão pequeno quanto possível. Deixando v percorrer todos os vetores do reticulados, a condição (3.1) implica em desigualdades sobre a matriz com entradas a_{ij}.

Dado um reticulado Λ em $\mathbb{R}^n$ e $f(x) = \langle x, x \rangle$, diremos que $B = \{e_1, \ldots, e_n\}$ é uma *base de Minkowski* se para cada t, $1 \leq t \leq n$,

$$||e_t||^2 \leq ||r||^2 \quad \text{para todos os vetores inteiros } r \text{ para o qual } e_1, \ldots, e_{t-1}, r \text{ podem ser estendidos a uma base de } \Lambda. \tag{3.2}$$

Dada uma base qualquer de um reticulado, uma base de Minkowski pode ser obtida de forma recursiva. O algoritmo aplicado na matriz geradora é de alta complexidade computacional, o que dificulta a obtenção de redução para dimensões altas.

Algumas dessas desigualdades podem ser facilmente escritas.

(i) É imediato de (3.1) que

$$0 < a_{11} \leq a_{22} \leq \cdots \leq a_{nn}. \tag{3.3}$$

(ii) Se tivermos $v = e_t - \sum_{s \in S} \epsilon_s e_s$ (para algum conjunto S de índices $s < t$ e coeficientes $\epsilon_s \in \mathbb{Z}$) a desigualdade $f(e_t) \leq f(v)$ torna-se

$$2\left(\sum_{s \in S} \epsilon_s a_{st} - \sum_{\substack{r,s \in S \\ r<s}} \epsilon_r \epsilon_s a_{rs}\right) \leq \sum_{s \in S} a_{ss}.$$

Nos casos $S = \{s\}, \{r, s\}, \{q, r, s\}, \ldots$, temos

$$2|a_{st}| \leq a_{ss} \quad (s < t), \tag{3.4}$$

$$2|a_{rs} \pm a_{rt} \pm a_{st}| \leq a_{rr} + a_{ss} \quad (r < s < t), \tag{3.5}$$

$$2|\alpha a_{qt} + \beta a_{rt} + \gamma a_{st} - \alpha\beta a_{qr} - \alpha\gamma a_{qs} - \beta\gamma a_{rs}| \leq a_{qq} + a_{rr} + a_{ss} \quad (q < r < s < t), \tag{3.6}$$

com $\alpha, \beta, \gamma = \pm 1$, etc.

Este é um teorema de Minkowski que para dimensão ≤ 4, basta verificar (3.1) para $v = e_t - \sum_{s \in S} \epsilon_s e_s$ com $\epsilon_s = 0, 1$ ou ± 1. As desigualdades (3.3), (3.3) e (3.4), (3.3) a (3.5), (3.3) a (3.6) $(q, r, s, t \leq n)$ definem uma forma reduzida de Minkowski para $n = 1, 2, 3$ e 4 respectivamente.

Obtivemos o teorema a seguir com o objetivo de estabelecer uma condição necessária e suficiente para que um reticulado obtido algebricamente seja um $\mathbb{Z}^n$-rotacionado, no lugar da condição apenas necessária encontrada na literatura.

Teorema 3.1.1. *Seja Λ um reticulado que admite uma base ortogonal ordenada $\beta = \{b_1, \ldots, b_n\}$, isto é, $||b_i|| \leq ||b_{i+1}||$ para $1 \leq i \leq n-1$, e $\alpha = \{e_1, \ldots, e_n\}$ uma base de Minkowski de Λ. Então $e_i = \pm b_i$, $\forall i = 1, \ldots, n$ a menos de uma possível reordenação entre os vetores de mesma norma em β.*

Demonstração: Primeiramente mostraremos que $e_1 = \pm b_1$.

Seja $e_1 = \sum_{i=1}^{n} x_i b_i, \quad x_i \in \mathbb{Z}$ com $mdc(x_1, \ldots, x_n) = 1$.

Assim,

$$||e_1||^2 = \sum_{i=1}^{n} x_i^2 b_{ii} \geq b_{kk}, \quad \forall\ 1 \leq k \leq j \ \text{ onde j é tal que } x_j \neq 0.$$

Podemos garantir que existe um único j tal que $x_j \neq 0$, pois α é base de Minkowski e assim e_1 é um vetor de norma mínima.

Afirmamos que $x_1 = \pm 1$ e todos os demais são nulos, isto é, $x_i = 0, \ \forall i = 2, \ldots, n$. De fato,

- Se todos os vetores b_i tiverem normas distintas então necessariamente $x_1^2 = 1$ e $x_i = 0, \ \forall i = 2, \ldots, n$. Assim, $e_1 = \pm b_1$.

- Se houver outros vetores b_i com normas iguais à norma mínima então pode ocorrer que $e_1 = b_j$, pois ele já é o menor. Assim, podemos supor que $x_1^2 = 1$, a menos de uma reordenação da base β. Logo, $e_1 = \pm b_1$.

Mostraremos por indução sobre n que $e_i = \pm b_i,\ \forall i = 1, \ldots, n$.

Se $n = 1$ então $e_1 = \pm b_1$.

Agora, vamos supor a condição válida para $n < k$ e mostrar que é válida para $n = k$.

Seja $e_k = \sum_{\ell=1}^{n} x_\ell b_\ell,\ \ x_\ell \in \mathbb{Z}$. Temos que mostrar que $\langle e_i, e_k \rangle = 0,\ \ \forall\ i < k$.

Suponha que $\langle e_i, e_k \rangle \neq 0$.

$$\langle e_i, e_k \rangle \overset{\substack{e_i = \pm b_i, \\ i<k}}{=} \pm \langle b_i, \sum_{\ell=1}^{n} x_\ell b_\ell \rangle = \pm x_i b_{ii} \neq 0.$$

Queremos mostrar que existe v tal que $||e_k||^2 > ||v||^2$, onde $\{e_1, \ldots, e_{k-1}, v\}$ pode ser estendido a uma base de Λ.

Seja $v = e_k - x_i b_i$, temos

$||v||^2 = \sum_{\substack{\ell=1 \\ \ell \neq i}}^{n} x_\ell^2 b_{\ell\ell}$

e

$||e_k||^2 = \sum_{\ell=1}^{n} x_\ell^2 b_{\ell\ell} = \sum_{\substack{\ell=1 \\ \ell \neq i}}^{n} x_\ell^2 b_{\ell\ell} + x_i b_{ii} > ||v||^2$.

Absurdo, pois $\alpha = \{e_1, \ldots, e_n\}$ é uma base de Minkowski (e_k é o vetor de norma mínima com esta propriedade).

Portanto, $\langle e_i, e_k \rangle = 0,\ \ i = 1, \ldots, k-1$. Logo, $x_j = 0,\ \forall j < k$.

Temos que b_ℓ tem norma mínima entre os vetores no reticulado gerado por $\{b_k, \ldots, b_n\}$. Pela mesma argumentação feita anteriormente, só exististirá um único índice ℓ, $\ell = k, \ldots, n$ tal que $x_\ell \neq 0$ e $x_\ell^2 = 1$.

Assim, $e_k = \pm b_\ell,\ \ \ell = k, \ldots, n$ e a menos de uma reordenação entre os vetores de norma mínima em $\{b_k, \ldots, b_n\}$, temos $e_k = \pm b_k$. ■

Uma consequência imediata deste teorema é portanto:

Corolário 3.1.1. *Um reticulado é um $\mathbb{Z}^n$-rotacionado se, e somente se, sua base reduzida de Minkowski tem por matriz de Gram a identidade.*

Os algoritmos que encontramos (Ex.o contido no programa Mathematica) para a redução de Minkowski são aplicados à matriz geradora que tenha coordenadas inteiras, o que não ocorre em grande parte dos reticulados obtidos algebricamente. O algoritmo computacional [34] que utilizamos foi desenvovido por J. Strapasson durante a nossa pesquisa e aplica-se diretamente à matriz de Gram, informando também qual a transformação linear correspodente à mudança de base envolvida.

Exemplo 3.1.1. *Seja $L = \mathbb{Q}(\zeta)$ um corpo ciclotômico e $K = \mathbb{Q}(\zeta + \zeta^{-1})$ seu subcorpo maximal real, onde $\zeta = \zeta_{2^4}$. Considere a base $\{e_0 = 1, e_1 = \zeta + \zeta^{-1}, e_2 = \zeta^2 + \zeta^{-2}, e_3 = \zeta^3 + \zeta^{-3}\}$ de $\mathcal{O}_K$ e $b_\alpha(x, y) = \frac{1}{8} Tr_{K/\mathbb{Q}}(\alpha xy)$, onde $\alpha = 2 - (\zeta + \zeta^{-1})$. Pelo Corolário 2.2.3, temos que a matriz de b_α é dada por*

$$G = \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}$$

Aplicando-se o algoritmo de redução de base de Minkowski [34], obtemos a matriz identidade de ordem 4, isto é, a matriz de Gram na base reduzida de Minkowski é I_4 e também a base reduzida é dada por $B = \{(1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1)\}$, e portanto, o reticulado obtido é o reticulado $\mathbb{Z}^4$.

3.1.2 O Algoritmo LLL

Introduzimos a seguir a redução de base LLL (Lenstra-Lenstra-Lovász). Esta redução vem sendo muito utilizada pois, embora não seja tão eficiente quanto a de Minkowski, tem complexidade computacional bem menor.

