UNIVERSIDADE ESTADUAL
PAULISTA "JÚLIO DE MESQUITA FILHO"
Câmpus de Ilha Solteira

AZUCENA MIREYA DUARTE ZELAYA

CODIFICAÇÃO DE CANAIS EM SISTEMAS DE COMUNICAÇÃO SEM FIO BASEADO EM RETICULADOS

Ilha Solteira
2015

AZUCENA MIREYA DUARTE ZELAYA

CODIFICAÇÃO DE CANAIS EM SISTEMAS DE COMUNICAÇÃO SEM FIO BASEADO EM RETICULADOS

Dissertação apresentada à Faculdade de Engenharia do Câmpus de Ilha Solteira - UNESP como parte dos requisitos para obtenção do título de Mestre Engenharia Elétrica.
Especialidade: Automação.

Prof. Dr. Jozué Vieira Filho
Orientador
Prof. Dr. Edson Donizete de Carvalho
Co-orientador

Ilha Solteira
2015

FICHA CATALOGRÁFICA
Desenvolvido pelo Serviço Técnico de Biblioteca e Documentação

D812c

Duarte Zelaya, Azucena Mireya .
Codificação de canais em sistemas de comunicação sem fio baseado em reticulados / Azucena Mireya Duarte Zelaya. -- Ilha Solteira: [s.n.], 2015
59 f. : il.

Dissertação (mestrado) - Universidade Estadual Paulista. Faculdade de Engenharia de Ilha Solteira. Área de conhecimento: Automação, 2015

Orientador: Jozué Vieira Filho
Co-orientador: Edson Donizete De Carvalho
Inclui bibliografia

1. Corpos ciclotômicos. 2. Códigos reticulados. 3. Quantização de canal.

unesp

UNIVERSIDADE ESTADUAL PAULISTA

CAMPUS DE ILHA SOLTEIRA

FACULDADE DE ENGENHARIA DE ILHA SOLTEIRA

CERTIFICADO DE APROVAÇÃO

TÍTULO: Codificação de canais em sistemas de comunicação sem fio baseado em reticulados

AUTORA: AZUCENA MIREYA DUARTE ZELAYA

ORIENTADOR: Prof. Dr. JOZUE VIEIRA FILHO

CO-ORIENTADOR: Prof. Dr. EDSON DONIZETE DE CARVALHO

Aprovada como parte das exigências para obtenção do Título de Mestre em Engenharia Elétrica , Área: AUTOMAÇÃO, pela Comissão Examinadora:

Prof. Dr. EDSON DONIZETE DE CARVALHO Edson D. Carvalho
Departamento de Matemática / Faculdade de Engenharia de Ilha Solteira

Prof. Dr. FRANCISCO VILLARREAL ALVARADO
Departamento de Matemática / Faculdade de Engenharia de Ilha Solteira

Prof. Dr. EDUARDO BRANDANI DA SILVA
Departamento de Matemática / Universidade Estadual de Maringa

Data da realização: 24 de fevereiro de 2015.

À minha família Duarte Zelaya, minha mãe Azucena, minha irmã Merary e meu irmão David.

AGRADECIMENTOS

Meus agradecimentos à minha família, Duarte Zelaya; à minha amiga Licien Moncada; aos professores Jozué Vieira Filho e Rubén Romero por acreditarem em mim; ao professor Edson Donizete de Carvalho por compartilhar comigo seus conhecimentos. Ao Brasil e, em particular, ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pela oportunidade e apoio financeiro.

“Todos o Ninguno”

RESUMO

A partir da teoria algébrica dos números e com base na estratégia compute-and-forward, propõe-se um método eficiente para quantização de coeficientes de um canal associado a problemas de comunicação em redes sem fio. O desenvolvimento desta técnica é realizado via partição de cadeias de reticulados definidas sobre o anel de inteiros de Eisentein Jacobi, obtidos a partir de corpos ciclotômicos $\mathbb{Q}(\zeta_{9.2^s})$ com $s \geq 2$, onde $\zeta_{9.2^s}$ denota a raíz 9.2^s-ésima da unidade.

Palavras-chave: Números algébricos. Estratégia compute-and-forward. Reticulados-Eisentein Jacobi.

ABSTRACT

From the algebraic number theory results, we propose an efficient method based on the compute-and-forward strategy for the quantization of channel coefficients. This procedure is based on Eisentein-lattices partition chain developed from the algebraic tool from the cyclotomic field $\mathbb{Q}(\zeta_{9.2^s})$ with $s \geq 2$, where $\zeta_{9.2^s}$ denotes the 9.2^s-th root of unity.

Keywords: Algebraic number. Compute-and-forward strategy. Eisentein-lattices.

LISTA DE FIGURAS

Figura 1- Modelo básico de sistemas de comunicação. 12

Figura 2- Modelo sistemas de comunicação digital. 13

Figura 3- Interferência de canal Gaussiano. 16

Figura 4- Interferência de canal Gaussiano, Modelo Completo. 17

Figura 5- Subgrupo. 23

Figura 6- Extensão de corpo $\mathbb{Q}(i)$ sobre $\mathbb{Q}$ 28

Figura 7- Extensão de corpo $\mathbb{Q}(\omega)$ sobre $\mathbb{Q}$ 28

Figura 8- Extensão Corpos Ciclotômico. 31

Figura 9- Reticulado. 33

Figura 10- Reticulado aninhado. 37

Figura 11- Reticulado $\mathbb{Z}^n$ $n = 2$. 37

Figura 12- Reticulado A n=2 38

Figura 13- Sistema MIMO numa rede AWGN. 41

Figura 14- Cadeia de Extensão de Corpos. 45

Figura 15- Grau da extensão de corpo. 46

LISTA DE TABELAS

Tabela 1- Classe Laterais à esquerda 24

Tabela 2- Exemplo de classes laterais 26

SUMÁRIO

1	**INTRODUÇÃO**	**12**
2	**REVISÃO DE ÁLGEBRA ABSTRATA**	**21**
2.1	GRUPO	21
2.1.1	**Grupo quociente**	**25**
2.2	ANÉIS	26
2.3	CORPOS	27
2.3.1	**Mergulho e grupo galois**	**29**
2.4	CORPOS CICLOTÔMICOS	30
3	**RETICULADOS ALGÉBRICOS**	**32**
3.1	DEFINIÇÕES FUNDAMENTAIS	32
3.2	PROPRIEDADES GEOMÉTRICAS DOS RETICULADOS	34
3.2.1	**Sub-reticulados, reticulados equivalentes e reticulados aninhados**	**35**
3.3	TIPOS DE RETICULADOS	37
3.4	RETICULADOS COMPLEXOS	38
4	**QUANTIZAÇÃO DE CANAL BASEADO NA TEORIA DE NÚMEROS ALGÉBRICOS**	**40**
4.1	ESTRATÉGIA COMPUTER-AND-FORDWARD	40
4.2	ESTRATÉGIA COMPUTE-AND-FORWARD BASEADA EM RETICULADOS SOBRE $\mathbb{Z}[\omega]$	41
5	**DESENVOLVIMENTO DA PROPOSTA**	**44**
5.1	PARTE I: TEORIA DE CORPOS ALGEBRICOS	44
5.2	PARTE II: APROXIMAÇÂO DOS COEFICIENTES DO CANAL H	47