Definição 3.1.1. *Sejam $\mathcal{B} = \{\mathbf{b_1}, \ldots, \mathbf{b_n}\}$ uma base do reticulado Λ e $\mathcal{B}^* = \{\mathbf{b_1^*}, \ldots, \mathbf{b_n^*}\}$ a base obtida do processo de ortogonalização de Gram-Schmidt. A base $\mathcal{B}$ é LLL reduzida se*

$$|\mu_{i,j}| \leq \frac{1}{2} \quad \textit{para} \quad 1 \leq j < i \leq n, \quad \textit{onde} \quad \mu_{i,j} = \frac{\langle \mathbf{b_i}, \mathbf{b_j^*} \rangle}{\langle \mathbf{b_j^*}, \mathbf{b_j^*} \rangle}$$

e

$$||\mathbf{b_i^*} + \mu_{i,i-1}\mathbf{b_{i-1}^*}||^2 \geq \frac{3}{4}||\mathbf{b_{i-1}^*}||^2 \quad \textit{para} \quad 1 < i \leq n,$$

ou equivalentemente

$$||\mathbf{b_i^*}||^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) ||\mathbf{b_{i-1}^*}||^2.$$

Teorema 3.1.2. *[10] Seja $\mathcal{B} = \{\mathbf{b_1}, \ldots, \mathbf{b_n}\}$ uma base LLL reduzida de um reticulado Λ. Então*

$$det(\Lambda) \leq \prod_{i=1}^{n} ||\mathbf{b_i}|| \leq 2^{n(n-1)/4} det(\Lambda), \tag{3.7}$$

$$||\mathbf{b_j}|| \leq 2^{(i-1)/2} ||\mathbf{b_i^*}||, \quad se \;\; 1 \leq j \leq i \leq n, \tag{3.8}$$

$$||\mathbf{b_1}|| \leq 2^{(n-1)/4} det(\Lambda), \tag{3.9}$$

Para todo $\mathbf{x} \in \Lambda$ *com* $\mathbf{x} \neq 0$ *temos*

$$||\mathbf{b_1}|| \leq 2^{(n-1)/2} ||\mathbf{x}||, \tag{3.10}$$

Mais geralmente, para quaisquer vetores linearmente independentes $\mathbf{x_1}, \ldots, \mathbf{x_t} \in \Lambda$ *temos*

$$||\mathbf{b_j}|| \leq 2^{(n-1)/2} max(||\mathbf{x_1}||, \ldots, ||\mathbf{x_t}||) \quad para \;\; 1 \leq j \leq t. \tag{3.11}$$

Exemplo 3.1.2. *Pelo Exemplo* 3.1.1*, vimos que a matriz de Gram do reticulado construído é dada por:*

$$G = \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}$$

Se aplicarmos o algorítmo LLL, obtemos a transformação H que precisamos para que $HGH^T = I_4$*, a matriz de Gram do* $\mathbb{Z}^4$*, isto é,*

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

e assim concluir que o reticulado obtido é isomorfo ao reticulado $\mathbb{Z}^4$*.*

3.2 Reticulados obtidos via Corpo Ciclotômico $\mathbb{Q}(\zeta_{p^r})$

Sejam p um número primo ímpar, e r um inteiro positivo. Sejam $L = \mathbb{Q}(\zeta_{p^r})$ e $K = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$ o subcorpo maximal real de L.

O anel dos inteiros algébricos de L é $\mathcal{O}_L = \mathbb{Z}[\zeta_{p^r}]$ e o de K é $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}]$.

Neste Capítulo estudaremos as relações existentes entre o reticulado ideal sobre $\mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$ e os reticulados já conhecidos.

Nesta seção faremos dois tipos de construção sobre o anel dos inteiros algébricos do subcorpo maximal real de $\mathbb{Q}(\zeta_{p^r})$, de acordo com o elemento α escolhido.

A primeira construção foi obtida do artigo conjunto [23], e a partir dele fizemos a caracterização dos reticulados construídos em algumas dimensões. A segunda construção foi realizada através da escolha do elemento α obtido de [24]. Através da nossa construção, e utilização dos algoritmos de redução de base, pudemos verificar e construir explicitamente uma família de reticulados do tipo soma ortogonal em todas as dimensões iguais a $n = \frac{(p-1)p^{r-1}}{2}$.

3.2.1 Construção de Reticulados

Vimos no Capítulo 2, que a condição necessária (2.2), para obtermos uma versão rotacionada de $\mathbb{Z}^n$, é que $det(\Lambda) = c^n$, onde c é um inteiro. Para satisfazer esta condição, precisamos encontrar um elemento $\alpha \in \mathcal{O}_K$ tal que

$$N(\alpha)|d_K| = c^n,$$

assumindo que $\mathcal{I} = \mathcal{O}_K$. O determinante de K é dado por $d_K = p^{\frac{1}{2}((p-1)(r+1)p^{r-1}-p^r-1)}$, Exemplo 2.2. Assim, para $c = p^r$ temos que

$$N(\alpha)|d_K| = N(\alpha)p^{\frac{1}{2}((p-1)(r+1)p^{r-1}-p^r-1)} = p^r \Rightarrow N(\alpha) = p^{\frac{1}{2}(p^{r-1}+1)}.$$

Portanto, temos que encontrar um elemento $\alpha \in \mathcal{O}_K$ com norma $p^{\frac{1}{2}(p^{r-1}+1)}$. Sabemos que

$$p\mathbb{Z}[\zeta_{p^r}] = (1-\zeta_{p^r})^{\phi(p^r)}\mathbb{Z}[\zeta_{p^r}]$$

em $\mathbb{Q}(\zeta_{p^r})$, onde $N_{L/\mathbb{Q}}(1-\zeta_{p^r}) = p$. Usando a transitividade da norma, obtemos

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

Assim, $\alpha = ((1-\zeta_{p^r})(1-\zeta_{p^r}^{-1}))^{\frac{1}{2}(p^{r-1}+1)}$ é um elemento de $\mathcal{O}_K$ de norma $p^{\frac{1}{2}(p^{r-1}+1)}$.

Os reticulados obtidos com $\alpha = ((1-\zeta_{p^r})(1-\zeta_{p^r}^{-1}))^{\frac{1}{2}(p^{r-1}+1)}$, têm matriz de Gram cujas entradas são dadas por : $b_\alpha(x,y) = \frac{1}{p^r}Tr_{K/\mathbb{Q}}(\alpha xy)$ na base $\{\zeta_{p^r}+\zeta_{p^r}^{-1}, \zeta_{p^r}^2+\zeta_{p^r}^{-2}, \ldots, \zeta_{p^r}^n+\zeta_{p^r}^{-n}\}$, onde $n = \phi(p^r)/2 = (p-1)p^{r-1}/2$.

A próxima proposição nos auxilia na caracterização dos reticulados construídos.

Proposição 3.2.1. *[11] Os reticulados inteiros gerados por vetores de normas* 1 *e* 2 *são completamente classificados. Tais reticulados podem ser escritos como soma ortogonal dos reticulados*

$$I_n(n \geq 1), \quad A_n(n \geq 1), \quad D_n(n \geq 4), \quad E_6, \quad E_7, \quad E_8.$$

Exemplo 3.2.1. *Sejam* $\mathbb{Q}(\zeta_{3^2})$ *e* $\alpha = \frac{1}{9}((1-\zeta_{3^2})(1-\zeta_{3^2}^{-1}))^2$. *Através da construção descrita, temos a seguinte matriz de Gram:*

$$G = \begin{pmatrix} 6 & -5 & 3 \\ -5 & 5 & -2 \\ 3 & -2 & 2 \end{pmatrix}.$$

Aplicando-se o algoritmo de redução de base de Minkowski [34], obtemos a matriz identidade de ordem 3. *Assim, pelo Teorema* 3.1.1, *podemos concluir que o reticulado obtido é isomorfo a* $\mathbb{Z}^3$.

Exemplo 3.2.2. *Sejam* $\mathbb{Q}(\zeta_{5^2})$ *e* $\alpha = \frac{1}{25}((1-\zeta_{5^2})(1-\zeta_{5^2}^{-1}))^3$. *Através da construção descrita anteriormente, temos a seguinte matriz de Gram:*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 1 & -1 & 0 & 1 & -1 & 0 \\ 0 & 0 & 2 & -1 & 0 & -1 & 1 & 1 & -1 & 0 \\ 0 & -1 & -1 & 2 & -1 & 1 & -1 & -1 & 1 & 0 \\ 0 & 1 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 1 & -1 & 2 & 0 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & -1 & 0 & -1 & 1 & 2 & -1 & 0 \\ 0 & -1 & -1 & 1 & 0 & 1 & 0 & -1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Aplicando-se o algoritmo de redução de base de Minkowski, e algumas operações com matrizes de determinante ± 1*, obtivemos a seguinte matriz:*

$$G = \left(\begin{array}{cc|cccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 2 & 0 & -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & -1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & -1 & 2 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 2 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 2 & 0 & -1 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 2 \end{array}\right)$$

Permutando linhas e colunas na segunda submatriz, isto é, reordenando os vetores da base, temos:

$$\tilde{G} = \left(\begin{array}{cc|cccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 2 \end{array}\right)$$

Claramente vemos que a primeira parte do somando é um $\mathbb{Z}^2$ *e a segunda, por* [11]*, podemos concluir que é a matriz de Gram do reticulado* E_8*.*

Portanto, o reticulado obtido é isomorfo a $\mathbb{Z}^2 \oplus E_8$*.*

Exemplo 3.2.3. *Sejam* $\mathbb{Q}(\zeta_{3^3})$ *e* $\alpha = \frac{1}{27}((1-\zeta_{3^3})(1-\zeta_{3^3}^{-1}))^3$*. De modo análogo aos exemplos anteriores temos a seguinte matriz de Gram:*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & -1 & 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & -1 & 2 & 0 & -1 & 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & 2 & 0 & -1 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 & 2 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 2 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & -1 & 0 & 2 & -1 & -1 \\ 0 & 0 & -1 & 0 & 1 & 0 & -1 & 2 & 0 \\ 0 & 1 & -1 & -1 & 0 & 0 & -1 & 0 & 2 \end{pmatrix}$$

Aplicando-se o algoritmo de redução de base de Minkowski, e algumas operações com matrizes de determinante ± 1*, obtivemos a seguinte matriz:*

$$\tilde{G} = \left(\begin{array}{c|cccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 2 & -1 & 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & -1 & 2 & 0 & -1 & 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & 2 & 0 & -1 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 & 2 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 2 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & -1 & 0 & 2 & -1 & -1 \\ 0 & 0 & -1 & 0 & 1 & 0 & -1 & 2 & 0 \\ 0 & 1 & -1 & -1 & 0 & 0 & -1 & 0 & 2 \end{array}\right)$$

Permutando linhas e colunas na segunda submatriz, temos:

$$\tilde{\tilde{G}} = \left(\begin{array}{c|cccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 2 \end{array}\right)$$

Portanto, o reticulado obtido é isomorfo a $\mathbb{Z} \oplus E_8$.