5.2.1 Construção de reticulados aninhados sobre $\mathbb{Z}[\omega]$ **47**

5.2.2 Construção da cadeia de reticulados aninhados sobre $\mathbb{Z}[\omega]$ **49**

6 CONCLUSÕES **53**

REFERÊNCIAS **55**

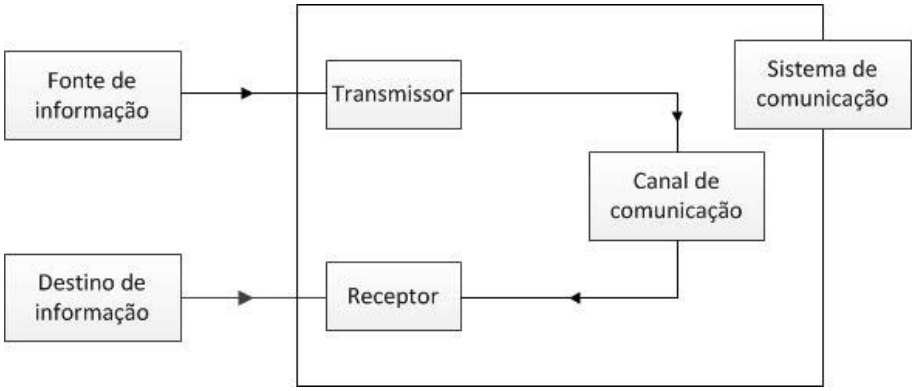
APÊNDICE A - IDEAIS PRIMOS TOTALMENTE RAMIFICADOS NA EXTENSÃO $\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(\omega)$ **57**

1 INTRODUÇÃO

A constante busca pelo homem por uma comunicação confiável vem desde os primórdios da história da humanidade e foi se modificando, adequando-se aos avanços tecnológicos e científicos. No início, o homem desenhava o que via ao seu redor, guardando a informação. Depois, o avanço acontece com a introdução do papel e da caneta, quando o homem começa a escrever e registrar, de forma natural, surgindo assim as linguagens como regras de comunicação.

As formas de se estabelecer uma comunicação mudaram ao longo dos tempos, mas o conceito básico de comunicação é o mesmo, ou seja: transferir informação de um ponto para outro. Neste contexto, entende-se como ponto um conjunto de equipamentos que são capazes de transmitir e/ou receber informação. Este conjunto de equipamentos é chamado de sistema de comunicação e é formado por: transmissor, receptor e canal (ver Figura 1). Neste trabalho o foco é o canal de comunicação que, apesar dos avanços tecnológicos, ainda é um dos principais limitadores para altas taxas de transmissão e recepção. Particularmente, o canal aqui explorado é o espaço livre, o que caracteriza uma comunicação sem-fio.

Figura 1 - Modelo básico de sistemas de comunicação.

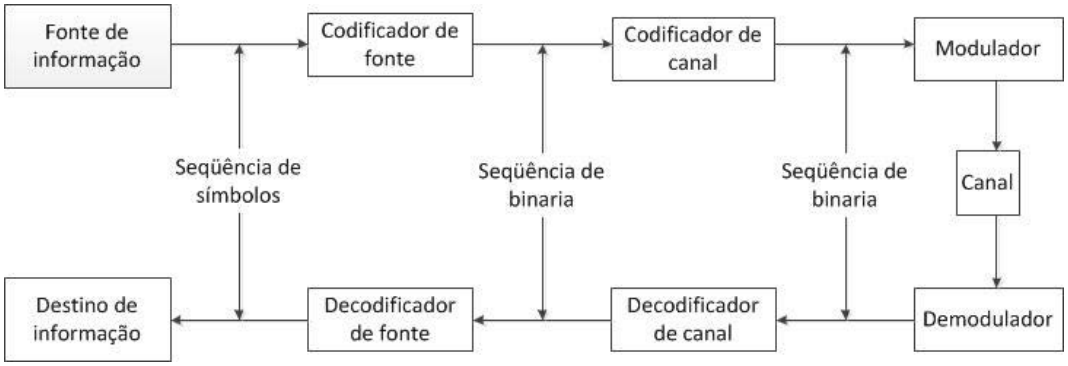


Fonte: Shammugam (1979)

A entrada de um sistema de comunicação pode ser analógica ou digital, mas a fonte de informação é, normalmente, um sinal analógico, como por exemplo, a voz, que é captada por um microfone para posterior modulação e transmissão através de um determinado canal. O canal realiza a conexão entre a fonte e o receptor da mensagem por diferentes formas como, por exemplo, ondas eletromagnéticas, fios de cobre ou fibra óptica. Assim, a tarefa do transmissor é enviar um sinal que passa por diferentes processos, como filtragem, amplificação e modulação, através do canal, enquanto que a tarefa do receptor é obter o mesmo sinal transmitido na saída do

canal. Através da modulação, é possível modificar o ruído e as interferências do sinal, gerando diferentes formas de onda com amplitude, frequência e fase, que trabalham como portadora do sinal de entrada para ser transmitida da melhor maneira possível no canal. Ao longo dos tempos, os sistemas de comunicação têm enfrentado diversas situações que tornaram difícil a obtenção de uma transmissão de qualidade, tais como o ruído e a interferência de canal. Com a crescente necessidade da sociedade de obter mais informações em um menor tempo possível, os sistemas de comunicação analógicos têm sido substituídos por sistemas de comunicação digitais, como ilustrado no diagrama de bloco da Figura 2 (SHANMUGAM, 1979).

Figura 2 - Modelo sistemas de comunicação digital.



Fonte: Shammugam (1979)

O codificador de fonte gera uma sequência de símbolos (letras ou números) discretos que representa o sinal de entrada associado a uma sequência única de bit, tornando a transmissão mais eficiente. Cada sequência de símbolos emitida pela fonte é uma mensagem e cada mensagem contém algum tipo de informação - algumas mais que outras. Para definir a quantidade de informação de uma mensagem define-se a taxa de informação por tempo. Porém, é necessário definir duas medidas: a medida para a informação que cada mensagem contém e a medida para cada símbolo que compõe as mensagens; assim, é possível obter a taxa de informação da fonte. Cada símbolo é representado por uma sequência de bits, cuja quantidade define o comprimento de cada símbolo. O comprimento do símbolo num codificador de fonte pode ser variável ou fixo, sendo que cada uma dessas opções possui vantagens e desvantagens, de acordo com a dependência ou independência da sequência de símbolos na transmissão da fonte. Quando a palavra-código possui comprimento fixo, a decodificação da sequência de bits passa a ser mais simples no receptor. A codificação do canal possibilita que dados digitais sejam protegidos de possíveis erros e, para tal, é necessário introduzir redundâncias nos dados transmitidos. Os códigos de canal usados para detectar erros são chamados de códigos de detecção de erro, enquanto os códigos que podem detectar e corrigir erros são chamados de códigos de correção de erros. Shannon (SHANNON, 1948) demonstrou que, por meio de uma codificação apropriada,

os erros introduzidos pelo canal com ruído podem ser reduzidos a qualquer nível desejado sem sacrificar a taxa de transferência de informação. A capacidade do canal de Shannon se aplica ao canal AWGN (Additive White Gaussian Noise, Ruido Aditivo Gaussiano Branco) e é dado por (RAPPAPORT, 2009):

$$C = B\log_2\left(1+\frac{P}{N_0 B}\right) = B\log_2\left(1+\frac{S}{N}\right), \tag{1}$$

onde C é a capacidade do canal (bits/seg), B é a largura de banda de transmissão (Hz), P é a potência do sinal recebido (W) e N_0 é a densidade da potência de ruído para um único lado (W/Hz).

A potência recebida é dada por:

$$P = R_b E_b, \tag{2}$$

onde E_b é a energia de bit média, e R_b é a taxa de transmissão de bit.

A equação pode ser normalizada pela largura de banda de transmissão da seguinte maneira:

$$\frac{C}{B} = \log_2\left(1+\frac{E_b}{N_0}\frac{R_b}{B}\right), \tag{3}$$

onde C/B indica a eficiência da largura de banda.

A finalidade básica das técnicas de detecção e correção de erro é introduzir redundância nos dados para melhorar o desempenho do enlace sem fio. A introdução de bits redundantes aumenta a taxa de dados bruta usada no enlace e, consequentemente, aumenta o requerimento de largura de banda para uma mesma taxa de dados. Isso reduz a eficiência de largura de banda do enlace em condições de alta SNR (Signal Noise Relation, Relação Sinal Ruido), mas oferece excelente desempenho BER (Bit Error Rate, Taxa de Erro de Bit) em baixos valores de SNR.

Estes conceitos são amplamente conhecidos na literatura das comunicações e um estudo mais detalhado sobre medidas de informação (entropia), razão de velocidade, capacidade de canal, probabilidades de erro, entre outros conceitos que descrevem um sistema de comunicação digital, pode ser encontrado em (SHANMUGAM, 1979; RAPPAPORT 2009).

O enfoque desse estudo é a comunicação sem fio, que tem como meio de comunicação o espaço livre, mas com diferentes possibilidades de modelo de canal. Nesse sentido, foca-se em um modelo de canal gaussiano com codificação de canal baseada na estratégia compute-and-forward, que será abordada de forma detalhada ao longo do desenvolvimento do trabalho.

As redes sem fio formam a maior parte dos sistemas de comunicações encontradas nos

dias atuais e o número de usuários cresce muito a cada dia. Assim, é fundamental melhorar o desempenho desses sistemas, o que passa, necessariamente, por um diagnóstico dos problemas inerentes a um sistema de comunicação sem fio.

Um dos problemas que podem ser citados é a limitação das taxas de transmissão das mensagens, já que existe uma escassez de espectro. Tal escassez exige o uso de canais muito próximos, aumentando interferências que prejudicam o desempenho dos sistemas de comunicação. Este é o principal problema a ser enfrentado no futuro das comunicações sem fio.

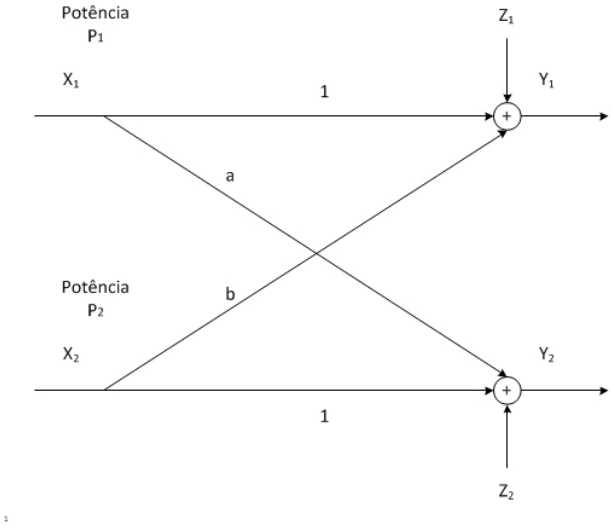
Existem outros problemas que dependem do ambiente em questão, tais como, reflexão, distorção e refração das ondas transmitidas, que são fenômenos do ambiente externo que modificam os níveis de potência do sinal da portadora da mensagem - mais detalhes em (RAPPAPORT, 2009).

Nesse trabalho, os estudos foram direcionados para os problemas relacionados à codificação de canal, com destaque para as temáticas que envolvem a capacidade do canal mediante as taxas de transmissão.

Em Costa (COSTA, 1985) a interferência foi definida por meio do esquema ilustrado na Figura 3 para duas entradas e duas saídas, mas pode ser estendido para mais nós. Nesse esquema, as entradas são dadas por X_1 e X_2, as saídas por Y_1 e Y_2, os coeficientes de interferência são dados por a e b e, Z_1 e Z_2 representam um ruído Gaussiano. As equações de saída, considerando que as entradas são independentes umas das outras e o ruído é independente das entradas, são definidas como seguem:

$$\begin{aligned} Y_1 &= X_1 + aX_2 + Z_1 \\ Y_2 &= bX_1 + X_2 + Z_2 \end{aligned} \tag{4}$$

Figura 3 - Interferência de canal Gaussiano.



Fonte: Costa (1985)

As palavras código de entrada $\mathbf{x_1} = (x_{(1)1}, x_{(2)1}, \ldots, x_{(n)1})$ e $\mathbf{x_2} = (x_{(1)2}, x_{(2)2}, \ldots, x_{(n)2})$ de qualquer bloco de complemento n, requer que as desigualdade dadas em (5) sejam satisfeitas, ou seja:

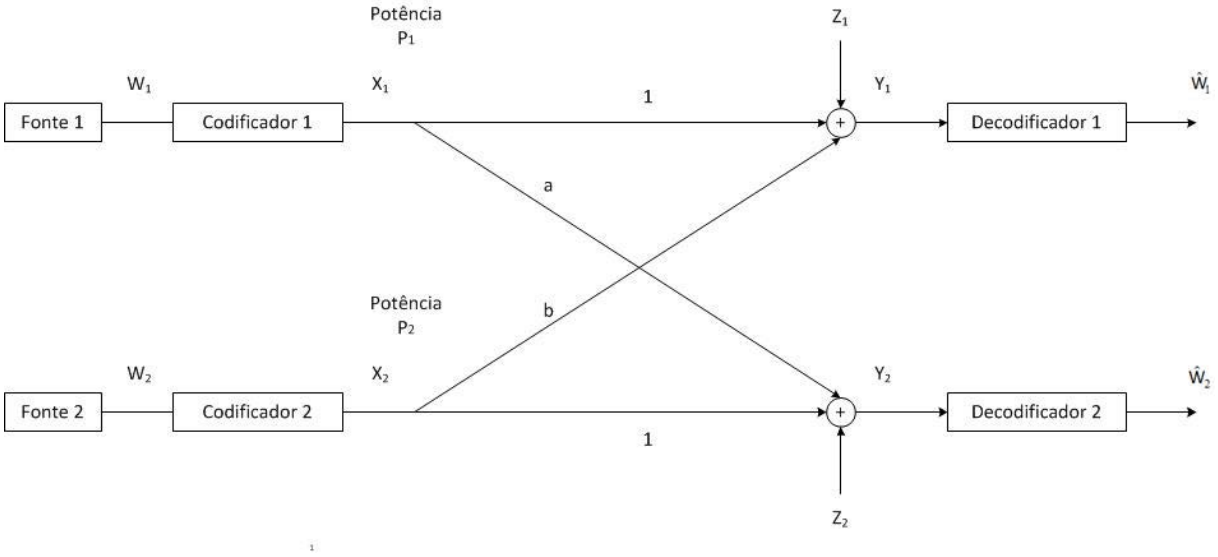
$$\frac{1}{n}\sum_{i=1}^{n} x_{(i)1}^2 \leq P_1$$

$$\frac{1}{n}\sum_{i=1}^{n} x_{(i)2}^2 \leq P_2. \tag{5}$$

Em (5), P_1 e P_2 denotam as potência de entradas.