Agora, faremos a segunda construção, que é baseada na primeira e no próximo teorema.

Denotaremos por $\mathcal{A}_p^r$ a soma ortogonal de $\frac{p^{r-1}-1}{2}$ cópias do reticulado raiz A_{p-1} (ver [11], para a definição de reticulado raiz do tipo A).

Teorema 3.2.1. *[24] Seja* $\tilde{\alpha} = \frac{1}{p^r}(1-\zeta_{p^r}^{p^{r-1}})(1-\zeta_{p^r}^{-p^{r-1}})$. *Então* $\tilde{\Lambda} = (\mathbb{Z}[\zeta_{p^r}+\zeta_{p^r}^{-1}], b_{\tilde{\alpha}})$, *onde* $b_{\tilde{\alpha}}(x,y) = Tr(\tilde{\alpha}xy)$, *é isomorfo à soma ortogonal* $\mathbb{Z}^{\frac{p-1}{2}} \oplus \mathcal{A}_p^r$.

A construção desses reticulados será feita de modo análogo à primeira, considerando-se $\tilde{\alpha} = \frac{1}{p^r}(1-\zeta_{p^r}^{p^{r-1}})(1-\zeta_{p^r}^{-p^{r-1}})$. Assim, a matriz de Gram é dada por $G = (Tr(\tilde{\alpha}xy))$, com x, y na base $\{\zeta_{p^r}+\zeta_{p^r}^{-1}, \zeta_{p^r}^2+\zeta_{p^r}^{-2}, \cdots, \zeta_{p^r}^n+\zeta_{p^r}^{-n}\}$, onde $n = \frac{\phi(p^r)}{2} = \frac{(p-1)p^{r-1}}{2}$.

Exemplo 3.2.4. *Seja* $\mathbb{Q}(\zeta_{3^3})$ *e* $\tilde{\alpha} = \frac{1}{3^3}((1-\zeta_{3^3}^{9})(1-\zeta_{3^3}^{-9}))]$. *A matriz de Gram é dada por:*

$$G = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Depois de permutar linhas e colunas obtemos a seguinte matriz:

$$\tilde{G} = \left(\begin{array}{c|cccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{array}\right)$$

Portanto o reticulado obtido tem dimensão $n = 9$ *e é isomorfo à soma ortogonal de* $\mathbb{Z}$ *com* 4 *cópias do reticulado raiz* A_2.

Exemplo 3.2.5. *Sejam* $\mathbb{Q}(\zeta_{5^2})$ *e* $\tilde{\alpha} = \frac{1}{25}((1-\zeta^{5})(1-\zeta^{-5}))$. *Aplicando-se a construção descrita, temos a seguinte matriz de Gram:*

$$G = \begin{pmatrix} 2 & 0 & 0 & -1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 2 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & -1 & 2 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Aplicando-se o algoritmo de redução de base de Minkowski [34], e depois permutando linhas e colunas convenientes, temos:

$$\tilde{G} = \left(\begin{array}{cc|cccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{array}\right)$$

Portanto, o reticulado obtido é isomorfo $\mathbb{Z}^2 \oplus 2A_4$.

3.3 Análise dos Reticulados obtidos via Corpos Ciclotômicos

Nesta seção analisaremos alguns parâmetros importantes na construção de boas constelações de sinais para o canal gaussiano e o canal com desvanecimento.

Analisaremos os parâmetros determinante, distância produto mínima e densidade de centro, em função de α e $\tilde{\alpha}$ e consequentemente, do número primo p e o inteiro positivo r, de acordo com o corpo ciclotômico utilizado para a construção do reticulado.

Denotaremos por Λ e $\tilde{\Lambda}$ os reticulados obtidos de α e $\tilde{\alpha}$, respectivamente.

3.3.1 Determinante

Pela Proposição (2.1.1), e usando o fato de que em nossas construções $\mathcal{I} = \mathcal{O}_K$, temos que :

$$det(\Lambda) = N(\alpha)d_K.$$

Logo, como $d_K = p^{\frac{1}{2}((p-1)(r+1)p^{r-1}-p^r-1)}$ então:

- $det(\Lambda) = 1$, se $\alpha = ((1-\zeta_{p^r})(1-\zeta_{p^r}^{-1}))^{\frac{1}{2}(p^{r-1}+1)}$;
- $det(\tilde{\Lambda}) = p^{\frac{1}{2}(p^{r-1}-1)}$, se $\tilde{\alpha} = \frac{1}{p^r}(1-\zeta_{p^r}^{p^{r-1}})(1-\zeta_{p^r}^{-p^{r-1}})$.

3.3.2 Distância Produto Mínima

Pelo Corolário 2.1.1, a distância produto mínima é dada por:

$$d_{p,min}(\Lambda) = \sqrt{\frac{det(\Lambda)}{d_K}} \tag{3.12}$$

Assim, substituindo em (3.12), o discriminante d_K e o determinante, temos:

- $d_{p,min}(\Lambda) = p^{-\frac{1}{4}((r+1)(p-1)p^{r-1}-p^r-1)}$, se $\alpha = ((1-\zeta_{p^r})(1-\zeta_{p^r}^{-1}))^{\frac{1}{2}(p^{r-1}+1)}$;
- $d_{p,min}(\tilde{\Lambda}) = p^{\frac{1}{4}((r+2)p^{r-1}-rp^r)}$, se $\tilde{\alpha} = \frac{1}{p^r}(1-\zeta_{p^r}^{p^{r-1}})(1-\zeta_{p^r}^{-p^{r-1}})$.

3.3.3 Densidade de Centro

Como vimos em (1.11) no Capítulo 1, a expressão para a densidade de centro de um reticulado algébrico é dada por:

$$\delta(\sigma(\mathcal{I})) = \frac{2^{r_2}\rho^n}{|d_K|^{1/2}N(\mathcal{I})}.$$

Substituindo (1.10) em (1.11), temos:

$$\delta(\sigma(\mathcal{I})) = \frac{\rho^n}{vol(\Lambda)}.$$

Nas duas construções que estudamos, consideramos $\mathcal{I} = \mathcal{O}_K$, isto é, $N(\mathcal{I}) = 1$ e também $r_2 = 0$, pois os corpos de números utilizados são totalmente reais.

Assim, temos:

- Para $\alpha = ((1-\zeta_{p^r})(1-\zeta_{p^r}^{-1}))^{\frac{1}{2}(p^{r-1}+1)}$ temos :

$$\delta(\Lambda) = \frac{\rho^{\frac{(p-1)p^{r-1}}{2}}}{vol(\Lambda)} = \frac{\rho^{\frac{(p-1)p^{r-1}}{2}}}{det(\Lambda)^{1/2}} \overset{det(\Lambda)=1}{=} \rho^{\frac{(p-1)p^{r-1}}{2}}.$$

- Para $\tilde{\alpha} = \frac{1}{p^r}(1-\zeta_{p^r}^{p^{r-1}})(1-\zeta_{p^r}^{-p^{r-1}})$ temos:

$$\delta(\tilde{\Lambda}) = \frac{\rho^{\frac{(p-1)p^{r-1}}{2}}}{vol(\tilde{\Lambda})} = \frac{\rho^{\frac{(p-1)p^{r-1}}{2}}}{det(\tilde{\Lambda})^{1/2}} = \frac{\rho^{\frac{(p-1)p^{r-1}}{2}}}{p^{\frac{1}{4}(p^{r-1}-1)}}.$$

3.3.4 Conclusão

As duas construções foram realizadas sobre corpos de números totalmente reais, logo garantimos diversidade máxima.

Um parâmetro importante no cálculo da densidade de centro é o raio de empacotamento do reticulado, e este é dado pela metade da distância mínima. Nas duas construções aqui apresentadas, os reticulados possuem um vetor com distância mínima igual a 1, pois nos dois casos o reticulado $\mathbb{Z}$ é um dos somandos, e assim o vetor de distância igual a 1, sempre estará presente.

Podemos observar que a densidade de centro dos reticulados na primeira construção são melhores que os da segunda. No primeiro caso, ela coincide com a densidade do $\mathbb{Z}^n$, porém com diversidade maior.

Para a distância produto mínima, obtivemos maiores valores na segunda construção.

Como exemplo, os reticulados em dimensão $n = 3$, obtidos do corpo ciclotômico $\mathbb{Q}(\zeta_{3^2})$, apresentam densidade de centro $\delta(\Lambda) = 0.125$ e $\delta(\tilde{\Lambda}) = 0.0138889$ e distância produto normalizada, $\mathrm{d}_{p,min}^{1/n}(\Lambda) = 0.48075$ e $d_{p,min}^{1/n}(\tilde{\Lambda}) = 0.57735$.

Em dimensão $n = 10$, os reticulados obtidos de $\mathbb{Q}(\zeta_{5^2})$, apresentam densidade de centro $\delta(\Lambda) = 0.0009765$ e $\delta(\tilde{\Lambda}) = 1.11803 \times 10^{-9}$ e distância produto $\mathrm{d}_{p,min}^{1/n}(\Lambda) = 0.25461$ e $d_{p,min}^{1/n}(\tilde{\Lambda}) = 0.29907$.

CAPÍTULO 4

Grafos Circulantes vistos como Quocientes de Reticulados

Este capítulo aborda um tema de pesquisa independente dos tratados até aqui, mas também associado a reticulados, em que também nos envolvemos durante o doutorado.