Com o intuito de obter um esquema mais completo, Costa fez algumas modificações na Figura 3 e introduziu no esquema, que ilustra a interferência de canal, as fontes, codificadores e decodificadores, como apresentado na Figura 4. O codificador irá realizar o mapeamento entre a saída da fonte $\mathbf{W_l}$ e $\mathbf{X_l} = \left(X_{(1)l}, X_{(2)l}, \ldots, X_{(n)l}\right)$ para $l = 1,2$; o decodificador mapeará também a saídas $\mathbf{Y_l} = \left(Y_{(1)l}, Y_{(2)l}, \ldots, Y_{(n)l}\right)$ para $\hat{\mathbf{W}}_\mathbf{l}$. Neste caso, os codificadores são trabalhados dentro dos inteiros $\mathbf{W_l} \in \mathbf{M_l} = \{1,2,\ldots,M_l\}$.

Figura 4 - Interferência de canal Gaussiano, Modelo Completo.



Fonte: Costa (1985)

Como consequencia do Teorema da Capacidade do Canal Gaussiano de Shannon (SHANNON, 1948), a região de capacidade do canal com interferência foi definida por Costa (COSTA, 1985). Nesse sentido, Costa (COSTA, 1985) define a velocidade e consequentemente a capacidade para diferentes valores de interferência, que é um modelo básico para o entendimento das regiões de capacidades. Outros trabalhos, como (CARLEIAL, 1975; HAN; KOBAYASHI, 1981; SATO 1981) definem a região de capacidade, considerando interferências fortes, moderadas ou leves.

Os sistemas de comunicações sem fio do tipo MIMO (Multiple Inputs Multiple Outputs, Múltiplas Entradas e Múltiplas Saídas) serão o estudo de caso neste trabalho. Tais sistemas permitem diminuir os efeitos de desvanecimento, pois maximizam o espectro através de técnicas de diversidade, transmitindo a informação por diferentes e independentes canais.

Considere um sistema MIMO onde cada transmissor está equipado com um codificador de canal representado por um diagrama de blocos ε_l. Sequências de comprimento k, dadas em $\mathbb{F}_p^k$ (palavras-código) e tomadas a partir de um alfabeto sobre um corpo finito, são mapeadas no corpo dos complexos $\mathbb{C}^n$, isto é, $\varepsilon_l : \mathbb{F}_p^k \to \mathbb{C}^n$ gera códigos em $\mathbb{C}^n$, formando reticulados $\mathbf{x}_l = \varepsilon_l(w_l)$ sendo $\mathbf{w}_l$ palavra código formada a partir de um código $\mathscr{C} \subset \mathbb{F}_p^k$.

O canal é dado pela matriz $\mathbf{H} \in \mathbb{C}^{(M \times L)}$ e sua resposta ao sinal transmitido é dada por:

$$\mathbf{y}_m = \sum_{l=1}^{L} h_{ml}\mathbf{x}_l + \mathbf{z}_m, \tag{6}$$

onde $h_{ml} \in \mathbb{C}$ são os coeficientes do canal e $\mathbf{z}_m$ é o ruído Gaussiano.

Do mesmo modo como Costa determina a potência da mensagem em (COSTA, 1985), Gasper e Nazer (NAZER; GASTPAR, 2011a) também definem a potência limitada para transmitir a mensagem como sendo a soma das componentes das palavra-código elevadas ao quadrado, dividindo-se pelo número do comprimento na qual são codificadas. Assim, define-se como:

$$\frac{1}{n}\sum_{l=1}^{L}\mathbf{x}_l^2 \leq P. \tag{7}$$

Assim também é definida a velocidade da mensagem R_l de cada transmissão como a largura da mensagem normalizada pelo número do canal usado, ou seja:

$$R_l = \frac{k_l}{n}\log p. \tag{8}$$

Uma estratégia utilizada para fazer uso deste modelo em um sistema MIMO é o Compute-and-Forward (NAZER; GASTPAR, 2011a) que, de fato, pode ser usada em qualquer rede chaveada (relay) com canais lineares e ruído aditivo branco Gaussiano (AWGN). Nesses casos, a rede chaveada pode decodificar as equações lineares da mensagem transmitida fazendo uso de combinações lineares do ruído gerado pelo canal, aumentando significativamente a probabilidade de a mensagem original chegar ao destino. A estratégia é baseada em códigos que apresentam uma estrutura linear - especificamente os códigos reticulados, que serão apresentados de forma mais detalhada no próximo capítulo deste trabalho.

As interferências em redes sem fio sempre foram consideradas obstáculos para o aumento na capacidade de transmissão e diversos métodos têm sido propostos para controlar ou reduzir seus efeitos. Porém, a partir da estratégia de Compute-and-Forward (NAZER; GASTPAR, 2011a), os autores utilizam a interferência de forma benéfica para o usuário.

Nazer e Gastpar (NAZER; GASTPAR, 2011a) mencionam as estratégias utilizadas anteriormente à técnica Compute-and-Forward e informações mais detalhadas sobre outras técnicas podem ser encontradas em (KRAMER; GASTPAR; P., 2005; CARLEIAL, 1975; LANEMANI; C.; W.; 2004; BORADE; ZHENG; GALLAGER, 2007).

- Decode-and Forward: nesta estratégia a decodificação é feita por partes, com parte da mensagem sendo decodificada inicialmente e enviada a um próximo bloco relay, que recupera os bits finais; a principal vantagem desta estratégia é a limitação da interferência feita pelo relay, que cresce com o número de mensagens transmitidas.

- Compress-and-Forward: a estratégia é caracterizada por não usar codificação na área in-

termediaria entre os nós (usuários). Neste caso, o sinal é inicialmente quantizado e depois enviado ao destino. Como não tem codificação, o sinal está mais sujeito às interferências durante a transmissão.

- Amplify-and-Forward: o relay faz a repetição e a transmissão de uma versão escalonada da mensagem recebida, com SNR suficientemente alta. Esta estratégia é desenvolvida com êxito, principalmente porque é uma estratégia que não codifica a modulação das mensagens e trabalha sobre o corpo dos complexos, fazendo o ganho das combinações lineares iguais ao do desempenho do canal.

A estratégia de Compute-and-Forward é baseada em códigos reticulados aninhados, os quais possuem estrutura linear. Como consequência, a estratégia Compute-and-Forward torna-se um modelo matemático ideal para o estudo de problemas de interferência em codificação de rede (NAZER; GASTPAR, 2011b). A estrutura linear dos códigos reticulados garante que a combinação de palavras-códigos de um código reticulados também seja uma palavra-código.

Como consequência, os blocos de chaveamente (relay) decodificam as combinações lineares das palavras código formadas, o que corresponde a decodificar combinações lineares sobre corpos finitos.

Eres e Zamir (EREZ; LITSYN; ZAMIR, 2005) mostram teoricamente que, por meio de códigos de reticulados aninhados, codificadores e decodificadores podem ser projetados para operarem próximos à capacidade máxima de transmissão. Neste sentido, Trinca (TRINCA, 2013) desenvolveu uma nova metodologia para aproximar os coeficientes do canal por meio de cadeias de códigos reticulados aninhados sobre $\mathbb{Z}[i]$ utilizando a estratégia Compute-and-Forward (NAZER; GASTPAR, 2011a). Este esquema de código requer apenas que cada relé conheça o coeficiente do canal de cada transmissor. Especificamente, cada relé m só precisa conhecer os coeficientes h_m e cada transmissor só precisa conhecer a velocidade da mensagem.