Seu conteúdo é parte integrante do artigo conjunto submetido "Circulant Graphs Viewed as Graphs on Flat Tori" [33], com alguns detalhamentos.

Grafos circulantes têm recebido significativa atenção nas últimas décadas seja teoricamente ou através de suas aplicações na construção de redes de intercomunicação para computação paralela. A teoria de grafos constitui uma poderosa ferramenta para modelar redes, onde processadores são representados como nós do grafo e os links de comunicação como as arestas conectando-os.

A associação que fizemos de grafos circulantes a quocientes de reticulados gerando grafos em toros planares (Proposições 4.1.5 e 4.1.7) permite uma abordagem geométrica para o estabelecimento de limitantes para o número de vértices de um grafo circulante com diâmetro d (Seção 4.2). Outros resultados sobre o gênero de grafos circulantes especiais e sobre a associação de grafos circulantes a códigos esféricos também foram obtidos posteriormente a partir desta associação [33], [34] e [35]. Algumas referências utilizadas no estudo deste tópico foram [25], [27], [31], [32] e [36].

4.1 Grafos Circulantes e Grafos sobre o Toro Plano

Nesta seção introduziremos as definições e notações, usadas neste capítulo, para grafos circulantes e grafos sobre o toro plano k-dimensional. Também discutiremos quando esses conceitos podem ser relacionados.

Definição 4.1.1. *Um* **grafo circulante** *com n vértices $\{v_0, \ldots, v_{n-1}\}$ e saltos $a_1, \ldots, a_m$ é um grafo não direcionado, no qual cada vértice v_j, $0 \leq j \leq n-1$, é adjacente a todos os vértices $v_{j \pm a_i \ mod \ n}$, com $1 \leq i \leq m$. Denotamos esses grafos por $C_n(a_1, \ldots, a_m)$.*

O grafo n-ciclo e o grafo completo de n vértices são exemplos de grafos circulantes denotados por $C_n(1)$ e $C_n(1, \ldots, \lfloor n/2 \rfloor)$.

Considerando a *distância do grafo* (número mínimo de arestas conectando dois vértices), o *diâmetro* de um grafo é a distância máxima entre dois vértices. Dizemos que um grafo circulante é *denso* se ele tem o número máximo possível de vértices para um dado diâmetro.

Dois grafos são ditos isomorfos (e também isométricos) se existe uma aplicação bijetora entre o conjunto de vértices que preserva a adjacência. Um importante resultado sobre isomorfismos de grafos circulantes é o seguinte:

Proposição 4.1.1. *Se existe $r \in \mathbb{Z}$, com $mdc(r, n) = 1$, tal que $(a_1, \ldots, a_m) = r(b_1, \ldots, b_m)$ mod n então $C_n(a_1, \ldots, a_m)$ é isomorfo a $C_n(b_1, \ldots, b_m)$.*

A recíproca deste resultado foi conjecturada para grafos circulantes por Ádám [29]. Esta conjectura é falsa para grafos em geral, mas é verdadeira para $m = 2$ [30].

Proposição 4.1.2. *[36] Seja $C_n(a, b)$ um grafo circulante tal que $a \not\equiv b (mod\ n)$ e $mdc(a, n) = 1$. Então o grafo $C_n(a, b)$ é isomorfo ao grafo $C_n(1, a^{-1}b \ mod \ n)$.*

Um grafo circulante é *conexo* se, e somente se, $mdc(a_1, \ldots, a_m, n) = 1$ [30].

Dado uma base $\alpha = \{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ de $\mathbb{R}^k$, o *toro plano* T_α é algebricamente definido como o espaço quociente $T_\alpha = \mathbb{R}^k / \Lambda_\alpha$, onde Λ_α é o reticulado gerado por α.

Ele pode ser também definido através da função módulo $\mu_\alpha : \mathbb{R}^k \to \mathbb{R}^k$

$$\mu_\alpha(\mathbf{x}) = \mathbf{x} \mod \Lambda_\alpha = \mathbf{x} - \sum_{i=1}^{k} \lfloor x_i \rfloor \, \mathbf{u}_i \tag{4.1}$$

onde $\mathbf{x} = \sum_{i=1}^{k} x_i \mathbf{u}_i$ e $\lfloor x_i \rfloor$ denota o maior inteiro menor ou igual a x_i. Dois vetores $\mathbf{x}$ e $\mathbf{y}$ de $\mathbb{R}^k$ estão na mesma classe lateral se, e somente se, $\mu_\alpha(\mathbf{x}) = \mu_\alpha(\mathbf{y})$, isto é, $\mathbf{x} - \mathbf{y} = \sum_{i=1}^{k} m_i \mathbf{u}_i$, $m_i \in \mathbb{Z}$.

A distância Euclidiana d em $\mathbb{R}^k$ induz a distância d_α sobre o toro plano T_α de uma forma natural [26]. A distância medida sobre o toro plano entre duas classes laterais $\overline{\mathbf{a}}$ e $\overline{\mathbf{b}}$ de $\mathbf{a}$ e $\mathbf{b}$, com $\mathbf{a}, \mathbf{b} \in \mathbb{R}^k$, é:

$$d_\alpha\left(\overline{\mathbf{a}}, \overline{\mathbf{b}}\right) = \min\left\{d(\mathbf{z}, \mathbf{y}) = ||\mathbf{z} - \mathbf{y}||\,;\ \mathbf{z} \in \overline{\mathbf{a}}, \mathbf{y} \in \overline{\mathbf{b}}\right\} \tag{4.2}$$

onde $||\mathbf{x}|| = \sqrt{\sum_{i=1}^{k} x_i^2}$ é a norma Euclidiana em $\mathbb{R}^k$.

Geometricamente, o toro plano T_α pode ser caracterizado como o quociente de $\mathbb{R}^k$ pelo grupo das translações gerado por α, também denotado por Λ_α. Para $k = 2$ e $\alpha = \{\mathbf{u}, \mathbf{v}\}$, este quociente T_α pode ser visto como o paralelogramo gerado por $\mathbf{u}$ e $\mathbf{v}$ com os lados opostos identificados (este paralelogramo contém representantes de todas as classes com redundância na borda).

A Figura 4.1 ilustra o toro plano para $k = 2$ e mostra as distâncias $d_\alpha\left(\overline{\mathbf{a}}, \overline{\mathbf{b}}\right)$ e $d_\alpha(\overline{\mathbf{a}}, \overline{\mathbf{c}})$, onde $\overline{\mathbf{a}}$, $\overline{\mathbf{b}}$ e $\overline{\mathbf{c}}$ são as classes de $\mathbf{a}$, $\mathbf{b}$ e $\mathbf{c}$, respectivamente, $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{R}^2$.

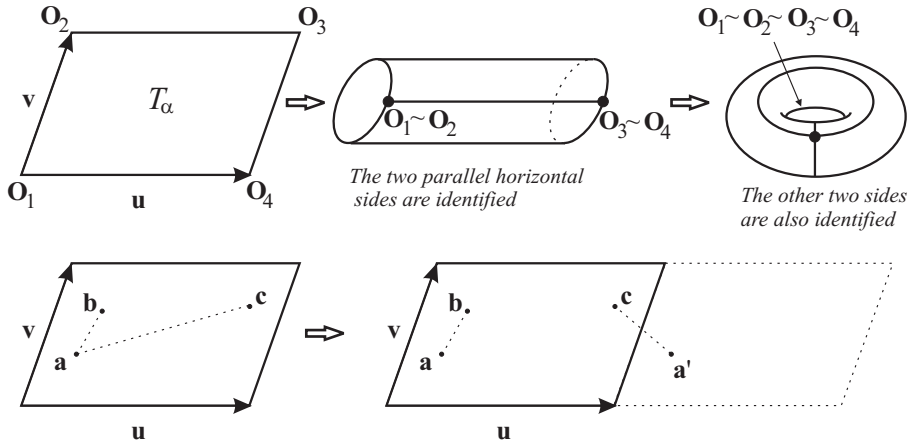


Figura 4.1: No topo, uma visão topologica do toro plano usual do $\mathbb{R}^3$ é obtida pela identificação dos lados opostos de um paralelogramo em dois passos. Abaixo, a distância d_α sobre o toro plano é vista como a distância euclidiana d em $\mathbb{R}^2$: $d_\alpha\left(\overline{\mathbf{a}}, \overline{\mathbf{b}}\right) = d(\mathbf{a}, \mathbf{b})$ mas $d_\alpha(\overline{\mathbf{a}}, \overline{\mathbf{c}}) = d(\mathbf{a}', \mathbf{c})$

Para $k = 2$, o toro plano pode também ser visto como o toro usual, superfície do espaço

Figura 4.2: Duas visões do grafo circulante $C_{13}(1,5)$.

euclidiano tri-dimensional (Figura 4.1). Contudo, ele pode ser distinguido deste último por ser análogo a um cilindro em $\mathbb{R}^3$: ele é perfeitamente homogêneo (nenhum ponto pode ser distinguido de um outro) e pode ser "cortado" e planificado em um paralelogramo.

4.1.1 Ladrilhamentos e Grafos sobre o Toro Plano Associados a Grafos Circulantes

Consideremos primeiro o plano $\mathbb{R}^2$ ladrilhado pelo reticulado $\mathbb{Z}^2$, o conjunto L.I. $\alpha = \{\mathbf{u}, \mathbf{v}\}$, onde $\mathbf{u} = (a, b)$, $\mathbf{v} = (c, d)$, a, b, c, d inteiros, e o sub-reticulado Λ_α gerado por $\mathbf{u}$ e $\mathbf{v}$. O quociente $\mathbb{Z}^2/\Lambda_\alpha$ induz um grafo com $n = \det \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ vértices e um ladrilhamento por quadrados sobre o toro plano T_α.