Em (TRINCA, 2013), verifica-se que que este método é obtido como consequência da construção de reticulados algébricos infinitos provenientes de corpos ciclotômicos $\mathbb{Q}(\zeta_{2^s})$ de grau $N = 2^{s-2}$ sobre definidos em $\mathbb{Q}(i)$. Os autores também demonstram que os reticulados aninhados infinitos correspondem à Construção A (associada a códigos cíclicos), com isomorfos, e a reticulados da forma cúbica do tipo $\mathbb{Z}[i]^N$. Porém, eles não são suficientemente densos, de modo que sua distância quadrática mínima é igual a 2.

Forney (1988a) demonstrou que existem reticulados mais densos, na forma $\mathbb{Z}[i]^N$, e utilizou reticulados da forma cúbica do tipo $\mathbb{Z}[\omega]^N$ onde $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Mostrou ainda que esses reticulados também correspondem a códigos. Dentre as correspondências entre reticulados e

códigos (Construção A), têm-se os códigos de Galois e o famoso reticulado de Leench.

Tunali (TUNALI et al., 2012) provaram a existência de bons códigos reticulados aninhados definidos sobre $\mathbb{Z}[\omega]$, para problemas de codificação de canais AWGN por meio da estratégia de Computer-and-Forward. Também demonstram que a velocidade de informação obtida com códigos reticulados aninhados sobre $\mathbb{Z}[\omega]$ é maior do que a obtida com os códigos reticulados aninhados sobre $\mathbb{Z}[i]$ proposta por Nazer e Gastpar (NAZER; GASTPAR, 2011a).

Neste trabalho é proposto uma metodologia alternativa para quantizar os coeficientes do canal por meio de códigos de reticulados aninhados sobre $\mathbb{Z}[\omega]$, baseados na estratégia compute-and-forward (NAZER; GASTPAR, 2011a; TUNALI et al., 2012). Isso resulta em uma nova classe de códigos reticulados aninhados que é resultado da construção de reticulados algébricos infinitos sobre $\mathbb{Z}[\omega]$, provenientes de corpos ciclotômicos $\mathbb{Q}(\zeta_{9.2^s})$ de grau $N = 3.2^{s-1}$ sobre $\mathbb{Q}(\omega)$, onde $\zeta_{9.2^s}$ denota a raiz 9.2^s da unidade. Estes reticulados são isomorfos a reticulados da forma cúbica $\mathbb{Z}[\omega]^N$, proposto por (FORNEY, 1988a).

2 REVISÃO DE ÁLGEBRA ABSTRATA

O objetivo deste capítulo é fornecer subsídios de álgebra abstrata, fundamentais para o desenvolvimento do trabalho na temática em questão. Neste sentido, serão apresentados de maneira clara e objetiva exemplos voltados a problemas de codificação que ajudam no entendimento desde tópico.

As principais referências neste capítulo são (OGGIER; BELFIORE; VITERBO, 2007; PALAZZO, 2003; GIRAUD; BOUTILON; BELFIORE, 1997).

2.1 GRUPO

Para uma melhor compreensão do conceito de grupo considere inicialmente um conjunto S não vazio dotado por operação definida em S.

Definição 2.1. *Uma operação binária $*$ sobre um conjunto S é uma regra que associa algum elemento de S a cada par ordenado $(a,\ b)$ de elementos de S.*

A notação $*$ denota uma operação binária definida em S. Porém, em problemas relacionados à teoria dos códigos, que é o do interesse neste trabalho, via de regra se utiliza a operação adição ou multiplicação.

Definição 2.2. *Uma operação binária sobre um conjunto S é dita comutativa se:*

$$a*b = b*a,\ \forall\ a,b \in S. \tag{9}$$

Definição 2.3. *Uma operação binária sobre um conjunto S é associativa se:*

$$(a*b)*c = a*(b*c),\ \forall\ a,\ b,\ c \in S. \tag{10}$$

Definição 2.4. *Dado um conjunto G não vazio dotado de uma operação binária $*$, diz-se que G é um grupo se as seguintes propriedades são satisfeitas:*

(i.) A operação binária $*$ é associativa.

(ii.) Existe um elemento e com relação à operação $*$ em G, chamado elemento neutro ou identidade tal que:

$$e * g = g * e = g, \forall\, g \in G. \tag{11}$$

(iii.) Para cada elemento $g \in G$, existe um elemento inverso $g^{'} \in G$ que satisfaz a propriedade:

$$g^{'} * g = g * g^{'} = e \tag{12}$$

Teorema 2.1. *Em todo grupo G, o elemento identidade é único. O inverso de cada elemento em G é único também.*

Exemplo 2.1.

(i.) O conjunto dos reais $\mathbb{R}$, dos racionais $\mathbb{Q}$, dos inteiros $\mathbb{Z}$ sob a operação de adição são grupos aditivos. Denota-se por $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$ e $(\mathbb{Z}, +)$, respetivamente.

(ii.) O conjunto $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ e $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$ sob a operação multiplicativa são grupos. Denota-se por $(\mathbb{R}, \cdot)$ e $(\mathbb{Q}, \cdot)$, respectivamente. Os grupos obtidos segundo a operação multiplicativa são ditos grupos multiplicativos.

Seguindo a mesma linha de raciocínio do Teorema 2.1, poderíamos especular se o conjunto dos inteiros não nulos $\mathbb{Z}^*$ também não seria um grupo multiplicativo. Observe que para qualquer $a \in \mathbb{Z}$, não nulo diferente de 1 e -1, não existe $b \in \mathbb{Z}$ tal que $a \cdot b = 1$. Portanto, a operação multiplicativa não é fechada em $\mathbb{Z}^*$.

Definição 2.5. *Um grupo G sob a operação $*$ é **abeliano**, se a sua operação $*$ for comutativa.*

Exemplo 2.2.

(i.) Pode-se citar $\mathbb{R}$ e $\mathbb{Z}$ sob a operação aditiva.

(ii.) O conjunto $\mathbb{Z}_n$ sob a adição modulo n, a ser introduzido posteriormente, é uma classe de grupos bastante usada em problemas de codificação. Esta operação é definida como o inteiro r é a soma dos inteiros s e t modulo n se r for o resto da divisão de $s+t$ por n. Tem-se, assim que:

$$\mathbb{Z}_n = \{0,\, 1,\, 2,\, \ldots,\, n-1\},\ \forall\, n \geq 2.$$

Seja G um grupo sob a operação binária $*$ definida em G e seja H um subconjunto de G. Dizemos que H é um subgrupo de G sob a operação binária caso H seja um grupo, denotando isto como $H \leq G$.

Seja G um grupo de cardinalidade finita. Neste caso, chama-se de ordem de G ao número de elementos de G e denota-se por $|G|$.

Exemplo 2.3.

(i.) Note que $\mathbb{Z}$ é um subconjunto de $\mathbb{Q}$. No Exemplo 2.1, vimos que $\mathbb{Q}$ é grupo aditivo. Caso faça uso dos items (i), (ii) e (iii) da Definição 2.4, sem muita dificuldade, mostra-se que $\mathbb{Z}$ sob a operação aditiva é um grupo. Logo, conclui-se que $\mathbb{Z}$ é um subgrupo de $\mathbb{Q}$ sob a operação aditiva.