Como um exemplo, para $\mathbf{u} = (3, 2)$ e $\mathbf{v} = (-2, 3)$, temos um grafo $\Gamma_{\{\mathbf{u},\mathbf{v}\}}$ sobre o toro plano com $n = \det \begin{bmatrix} 3 & -2 \\ 2 & 3 \end{bmatrix} = 13$ vértices e a tesselação associada tem também 13 quadrados (Figura 4.2 à direita).

A translação plana vertical pelo vetor $\mathbf{w} = (0, 1)$ induz um rotulamento cíclico em $\Gamma_{\{\mathbf{u},\mathbf{v}\}}$. Notamos que os segmentos verticais sobre o grafo são conectados quando identificamos os lados opostos e os vértices do grafo são localizados sobre esta curva sobre a superfície do toro. Visto no toro do $\mathbb{R}^3$ esta curva fechada é um nó "trefoil". Este rotulamento circular, induz um isomorfismo natural entre o grafo $\Gamma_{\{\mathbf{u},\mathbf{v}\}}$ e o grafo circulante $C_{13}(1, 5)$, que transporta a distância do grafo para o toro plano.

Com este exemplo, surge uma questão natural: para quais bases $\alpha = \{(a, b), (c, d)\}$ e

quais translações planas $\mathbf{w} = (e, f)$ em $\mathbb{R}^2$ podemos afirmar que Γ_α é cíclico e rotulado por $\mathbf{w}$ tal que este rotulamento estabelece um isomorfismo com um grafo circulante?

A seguir, discutiremos esta questão estendida a conexões entre grafos sobre o toro plano k-dimensional e grafos circulantes.

Sejam $\alpha = \{\mathbf{u}_1, \ldots \mathbf{u}_k\}$ uma base de $\mathbb{R}^k$ com coordenadas inteiras e T_α o toro plano associado. A existência do grafo e ladrilhamento de T_α por hipercubos é dada pela próxima proposição.

Proposição 4.1.3. *[25] Seja $\alpha = \{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ uma base de $\mathbb{R}^k$ com coordenadas inteiras, Λ_α o reticulado gerado por α e T_α o toro plano associado. $\mathbb{Z}^k \subset \mathbb{R}^k$ induz, através da aplicação quociente $\overline{\mu}_\alpha$, um grafo regular $\Gamma_\alpha = \dfrac{\mathbb{Z}^k}{\Lambda_\alpha}$ e um ladrilhamento de T_α por hipercubos unitários onde*

a) *$\overline{\mu}_\alpha\left(\mathbb{Z}^k\right)$ são os vértices de Γ_α.*

b) *$\overline{\mu}_\alpha\left([i_1, i_1+1] \times \mathbb{Z}^{k-1}\right) \cup \overline{\mu}_\alpha\left(\mathbb{Z} \times [i_2, i_2+1] \times \mathbb{Z}^{k-2}\right) \cup \ldots \cup \overline{\mu}_\alpha\left(\mathbb{Z}^{k-1} \times [i_k, i_k+1]\right)$, $i_j = 1, \ldots, k$, inteiros, é a união das arestas.*

c) *$\overline{\mu}_\alpha\left([i_1, i_1+1] \times [i_2, i_2+1] \times \ldots \times [i_k, i_k+1]\right)$, $i_j = 1, \ldots, k$, inteiros, são os ladrilhos hipercubos.*

d) *O número de vértices, V, e o número de ladrilhos hipercubos, F, de Γ_α são ambos iguais a $\left|\det\left[\mathbf{u}_1, \ldots, \mathbf{u}_k\right]\right|$.*

As questões naturais são:

1) Quando o grafo Γ_α, dado pelo quociente de reticulados $\Gamma_\alpha = \dfrac{\mathbb{Z}^k}{\Lambda_\alpha}$ é cíclico?

2) Neste caso, onde ele pode ser rotulado ciclicamente por $\overline{\mathbf{w}}$, onde $\mathbf{w} \in \mathbb{Z}^k$, qual é o grafo circulante Γ_α^w associado a Γ_α e $\mathbf{w}$?

O próximo resultado é obtido como consequência da Proposição 23 de [25].

Proposição 4.1.4. *Sob as hipóteses da Proposição 4.1.3, $\Gamma_\alpha = \dfrac{\mathbb{Z}^k}{\Lambda_\alpha}$ é cíclico se, e somente se, existe um vetor $\mathbf{w} = (w_1, \ldots, w_k) \in \mathbb{Z}^k$ e inteiros $h_1, \ldots, h_{k+1}$ tal que*

$$M = \left[\begin{array}{ccc|c} & & & w_1 \\ & A & & \vdots \\ & & & w_k \\ \hline h_1 & \cdots & h_k & h_{k+1} \end{array}\right], \tag{4.3}$$

tem determinante 1*, onde A é uma matriz na qual as colunas são os vetores* $\mathbf{u}_i$*. Neste caso,* $\langle\overline{\mathbf{w}}\rangle = \Gamma_\alpha$.

Demonstração: Para $\mathbf{u}, \mathbf{w} \in \mathbb{Z}^\mathbf{k}$, $\overline{\mathbf{u}}$=$\overline{\mathbf{w}}$ em Γ_α se, e somente se, $\mathbf{u} - \mathbf{w} \in \Lambda_\alpha$. Em outras palavras, existe $\mathbf{x} \in \mathbb{Z}^k$ tal que $A\mathbf{x} = \mathbf{u} - \mathbf{w}$. Assim, a ordem de $\overline{\mathbf{w}}$ é o menor inteiro positivo r tal que o sistema $A\mathbf{x} = r\mathbf{w}$ tem uma solução $\mathbf{x}$ com coordenadas inteiras (fórmula de Crammer).

Como A é invertível, pela fórmula de Crammer o sistema $A\mathbf{x} = \mathbf{w}$ tem uma única solução dada por $\mathbf{x} = |A|^{-1}(|A_1|, \ldots, |A_k|)$, onde a matriz A_i é a matriz A com a i-ésima coluna substituída por $\mathbf{w}$ e $|A| = |\det A|$. Isto significa que $A\mathbf{x}_0 = |A|\mathbf{w}$ tem a solução $\mathbf{x}_0 = (|A_1|, \ldots, |A_k|) \in \mathbb{Z}^k$.

Como $|A| = |\mathbb{Z}^k/\Lambda_\alpha|$, se r é a ordem de $\overline{\mathbf{w}} = \mathbf{w} + \Lambda_\alpha$ então r divide $|A|$. Isto implica que $|A| = rl$, e a única solução de $A\mathbf{x} = r\mathbf{w}$ é dada por $\mathbf{x} = (1/l)\mathbf{x}_0$. Assim, l divide cada $|A_i|$. Agora, para outro inteiro l_1 tal que l_1 divide $|A|, |A_1|, \ldots, |A_k|$, seja r_1 dado por $|A| = r_1 l_1$. Então $r|r_1$, o que implica que $l_1|l$. Isto mostra que $l = mdc\{|A|, |A_1|, \ldots, |A_k|\}$, e que $r = |A|/mdc\{|A|, |A_1|, \ldots, |A_k|\}$.

Γ_α é cíclico se, e somente se, existe $\overline{\mathbf{w}}$ com ordem $|A|$, o qual, pela forma acima satisfaz $mdc\{|A|, |A_1|, \ldots, |A_k|\} = 1$. Isto é equivalente a existir constantes inteiras $h_1, \ldots, h_{k+1}$ tais que

$$h_1|A_1| + \ldots + h_k|A_k| + h_{k+1}|A| = 1. \tag{4.4}$$

Em outras palavras, Γ_α é cíclico se, e somente se, existem $h_1, \ldots, h_{k+1}$ tais que, pelo desenvolvimento de Laplace aplicado a $(k+1)$-linha de M, $\det M$ é igual a
$= (-1)^{k+1}h_1(-1)^{k-1}|A_1| + \ldots + (-1)^{k+k}h_k(-1)^{k-k}|A_k| + (-1)^{2k+2}h_{k+1}|A|$
$= h_1|A_1| + \ldots + h_k|A_k| + h_{k+1}|A| = 1.$

■

O próximo resultado descreve Γ_α como um grafo circulante quando a condição da Proposição 4.1.4 é satisfeita:

Proposição 4.1.5. *Sob as condições da Proposição 4.1.4, a aplicação de rotulamento por* $\mathbf{w}$ *induz um isomorfismo de grafos*

$$\Gamma_\alpha^\mathbf{w} \approx C_n(s_1, \ldots, s_k)$$

onde $n = |\det A|$ *e*

$$s_i = \min\{\textit{Cofator } M_{i\,k+1} \mod n, n - \textit{Cofator } M_{i\,k+1} \mod n\}.$$

Demonstração: A relação de adjacência em Γ_α é a induzida por $\mathbb{Z}^k$. Assim, os vértices adjacentes a $\overline{0}$ são $\pm\overline{\mathbf{e}_i}'s$. Precisamos mostrar que

$$\begin{aligned} s_i\mathbf{w} \approx \mp\mathbf{e}_i &\iff \exists\, r_1, \ldots, r_k \in \mathbb{Z} \text{ tal que } s_i\mathbf{w} \pm \mathbf{e}_i = r_1\mathbf{u}_1 + \cdots + r_k\mathbf{u}_k \\ &\iff r_1\mathbf{u}_1 + \cdots + r_k\mathbf{u}_k - s_i\mathbf{w} = \pm\mathbf{e}_i \iff \end{aligned}$$

$$\begin{cases} r_1 a_{1\,1} + \cdots r_k a_{1\,k} - s_i w_1 = 0 \\ \vdots \\ r_1 a_{i\,1} + \cdots r_k a_{i\,k} - s_i w_i = \pm 1 \\ \vdots \\ r_1 a_{k\,1} + \cdots r_k a_{k\,k} - s_i w_k = 0 \end{cases} \tag{4.5}$$