(ii.) Note que $\mathbb{Z}^* = \mathbb{Z}\backslash\{0\}$ é um subconjunto de $\mathbb{Z}$. No item (ii) do Exemplo 2.1 vimos que $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$ é um grupo multiplicativo. Porém, como visto no item (iii) da Definição 2.4, temos que $\mathbb{Z}^*$ não é grupo multiplicativo. Logo em particular sob a operação multiplicativa , $\mathbb{Z}^*$ não é um subgrupo multiplicativo de $\mathbb{Q}^*$.

Exemplo 2.4. *Seja $G = \mathbb{Z}$ um grupo aditivo e $H = 2\mathbb{Z}$. É possível mostrar que H é um subgrupo de G. Para todo $x \in \mathbb{Z}$, existe de maneira única pelo algoritmo da divisão euclidiana, $q,\ r \in \mathbb{Z}$, com $|r| < 2$:*

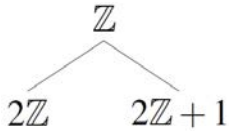
$$x = 2q + r$$

Sendo $r = 0$ ou $r = 1$.
Se $r = 0$, então tem-se que $x = 2q$ para algum $q \in \mathbb{Z}$. Neste caso tem-se que $x \in 2\mathbb{Z}$.
Já se $r = 1$ então tem-s que $x = 2q + 1$ para algum $q \in \mathbb{Z}$. Neste caso tem-se que $x \in 2\mathbb{Z} + 1$.

Chame-se a atenção que, neste caso, os inteiros são particionados em dois conjuntos: os da forma $2\mathbb{Z}$, inteiros que ao serem divididos por 2 têm resto 0 e os da forma $2\mathbb{Z}+1$, inteiros que ao serem divididos por 2 têm resto 1.

A Figura 5 ilustra de forma clara o que foi mencionado, ou seja, o subgrupo $2\mathbb{Z}$ induz a uma partição de $\mathbb{Z}$. Será mostrado adiante que esse fato está associado aos conceitos de grupo quocientes e das classes laterais definidas nos grupos quocientes em questão.

Figura 5 - Subgrupo.



Fonte: o próprio autor

Seja G um grupo, caso exista ao menos um elemento $a \in G$, satisfazendo (13). Diz-se que

G é um grupo cíclico, isto é, um grupo gerado pelo elemento a e denotado por $G =< a >$.

$$G = \{a^n \mid n \in Z\} \tag{13}$$

Exemplo 2.5. *Os inteiros $\mathbb{Z}$ sob adição ordinária formam um grupo cíclico gerado por* 1*, em outras palavras qualquer elemento de $\mathbb{Z}$, pode ser obtido somando o elemento* 1 *n vezes.*

Diz que um grupo G é finito, caso sua ordem seja finita.

Seja G um grupo finito e H um subgrupo de G denotado por $H = \{h_1 = 1\ , h_2\ , \ldots, h_n\}$ um subgrupo de G. A partir de H, pode-se construir uma tabela como descrita a seguir:

Tabela 1 - Classe Laterais à esquerda

$h_1 = 1$	h_2	h_3	$\ldots$	h_n
g_1	g_1h_2	g_1h_3	$\ldots$	g_1h_n
g_2	g_2h_2	g_2h_3	$\ldots$	g_2h_n
g_3	g_3h_2	g_3h_3	$\ldots$	g_3h_n
		$\vdots$		
g_j	g_jh_2	g_jh_3	$\ldots$	g_jh_n

Fonte: Palazzo (2003)

onde os elementos de G estarão dispostos nas linhas e colunas da Tabela 1 da seguinte forma: a primeira linha da tabela é constituída por elementos do subgrupo H. A segunda linha da tabela é obtida da seguinte maneira; considera um elemento $g \in G$ que não aparece na primeira linha obtida na tabela a partir de H, a próxima etapa é considerar a operação binária definida em G, toma-se a operação de g_1 com cada elemento $h_1,\ h_2, \ldots, h_n$ obtendo-se, assim os elementos $g_1,\ g_1h_2, \ldots,\ g_1h_n$, onde cada elemento g_1h_i está disposto na coluna i.

Para a j-ésima linha, novamente, considere um elemento g_{j-1} em G que satisfaça à condição de que não tenha aparecido na disposição das $j-1$ colunas anteriores da tabela.

Novamente, a próxima etapa é considerar a operação de g_{j-1} com cada elemento $h_1,\ h_2, \ldots, h_n$ da primeira linha, obtém-se desta forma os elementos $g_{j-1},\ g_{j-1}h_2,\ g_{j-1}h_n$.

Como o número de elementos do grupo G é finito, o processo é garantido

Porém, pela forma com que a tabela foi construída, nenhum elemento foi repetido, pois foi utilizado o conceito de inverso segundo a operação $*$ definida em G que por meio desta tabela, verifica-se que na linha $j-1$, se $g_jh_i = g_jh_t$ e se na coluna j se $g_ih_j = g_th_j$, $\forall\ j \in \{1, \ldots, n\}$ e $t \in \{1, \ldots, n\}$.

H particiona G, ou seja, G é uma união das linhas e das colunas da tabela construída via

este procedimento.

O procedimento que utilizamos no processo de construção da Tabela 1 nos conduz ao conceito de classes laterais e grupo quocientes.

Definição 2.6. *Classe lateral: a Tabela 1 é a decomposição de G em classes laterais (com respeito a H). Cada linha é chamada de classe lateral à esquerda e o primeiro elemento de cada linha é chamado de líder de classe lateral.*

2.1.1 Grupo quociente

O objetivo desta seção é introduzir os grupos quocientes. Porém, para que isto seja possível, precisa-se, inicialmente, introduzir conceito de subgrupo normal.

Definição 2.7. *Subgrupo Normal: Seja H um subgrupo de um grupo G. Diz-se que H é normal em G, ou que H é um grupo normal de G se quaisquer umas das seguintes condições foram satisfeitas:*

- $gH = Hg$, $\forall\, g \in G$.
- $gHg^{-1} = H$, $\forall\, g \in G$.
- $gHg^{-1} \subset H$, $\forall\, g \in G$.
- $ghg^{-1} \in H$, $\forall\, g \in G$ *e* $h \in H$.

Como consequência, tem-se que, dado um grupo G e um subgrupo H de G, as classes laterais à esquerda e à direita coincidem e formam um grupo denotado pelo G/H cuja operação é bem definida, se e somente se, H for um subgrupo normal de G. Obviamente, se G for um grupo abeliano as condições da Definição 2.7 são trivialmente satisfeitas. Estes são os casos de interesse deste trabalho.

Exemplo 2.6. *Considere o conjunto dos números inteiros $\mathbb{Z}$ sob a operação da adição usual. Sem muita dificuldade, mostre-se que o conjunto $4\mathbb{Z}$ forma um subgrupo em $\mathbb{Z}$. Como $4\mathbb{Z}$ é um sub-grupo normal em $\mathbb{Z}$, faz sentido considerar o grupo quociente $\mathbb{Z}/4\mathbb{Z}$. Logo os elementos de $\mathbb{Z}/4\mathbb{Z}$ são dados pelas classes laterais $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, onde:*

$$\bar{0} = 0 + 4\mathbb{Z} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$$
$$\bar{1} = 1 + 4\mathbb{Z} = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$$
$$\bar{2} = 2 + 4\mathbb{Z} = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$$
$$\bar{3} = 3 + 4\mathbb{Z} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$$

Apenas para esclarecer mais os conceitos utilizados até aqui, sob a operação aditiva módulo 4, verifica-se via Tabela 2 que $\mathbb{Z}/4\mathbb{Z}$ é um grupo aditivo.

Tabela 2 - Exemplo de classes laterais

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Fonte: o próprio autor

2.2 ANÉIS

Seja R um conjunto não vazio dotado de duas operações binárias $+$ e $\cdot$ (chamadas adição e multiplicação). O conjunto R é dito um anel se as propriedades a seguir são verificadas

- $(R, +)$ é um grupo abeliano.
- A multiplicação é associativa.
- Para todos a, b, $c \in R$, valem a lei distributiva à esquerda e a lei distributiva à direita, como descritos em (14) e (15):

$$a(b+c) = (ab) + (ac), \tag{14}$$

$$(a+b)c = (ac) + (bc). \tag{15}$$

Na literatura também aparece a notação $(\mathbb{R}, +, \cdot)$ para representar o anel dotado das operações binárias $+$ e $\cdot$.

Exemplo 2.7.

i. $(\mathbb{Q}, +, \cdot)$*, onde* $\mathbb{Q}$ *denota o conjunto dos reacionais.*

ii. $(\mathbb{R}, +, \cdot)$*, onde* $\mathbb{R}$ *denota o conjunto dos reais.*

iii. $(\mathbb{C}, +, \cdot)$*, onde* $\mathbb{C}$ *denota o conjunto dos complexos.*

iv. $(\mathbb{Z}, +, \cdot)$*, onde* $\mathbb{Z}$ *denota o conjunto dos inteiros.*

Diz-se que N é um subanel de um anel R se $N \subseteq R$. Obviamente, neste caso, tem-se que N também forma um anel com as operações adição e multiplicação herdadas de R.

Um anel no qual a multiplicação é comutativa é chamado de anel comutativo.

Seja R um anel dotado de uma unidade multiplicativa 1 satisfazendo a (16). Uma identidade multiplicativa em um anel é uma unidade.

$$1 \cdot x = x \cdot 1 = x, \ \forall \, x \in R. \tag{16}$$

Os subanéis I de interesse são os que possuem uma estrutura de **ideal** em um anel comutativo R, isto é, para quaisquer $a \in R$ e $x \in I$ verifica-se que $ax \in I$.

Um ideal $\mathscr{P}$ em um anel comutativo R é chamado de ideal **primo**, se $\mathscr{P} \neq R$, e se para quaisquer $a, b \in R$ for verificada a condição de que $ab \in \mathscr{P}$ implicar em $a \in \mathscr{P}$ ou $b \in \mathscr{P}$.

2.3 CORPOS

Corpo é um anel especial comutativo com unidade tal que todo elemento não nulo é inversível. Seriam feitas as seguintes observações

Observação 2.1.

i. Os inteiros $\mathbb{Z}$ não formam um corpo. Embora, satisfaça a condição de ser um anel, não tem elemento inversível.

ii. Embora $\mathbb{Z}$ não seja um corpo, mas se consideramos subgrupos em $\mathbb{Z}$ da forma $p\mathbb{Z}$, temos que o grupo quociente obtido $\mathbb{Z}_p$ é isomorfo a $\mathbb{Z}_p \cong \frac{\mathbb{Z}}{p\mathbb{Z}}$.

Será introduzida agora uma classe especial de corpos, denominados de corpos de números, que é fundamental em problemas de quantização de canal. Trata-se de uma classe de corpos que contém o corpo $\mathbb{Q}$.

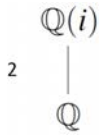
Definição 2.8. *Sejam dados os corpos K e L, tais que $K \subseteq L$, então, diz-se que L é uma extensão do corpo K, sendo denotado por L/K.*

Neste trabalho os corpos de interesse serão $\mathbb{Q}$, $\mathbb{Q}(i)$ e $\mathbb{Q}(\omega)$.

Exemplo 2.8. *O corpo $\mathbb{Q}(i)$ é uma extensão do corpo $\mathbb{Q}$, onde $i = \sqrt{-1}$ e $\mathbb{Q}(i)$ é descrito na forma:*

$$\mathbb{Q}(i) = \{w = x + yi \mid x, y \in \mathbb{Q}\}.$$

Figura 6 - Extensão de corpo $\mathbb{Q}(i)$ sobre $\mathbb{Q}$

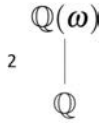


Fonte: o próprio autor

Exemplo 2.9. *O corpo $\mathbb{Q}(\omega)$ é uma extensão do corpo $\mathbb{Q}$, onde $\omega = -1/2 + (i\sqrt{3}/2)$ e $\mathbb{Q}(\omega)$ é descrito na forma:*

$$\mathbb{Q}(\omega) = \{w = x + y\omega \mid x, y \in \mathbb{Q}\}.$$

Figura 7 - Extensão de corpo $\mathbb{Q}(\omega)$ sobre $\mathbb{Q}$



Fonte: o próprio autor

Seja L/K um corpo estendido. Chama-se grau de L sobre K, como sendo a dimensão de espaço vetorial L sobre K, denotado por $[L : K]$. Se o grau $[L : K]$ é finito, diz-se que L é uma extensão finita de K.

Definição 2.9. *Um corpo de extensão finita sobre $\mathbb{Q}$ é chamado de corpo de números.*

Considere-se os corpos $\mathbb{Q}(i)$ e $\mathbb{Q}(\omega)$. Verifica-se facilmente que $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ e $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$. Logo $\mathbb{Q}(i)$ e $\mathbb{Q}(\omega)$ são exemplos de corpos de números.

Definição 2.10. *Seja L/K uma extensão de corpos sobre K e $\alpha \in L$. Se existe um polinômio mônico não nulo $p(x) \in K[x]$ tal que $p(\alpha) = 0$, diz-se que α é um número algébrico sobre K. Já, o polinômio $p(x)$ é chamado o polinômio minimal de α sobre K.*

Temos que:

i. Note que $i = \sqrt{-1}$ é raiz do polinômio $p(x) = x^2 + 1 \in \mathbb{Q}[x]$. Logo, i é um número algébrico sobre $\mathbb{Q}$ e $p(x) = x^2 + 1$ é o polinômio minimal de i sobre $\mathbb{Q}$.

ii. Note que $\omega = -1/2 + (i\sqrt{3}/2)$ é raiz do polinômio $p(x) = x^2 + x + 1 \in \mathbb{Q}[x]$. Logo , ω é um número algébrico sobre $\mathbb{Q}$ e $p(x) = x^2 + x + 1$ é o polinômio minimal de ω sobre $\mathbb{Q}$.

Definição 2.11. *Se todos os elementos de L são números algébricos sobre $\mathbb{Q}$, então diz-se que L é uma extensão algébrica de $\mathbb{Q}$, ou equivalentemente: um corpo de números algébricos.*

Dado $L = \mathbb{Q}(i)$ ou $\mathbb{Q}(\omega)$. Prova-se, sem muita dificuldade que todo elemento $\alpha \in L$ é um número algébrico sobre $\mathbb{Q}$ e mais, o polinômio minimal associado a este elemento é um polinômio $p(x) \in \mathbb{Q}[x]$ de grau 2.

De um modo geral, temos a situação dada pelo Teorema 2.2.