Podemos garantir que $r_1 = \pm(-1)^{i+1}M_{i\,1}$, ..., $r_k = \pm(-1)^{i+k}M_{i\,k}$ e $s_i = \pm(-1)^{i+k}M_{i\,k+1}$ é a solução para o sistema (4.5). De fato, a i-ésima equação pode ser vista como o desenvolvimento de Laplace de M dado em (4.3) pela i-ésima linha. As outras equações podem ser vistas como o determinante da matriz com duas linhas iguais. Assim $\overline{s_i\mathbf{w}}$ é um vizinho (adjacente a) de $\overline{0}$. Logo $\Gamma_\alpha^{\mathbf{w}}$, o grafo Γ_α rotulado por $\mathbf{w}$, é isomorfo ao grafo circulante $C_n(\pm\overline{s_1}, \ldots, \pm\overline{s_k})$, onde

$$\overline{s_i} = \min\{M_{i\,k+1} \mod n, n - M_{i\,k+1} \mod n\}$$

■

Observação 4.1.1. *A distância do grafo em* $\Gamma_\alpha^{\mathbf{w}}$ *é a induzida pela distância do grafo em* $\mathbb{Z}^k$. *Para* $\overline{a}$, $\overline{b} \in \Gamma_\alpha = \dfrac{\mathbb{Z}^k}{\Lambda_\alpha}$, *temos que:*

$$\mathrm{d}_{\Gamma_\alpha}(\overline{a}, \overline{b}) = \min\left\{\sum_{i=1}^{k} |a_i - b_i|, a = (a_1, \ldots, a_k) \in \overline{a} \textit{ and } b = (b_1, \ldots, b_k) \in \overline{b}\right\}.$$

Para outro $\mathbf{w}'$, e $h'_1, \ldots, h'_{k+1}$ satisfazendo (4.3) obtemos, pela Proposição 4.1.4, um grafo circulante diferente $C_n(s'_1, \ldots, s'_k)$, mas ambos devem ser isomorfos, como veremos a seguir.

Proposição 4.1.6. *Se existirem outros* $\mathbf{w}'$ *e* $\mathbf{h}'$ *satisfazendo a Proposição 4.1.4 para a mesma submatriz A de M (4.3), então*

$$C_n(a_1, \ldots, a_k) \approx C_n(a'_1, \ldots, a'_k).$$

Demonstração: Pela Proposição 4.1.4, $\Gamma_\alpha^{\mathbf{w}}$ e $\Gamma_\alpha^{\mathbf{w}'}$ são cíclicos e gerados por $\overline{\mathbf{w}}$ e $\overline{\mathbf{w}'}$, respectivamente. Assim $\langle\overline{\mathbf{w}}\rangle = \langle\overline{\mathbf{w}'}\rangle$, o que significa que existem inteiros r, t primos com n tal que $\overline{\mathbf{w}} = r\overline{\mathbf{w}'}$ e $\overline{\mathbf{w}'} = t\overline{\mathbf{w}}$. Em outras palavras,

$$\overline{\mathbf{w}} = r\overline{\mathbf{w}'} = rt\overline{\mathbf{w}} \Longleftrightarrow rt = 1 \mod n.$$

Contudo $\mathbf{e}_i \approx a_i\mathbf{w} \approx a_i r\mathbf{w}'$ e $\mathbf{e}_i \approx a'_i\mathbf{w}'$, então $\overline{a'_i\mathbf{w}'} = \overline{a_i r\mathbf{w}'}$. Assim $a'_i \approx a_i r \mod n$ e então

$$C_n(a_1, \ldots, a_k) \approx C_n(a'_1, \ldots, a'_k).$$

■

Exemplo 4.1.1. *O lado direito da Figura 4.2 mostra o grafo circulante* $C_{13}(1,5)$ *sobre o toro planar gerado por* $v_1 = (3,2)$ *e* $v_2 = (-2,3)$ *rotulado por* $\mathbf{w} = (0,1)$ *(*$h_1 = 1, h_2 = -1, h_3 = 0$*). Se considerarmos um rotulamento por* $\mathbf{w}' = (1,1)$ *(*$h_1 = h_3 = 0$ *e* $h_2 = -1$*), temos, pela Proposição 4.1.4,* $C_{13}(2,3)$ *sobre o toro planar com o mesmo conjunto de vértices (Figura 4.3). De acordo com a Proposição 4.1.6 esses grafos circulantes são isomorfos.*

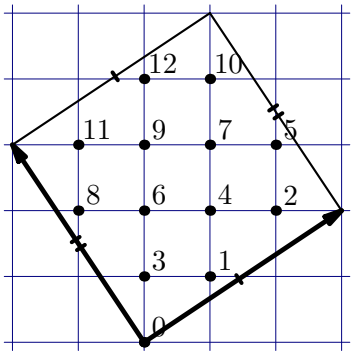


Figura 4.3: O grafo circulante $C_{13}(2,3) \approx C_{13}(1,5)$ rotulado por $\mathbf{w} = (1,1)$

4.1.2 Grafos Circulantes Realizados como Grafos sobre o Toro Plano

Pela Proposição 4.1.5 vemos que nem todos os grafos que ladrilham um toro plano por hipercubos nos dão um grafo circulante, mas a recíproca é verdadeira como veremos na próxima proposição. A prova deste resultado é baseada na Proposição 10 de [36] adaptada para nosso contexto.

Proposição 4.1.7. *Qualquer grafo circulante conexo $C_n(a_1, \ldots, a_k)$ de grau $2k$ com vértices $\{v_1, \ldots, v_n\}$ é isomorfo a um grafo Γ_α que tessela um toro plano k-dimensional T_α por hipercubos. Isto é, existe uma base $\alpha = \{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ de $\mathbb{R}^k, \mathbf{u}_i \in \mathbb{Z}^k$ e um vetor $\mathbf{w} \in \mathbb{Z}^k$ tais que, para o reticulado $\Lambda_\alpha = \langle u_1, \ldots, u_k \rangle$,*

$$\Gamma_\alpha^w = \frac{\mathbb{Z}^k}{\Lambda_\alpha} = \langle \overline{\mathbf{w}} \rangle \approxeq \mathbb{Z}_n \text{ e } \Psi(v_i) = i\overline{\mathbf{w}} \text{ é um isomorfismo de grafo.}$$

Demonstração: Primeiro notamos que como $C_n(a_1, \ldots, a_k)$ é conexo, $mdc(a_1, \ldots, a_k, n) = 1$ e assim existem inteiros $w_1, \ldots, w_{k+1}$ tais que

$$w_1 a_1 + \cdots + w_k a_k + n w_{k+1} = 1. \tag{4.6}$$

Consideremos $\tilde{\mathbf{w}} = (w_1, \ldots, w_{k+1})$. Para $\mathbf{s} = (a_1, \ldots, a_k, n)$, tome a base $\tilde{\alpha} = \{\tilde{\mathbf{u}}_1, \ldots, \tilde{\mathbf{u}}_k\}$, $\tilde{\mathbf{u}}_i = (u_{1\,i}, \ldots, u_{k+1\,i}) \in \mathbb{Z}^{k+1}$, do sub-reticulado de $\mathbb{Z}^{k+1}$ definido pelo hiperplano $\mathbf{s}^\perp$ ortogonal a $\mathbf{s}$ em $\mathbb{R}^{k+1}$ e $A = \{u_{i\,j}\}$. Mostraremos a seguir que a matriz $(k+1) \times (k+1)$ M no qual as colunas são $\tilde{\mathbf{u}}_1, \ldots, \tilde{\mathbf{u}}_k$ e $\tilde{\mathbf{w}}$ tem determinante igual a um e sua submatriz superior esquerda A tem determinante n:

$$M = \left[\begin{array}{ccc|c} u_{1\,1} & \cdots & u_{k\,1} & w_1 \\ \vdots & \ddots & \vdots & \vdots \\ u_{k\,1} & \cdots & u_{k\,k} & w_k \\ \hline u_{k+1\,1} & \cdots & u_{k+1\,k} & w_{k+1} \end{array}\right], \ \det(M) = 1. \tag{4.7}$$

A afirmação desta proposição será então derivada da Proposição 4.1.4 tomando $\alpha = \{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ e $\mathbf{w}$ onde $\mathbf{u}_i$ e $\mathbf{w}$ são obtidos de $\tilde{\mathbf{u}}_i$ e $\tilde{\mathbf{w}}$ desprezando a última coordenada.

Seguindo [36], consideramos a aplicação:

$$\begin{array}{rccc} \varphi: & \mathbb{Z}^k & \longrightarrow & \mathbb{Z}_n \\ & (x_1, \ldots, x_k) & \longmapsto & \overline{x_1\, a_1 + \ldots + x_k\, a_k} \end{array},$$

a qual é um isomorfismo de grupo. Assim por (4.6) $\varphi(\mathbf{w}) = \varphi(w_1, w_2, \ldots, w_k) = \overline{1}$, e φ é injetiva. Seu núcleo é um reticulado Λ em $\mathbb{R}^k$ satisfazendo

$$\mathrm{vol}(\Lambda) = \left|\frac{\mathbb{Z}^k}{\Lambda}\right| = |\mathbb{Z}_n| = n.$$

Note que $\alpha = \{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ definido como acima é uma base para este reticulado pois $\mathbf{v} \in \Lambda \iff \exists \lambda \in \mathbb{Z}; (\mathbf{v}, \lambda) \in \mathbf{s}^{\perp} \cap \mathbb{Z}^k$. Isto implica que

$$|\det(A)| = \mathrm{vol}(\Lambda) = n.$$

Consideraremos $\det(A) = n$ permutando dois vetores nesta base, se necessário.

De volta a $\mathbb{R}^{k+1}$, escolhemos $\mathbf{m} = (m_1, \ldots, m_{k+1})$ como o produto vetorial $\mathbf{u}_1 \wedge \cdots \wedge \mathbf{u}_k$, o qual é o único vetor tal que

$$\mathbf{u} \cdot \mathbf{m} = \det[\mathbf{u}_1, \ldots, \mathbf{u}_k, \mathbf{u}]$$

para todo $\mathbf{u} \in \mathbb{R}^{k+1}$. As coordenadas deste produto vetorial podem ser escritas usando a última coluna dos cofatores da matriz M dada acima: $m_i = M_{i\,k+1}$ [37]:

$$m_i = \mathbf{e}_i \cdot \mathbf{u} = \det[\mathbf{u}_1, \ldots, \mathbf{u}_k \mathbf{e}_i] = M_{j\,k+1}$$

e, em particular, $m_{k+1} = \det(A) = n$. Além disso,

$$\mathbf{u}_i \cdot \mathbf{m} = \det[\mathbf{u}_1, \ldots, \mathbf{u}_k, \mathbf{u}_i] = 0;$$

pois os $\mathbf{u}_i$'s formam uma base do hiperplano ortogonal a $\mathbf{s}$. Logo, concluímos que $\mathbf{m} = \lambda \mathbf{s}$ para algum $\lambda \in \mathbb{R}$. Assim, de (4.7) obtemos $m_{k+1} = \det(A) = \lambda \det(A)$, i.e., $\lambda = 1$ e $\mathbf{m} = \mathbf{s}$. Desenvolvendo o determinante da matriz $M = [\tilde{\mathbf{u}}_1, \ldots, \tilde{\mathbf{u}}_k, \tilde{\mathbf{w}}]$, pela última coluna temos então

$$\det(M) = \widetilde{\mathbf{w}} \cdot \mathbf{m} = \widetilde{\mathbf{w}} \cdot \mathbf{s} = 1,$$

o qual conclui nossa prova. ■

Exemplo 4.1.2. *Para construir Γ_α^w isomorfo a $C_{13}(3,5)$ devemos encontrar uma base para o reticulado $\mathbb{Z}^3 \cap (3,5,13)^{\perp}$. Usando a forma normal de Hermite, temos a base $\{u_1, u_2\}$, onde $u_1 = (-5,3,0)$ e $u_2 = (1,2,-1)$ e o vetor $\widetilde{w} = (2,-1,0)$. Assim, o toro plano será gerado pelos vetores $v_1 = (1,2)$ e $v_2 = (-5,3)$ e temos $\Gamma_\alpha^w \approx C_{13}(3,5)$, rotulado por $w = (2,-1)$ (Figura 4.4). Como 9 é o inverso de 3 em $\mathbb{Z}_{13}$, segue que $C_{13}(3,5) \approx C_{13}(1,6)$.*

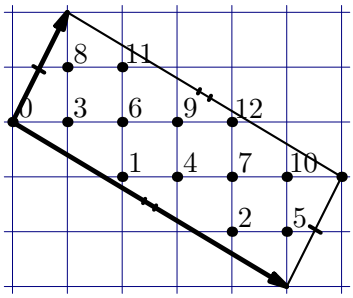


Figura 4.4: O grafo circulante $C_{13}(3,5)$ sobre o toro plano, rotulado por $\mathbf{w} = (2,-1)$.

Observação 4.1.2. *Dado o grafo circulante $C_n(a_1,\ldots,a_n)$, a maneira de construir uma matriz M como em (4.3) e seu correspondente grafo isomorfo Γ_α^w sobre um toro plano está longe de ser única. As condições usadas na construção da Proposição, as quais implicam nas k primeiras colunas serem ortogonais a $(a_1,\ldots,a_k,n)$, é uma condição suficiente mas não necessária. Como vimos no Exemplo 4.1.1,*

$$M = \begin{bmatrix} 3 & -2 & 0 \\ 2 & 3 & 1 \\ -1 & -1 & 0 \end{bmatrix}$$

produz, pela Proposição 4.1.7, o grafo circulante $C_{13}(1,5)$.

4.2 Limitantes para o Número de Vértices de um Grafo Circulante com Grau $2k$ e Diâmetro d.

Uma questão pertinente, a qual tem sido respondida para casos específicos é: para um dado diâmetro d, qual é o número máximo de vértices $n = \rho(d,k)$ para o qual existe um grafo circulante $C_n(a_1,...,a_k)$ com diâmetro d de grau $2k$?

Uma aplicação para grafos otimizados neste sentido está na construção de redes de intercomunicações para processamento paralelo, onde queremos ter um grande número de processadores sem requerer um grande número de conexões a um único processador ou uma longa demora nas mensagens de um processador para outro.

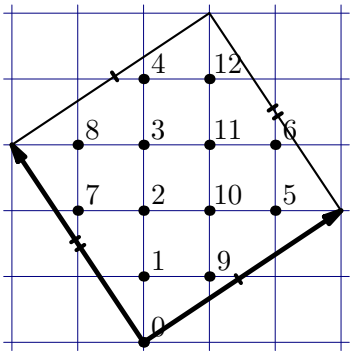
Uma abordagem geométrica da questão proposta acima pode ser dada pela Proposição 4.1.7.

Comecemos com $k = 2$. Como uma bola (sobre a distância do reticulado) em $\mathbb{Z}^2$ de raio d tem precisamente $\mu_2(d) = 1 + 4 + 4 \cdot 2 + ... + 4\,d = (d+1)^2 + d^2$ vértices e, pela Proposição 4.1.7, qualquer grafo circulante de grau 4 pode ser visto como um grafo e ladrilhamento induzido por $\mathbb{Z}^2$ sobre o toro plano, $\mu_2(d)$ deve ser um limitante superior para n neste caso.

Este é um limite conhecido obtido via teoria combinatória. A abordagem geométrica aqui apresentada permite ver porque este número pode ser alcançado para $C_{(d+1)^2+d^2}(1, 2d+1)$. De fato, podemos ver que este grafo circulante pode ser obtido por uma matriz construída como na Proposição 4.1.4,

$$M = \left[\begin{array}{cc|c} d+1 & -d & 0 \\ d & d+1 & 1 \\ \hline 1 & -1 & 0 \end{array}\right], \ \det(M) = 1,$$

e assim os vetores definidos sobre o toro plano e o reticulado Λ são $v_1 = (d+1, d)$ e $v_2 = (-d, d+1)$, $\det(A) = (d+1)^2 + d^2$, $s_1 = 2d+1$ e $s_2 = 1$.



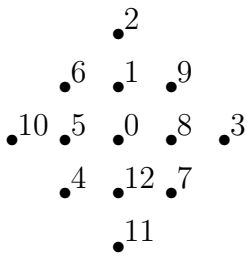


Figura 4.5: $C_{13}(1, 5)$ representado como $\frac{\mathbb{Z}^2}{\Lambda} = \Gamma_\alpha$ sobre o toro plano gerado por $\alpha = \{(3, 2), (-2, 3)\}$ e representantes de Γ_α mais próximos da origem.

Os representantes de $\dfrac{\mathbb{Z}^2}{\Lambda}$ mais próximos da origem irão compor uma bola de raio d em $\mathbb{Z}^2$. Também $C_{(d+1)^2+d^2}(1, 2d+1)$ é o grafo circulante de grau 4 mais denso para um dado diâmetro d.

Para $k = 3$, uma bola em $\mathbb{Z}^3$ de raio d pode ser considerada como camadas da bolas 2-dimensionais: Uma $2D$-bola de raio d no nível zero, uma $2D$-bola de raio $d-1$ nos níveis 1 e -1, ..., uma $2D$-bola de raio $d-j$ nos níveis j e $-j$, para $j = 1, \ldots, d$. Assim, o número

de vetores da bola de raio d em $\mathbb{Z}^3$ é:

$$\mu_3(d) = (d+1)^2 + d^2 + 2\sum_{j=1}^{d}(j+1)^2 + j^2 = \frac{1}{3}(4d^3 + 6d^2 + 8d + 3)$$

A expressão para o número de vértices, $\mu_k(d)$, da bola de raio d em $\mathbb{Z}^k$ pode ser deduzida recursivamente (bolas na mais baixa próxima dimensão) e expressa como

$$\mu_k(d) = \mu_{k-1}(d) + 2\sum_{j=1}^{d}\mu_{k-1}(d-j). \tag{4.8}$$

Também podemos deduzir

$$\mu_k(d) = \sum_{j=0}^{k} 2^j k!d!/((k-j)!(d-j)!(j!)^2) = Hypergeometric2F1[-d,-k,1,2]. \tag{4.9}$$

Para esta última expressão $\mu_k(d)$ pode ser explicitamente dada como um polinômio de grau k em d (usamos o programa Mathematica para esses cálculos):

$$\begin{aligned}
\mu_2(d) &= 1 + 2\,d + 2\,d^2\\
\mu_3(d) &= \tfrac{3+8\,d+6\,d^2+4\,d^3}{3}\\
\mu_4(d) &= \tfrac{3+8\,d+10\,d^2+4\,d^3+2\,d^4}{3}\\
\mu_5(d) &= \tfrac{15+46\,d+50\,d^2+40\,d^3+10\,d^4+4\,d^5}{15}\\
\mu_6(d) &= \tfrac{45+138\,d+196\,d^2+120\,d^3+70\,d^4+12\,d^5+\ 4\,d^6}{45}\\
\mu_7(d) &= \tfrac{315+1056\,d+1372\,d^2+1232\,d^3+490\,d^4+224\,d^5+\ 28\,d^6+8\,d^7}{315}\\
\mu_8(d) &= \tfrac{315+1056\,d+1636\,d^2+1232\,d^3+798\,d^4+224\,d^5+\ 84\,d^6+8\,d^7+2\,d^8}{315}\\
\mu_9(d) &= \tfrac{2835+10134\,d+14724\,d^2+14360\,d^3+7182\,d^4+\ 3612\,d^5+756\,d^6+240\,d^7+18\,d^8+4\,d^9}{2835}
\end{aligned}$$

Novamente, vemos, através da Proposição 4.1.5, que $\mu_k(d)$ *é um limite superior para o número máximo de vértices de um grafo circulante de grau* $2k$ *e diâmetro* d. Este limite geometricamente indica como (4.8) foi deduzido em [31] usando técnicas de contagem combinatória.

É importante observar que, ao contrário do que acontece no caso $2D$ ($k = 2$), este limite pode não ser alcançado. Por exemplo, para $k = 3$ e $d = 2$ temos $\mu_3(2) = 25$ e o número máximo de vértices neste caso é 21. A este respeito em [32] é provado que para todo $d \geq 0$,

existe um grafo de Cayley (de fato, cíclico) o qual tem diâmetro d e tamanho n, onde

$$n = \begin{cases} (32d^3 + 48d^2 + 54d + 27)/27 & \text{if } d = 0(\mod 3) \\ (32d^3 + 48d^2 + 78d + 31)/27 & \text{if } d = 1(\mod 3) \\ (32d^3 + 48d^2 + 54d + 11)/27 & \text{if } d = 2(\mod 3) \end{cases},$$

os autores conjecturaram que os grafos dados por este teorema são realmente os maiores grafos de Cayley de grupos abelianos sobre três geradores para cada diâmetro d. Note que um grafo circulante de ordem n é um grafo de Cayley sobre $\mathbb{Z}_n$.

A abordagem de grafos circulantes como grafos em toros planares que fizemos permite uma explanação geométrica pela qual o limite superior $\mu_k(d)$ nem sempre é alcançado é que o alcance de tal limite requer a existência de um ladrilhamento de $\mathbb{Z}_d^k$, por bolas completas de diâmetro d, induzidas por translações de $(a_1, \ldots, a_k)$. Como vimos, isto é possível para $k = 2$ e qualquer d. Para $k > 2$ e $d > 2$ isto não será possível pois o poliedro k-dimensional associado à "bola" não ladrilha $\mathbb{R}^k$.

Perspectivas Futuras

Neste trabalho pudemos verificar, através de propriedades geométricas como redução de base, que a transformação de mudança de base mostrada na Subseção 2.2.2 do Capítulo 2, a qual permitiu concluir pelos resultados obtidos do artigo conjunto [22], corresponde às transformações do algoritmo de redução de Minkowski. No Teorema 3.1.1 mostramos que um reticulado apresenta uma base ortogonal ordenada se, e somente se, sua base reduzida de Minkowski é igual a essa base, a menos de reordenação. Logo, com esse resultado passa a ser possível a verificação, dada a matriz de Gram, se um reticulado algébrico com tal matriz é ou não um $\mathbb{Z}^n$-rotacionado. Como uma linha de pesquisa futura, acreditamos que o mesmo resultado valha para o algoritmo LLL, fato que conseguimos verificar até agora apenas nas dimensões 2 e 3. A vantagem de obtermos também este critério está na complexidade mais baixa do algoritmo, o que permitirá, na prática, que os "testes"sejam feitos em dimensões muito mais altas.

Na segunda construção sobre o p^r-ésimo corpo ciclotômico (Subseção 3.2.1), onde usamos o elemento α obtido de [24], o que fizemos foi verificar através da redução de base, o isomorfismo provado no Teorema 3.2.1. Na primeira construção (Subseção 3.2.1), não obtivemos a caracterização geométrica em todas as dimensões $n = (p-1)p^{r-1}/2$. Uma linha de pesquisa para trabalhos futuros seria exatamente obter condições sobre o primo p e o inteiro positivo r para os quais os reticulados associados são somas ortogonais dos reticulados clássicos. Também pretendemos pesquisar novos elementos α, que gerem novas famílias de reticulados com boas propriedades e que possam eventualmente ser classificados através de redução de

base.

Uma outra perspectiva de pesquisa é a ligada a códigos geometricamente uniformes em toros planares [25]. Uma interessante abordagem seria a de usar teoria de reticulados ideais para expressar diversidade e distância produto mínima destas constelações que são quocientes de reticulados. Um caso especialmente interessante, pela possibilidade da obtenção de códigos esféricos associados a este quociente, é a procura de reticulados algébricos com boa densidade de empacotamento e contendo sub-reticulados admitindo bases ortogonais.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] S. Benedetto, E. Biglieri, *Principles of Digital Transmission With Wireless Applications*, Kluwer Academic / Plenum Publishers, New York, 1999.

[2] J. Boutros, E. Viterbo, C. Rastello, J. Belfiore, *Good Lattice Constellations for Both Rayleigh Fading and Gaussian Channels*, IEEE Trans. on Inform. Theory, 42 (1996) 502-518.

[3] P. Samuel, *Algebraic theory of numbers*, ed. Hermann, Paris, 1971.

[4] I. N. Stewart e D.O. Tall, *Algebraic Number Theory*, Chapman and Hall, London, 1979.

[5] O. Endler, *Teoria dos Números Algébricos*, Projeto Euclides, Rio de Janeiro, 1986.

[6] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer, New York, 2001.

[7] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer - 2^o Edição, 1982.

[8] J. Esmonde e M. Ram Murty, *Problems in Algebraic Number Theory*, Springer, 1991.

[9] D. A. Marcus, *Number Fields*, Springer-Verlag, 1977.

[10] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993.

[11] J. H. Conway e N.J.A. Sloane, *Sphere Packings, Lattices and Groups* - especialmente os capítulos $1, 2, 3$ e 4, Springer, 1999.

[12] E. Viterbo e E. Biglieri, *A universal lattice decoder*, 14^{eme} Colloque GRETSI, Juan-les-Pins, 611-614, Sept. 1993.

[13] E. Bayer-Fluckiger, F. Oggier e E. Viterbo, *New Algebraic Constructions of Rotated* $\mathbb{Z}^n$*-Lattice Constellations for the Rayleigh Fading Channel*, IEEE Trans. on Inform. Theory, Vol.50, n^o4, April 2004, 702-714.

[14] F. Oggier, *Algebraic Methods for Channel Coding*, Tese de Doutorado, Lausanne - EPFL, 2005.

[15] E. Bayer-Fluckiger, F. Oggier e E. Viterbo, *Algebraic Lattice Constellations: Bounds on Performance*, IEEE Trans. on Inform. Theory, Vol.52, n^o1, January 2006, 319-327.

[16] E. Bayer-Fluckiger, *Lattices and Number Fields*, Contemporary Mathematics, Vol. 241, 1999, 69-84.

[17] E. Bayer-Fluckiger, *Ideal Lattices*, 168-184.

[18] J. O. D. Lopes, T. P. da N. Neto, J. C. Interlando, *On computing discriminant of subfields of* $\mathbb{Q}(\xi_{p^r})$, Journal of Number Theory, Vol. 96, n^o2, October 2002, 319-325.

[19] J. O. D. Lopes, *Discriminant of Subfields of* $\mathbb{Q}(\xi_{2^r})$, Journal of Algebra and Its Applications, Vol. 2, December 2003, 463-469.

[20] J. O. D. Lopes, T. P. da N. Neto, J. C. Interlando, *The Discriminant of Abelian Number Fields*, Journal of Algebra and Its Applications, Vol. 5, n^o1, January 2006, 1-7.

[21] A. L. Flores, *Reticulados em Corpos Abelianos*, Tese de Doutorado, FEEC-Unicamp, Campinas-SP, (2000).

[22] A. A. Andrade, C. Alves e T. B. Carlos , *Rotated Lattice via the Cyclotomic Field* $\mathbb{Q}(\zeta_{2^r})$, International Jounal of Applied Mathematics, Vol.19, n^o3, 321-331, 2006.

[23] A. A. Andrade, C. Alves e T. B. Carlos , *Rotated Lattice via the Cyclotomic Field* $\mathbb{Q}(\zeta_{p^r})$, a ser publicado.

[24] E. Bayer-Fluckiger, *Upper bounds for Euclidean minima*, J. Number Theory (to appear).

[25] S. I. R. Costa, M. Muniz, E. Agustini and R. Palazzo, Graphs, Tessellations, and Perfect Codes on Flat Tori, IEEE Trans. Inform. Theory, 50(10) (2004) 2363-2378.

[26] J. Stillwell, Geometry and Surfaces, New York, Springer Verlag, 1992.

[27] C. Martínez, R. Beivide, J. Gutierrez e E. Gabidulin, *On the Perfect t-Dominating Set Problem in Circulant Graphs and Codes over Gaussian Integers*, ISIT 2005 IEEE, Australia.

[28] C. Martínez, R. Beivide, C. Izu e J. Miguel-Alonso, *Characterization of the Class of Optimal Dense Circulant Graphs of Degree Four*, XIV Jornadas de Paralelismo - Leganés, Setembro 2003.

[29] A. Adam, Research problem 2-10, J. Combinatorial Theory, 2 (1967) 393.

[30] F. Boesch, R. Tindell, Circulant and Their Connectivities, J. of Graph Theory, 8 (1984) 487-499.

[31] F. P. Muga II, Undirected Circulant Graphs, International Symposium on Parallel Architectures, Algorithms and Networks, (1994) 113-118.

[32] R. Dougherty and V. Faber, The Degree-Diameter Problem for Several Varieties of Cayley Graphs, I: The Abelian Case, SIAM J. Discret Math. 17(3) (2004) 478-519.

[33] S.I.R. Costa, J.E.Strapasson, T.B. Carlos, M. Muniz, *Circulant Graphs Viewed as Graphs on Flat Tori*, Pré-print.

[34] J.E.Srapasson, *Geometria Discreta e Códigos*, Tese de Doutorado, UNICAMP, Campinas, 2007.

[35] S.I.R. Costa, J.E. Strapasson, M. Muniz, R.M. Siqueira, *Circulant graphs, lattices and spherical codes*, (aceito) Int. Journal of Applied Mathematics, 2007.

[36] C. Heuberger, On planarity and colorability of circulant graphs, Discret Mathematics, 268 (2003) 153-169.

[37] M. Spivak, Calculus on Manifolds, Perseu Books Publishing, 1965.

ÍNDICE REMISSIVO