Teorema 2.2. *Se L é um corpo de números, então $L = \mathbb{Q}(\theta)$ para algum número algébrico $\theta \in L$, chamado elemento primitivo.*

Com base no Teorema 2.2, L é um espaço vetorial sobre $\mathbb{Q}$. O corpo L tem grau n sobre $\mathbb{Q}$, então $\{1, \theta, \theta^2, \ldots, \theta^{(n-1)}\}$ é a base de L sobre $\mathbb{Q}$; L pode ser escrita conforme a (17); e o grau do polinômio mínimo de θ é n. Como consequência, dado elementos $x \in L$, é escrito na forma:

$$x = \sum_{i=0}^{n-1} a_i \theta^i,\ a_i \in \mathbb{Q}. \tag{17}$$

Exemplo 2.10. *Seja L o corpo dado por $L = \mathbb{Q}(\theta)$ onde $\theta = i$. Note-se que $\theta = i$ é raiz do polinômio minimal $p(x) = x^2 + 1$ (grau do polinômio, $n = 2$). Ou seja, o grau de extensão de $\mathbb{Q}(i)$ sobre $\mathbb{Q}$ é igual a 2. A base de $\mathbb{Q}(i)$ sobre $\mathbb{Q}$ é dada por $\{1, i\}$.*

Exemplo 2.11. *Seja $L = \mathbb{Q}(\omega)$, onde $\omega = -1/2 + (i\sqrt{3}/2)$. Note-se que ω é raiz do polinômio minimal $p(x) = x^2 + x + 1$ (grau do polinômio 2). Ou seja, o grau de extensão $\mathbb{Q}(\omega)$ sobre $\mathbb{Q}$ é 2. A base de $\mathbb{Q}(\omega)$ sobre $\mathbb{Q}$ é dada por $\{1, \omega\}$.*

2.3.1 Mergulho e grupo galois

Definição 2.12. *Seja $K/\mathbb{Q}$ e $L/\mathbb{Q}$ dois corpos estendidos de $\mathbb{Q}$. Chama-se $\varphi : K \to L$ um $\mathbb{Q}$-homomorfismo se φ é um homomorfismo de corpos que satisfaz $\varphi(a) = a$ para todo $a \in \mathbb{Q}$.*

Chamamos o $\mathbb{Q}$-homomorfismo $\varphi : K \to \mathbb{C}$ de mergulho de K em $\mathbb{C}$.

Teorema 2.3. *Seja $L = \mathbb{Q}(\zeta)$ um corpo de números de grau n sobre $\mathbb{Q}$. Existem exatamente n mergulhos distintos de L em $\mathbb{C}$ dados por $\sigma_i : L \to \mathbb{C}$, $\sigma_i(\theta) = \zeta_i$, $i = 1, \ldots, n$, onde θ_i são os zeros distintos em $\mathbb{C}$ do polinômio minimal de θ sobre $\mathbb{Q}$.*

Note que $\sigma_1(\theta) = \theta_1 = \theta$, o mergulho σ_1 é a identidade. Quando se aplica um mergulho $\sigma_i \in Gal(L/\mathbb{Q})$ em um elemento arbitrário $x \in L$, $x = \sum_{k=1}^{n} a_k \theta^k$, $a_k \in \mathbb{Q}$, (17), se obtém fazendo uso das propriedades de $\mathbb{Q}$-homomorfismo a expressão:

$$\sigma_i(\alpha) = \sigma_i\left(\sum_{k=1}^{n} a_k \theta^k\right),\ a_k \in \mathbb{Q} = \sum_{k=1}^{n} \sigma_i(a_k)\sigma_i(\theta)^k = \sum_{k=1}^{n} a_k \theta_i^k. \tag{18}$$

Definição 2.13. *Seja $x \in L$. Os elementos $\sigma_1(x),\ \sigma_2(x), \ldots, \sigma_n(x)$ são chamados de isomorfismos e a norma do elemento x é definida por:*

$$N_{L/\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x). \tag{19}$$

Outros resultados importantes associados à extensão de corpos de L sobre $\mathbb{Q}$ relacionados à sua norma são dados a seguir:

$$N_{L/F}(xy) = N_{L/F}(x)N_{L/F}(y). \tag{20}$$

Desde que $L/K/F$ é uma extensão finita de corpos, então

$$N_{L/F}(\theta) = N_{K/F}(N_{L/K}(\theta)). \tag{21}$$

Definição 2.14. *Uma extensão de corpos de números L é extensão Galois se cada polinômio irredutível sobre na qual tem todos os zeros em L.*

Exemplo 2.12. *Tomando o Exemplo 2.10, as duas raízes do polinômio x^2+1 pertencem a $\mathbb{Q}(i)$. Então $\mathbb{Q}(i)/\mathbb{Q}$ é a um extensão Galois.*

2.4 CORPOS CICLOTÔMICOS

O objetivo desta seção é introduzir uma classe especial de corpos de números algébricos, denominados de corpos ciclotômicos, que possuem um ferramental algébrico importante em problemas de codificação.

Seja L um corpo de números. Diz-se que L é um corpo ciclotômico se L pode ser expresso na forma $\mathbb{Q}(\theta)$, onde

$$\theta = \zeta_n = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right) \tag{22}$$

para algum $n \geq 3$, isto é, ζ_n é uma raíz n-ésima da unidade.

Tem-se que:
Se $L = \mathbb{Q}(\zeta_n)$ para algum $n \geq 3$, então a extensão de corpos $L/\mathbb{Q}$ é cíclica com grau

$$[L : \mathbb{Q}] = \varphi(n), \tag{23}$$

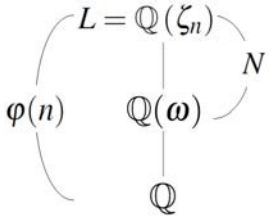
onde φ denota a função de Euler. A função de Euler é definida da seguinte forma $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ se p é primo a vale a propriedade multiplicativa, isto é, $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$.

Para o interesse de este trabalho, temos também que se $L = \mathbb{Q}(\zeta_n)$ para algum $n \geq 3$, então a extensão de corpos $L/\mathbb{Q}(\omega)$ é cíclica com grau :

$$[L : \mathbb{Q}(\omega)] = N. \tag{24}$$

O caso de interesse desde trabalho são as extensões cíclicas de corpos do tipo $L/\mathbb{Q}(\omega)$, onde $L = \mathbb{Q}(\zeta_n)$ para algum $n \geq 3$ e $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

Figura 8 - Extensão Corpos Ciclotômico.



Fonte: o próprio autor

A extensão de corpos é uma extensão de Galois onde o grupo de Galois associado é dado por:

$$Gal(L/\mathbb{Q}) = \{\sigma_j : \sigma_j(\zeta_m) = \zeta_m^j, \text{ onde } MDC(m, j) = 1\}, \tag{25}$$

e é isomorfo ao grupo das unidades em $\mathbb{Z}/m\mathbb{Z}$ e denotado por $U(\mathbb{Z}/m\mathbb{Z})$.

O maior anel em $\mathbb{Q}(\zeta_n)$ é chamado de anel de inteiros e é denotado por $\mathcal{O}_L = \mathbb{Z}[\zeta_n]$.

Os elementos de $\mathbb{Z}[\zeta_n]$ são escritos como combinação linear sobre $\mathbb{Z}$ da base B (ver Teorema 2.2) dada por

$$B = \{1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}\}, \tag{26}$$

a base B também é chamada de base integral.

3 RETICULADOS ALGÉBRICOS

Neste capítulo serão estudados os conceitos básicos de reticulados, considerando a teoria apresentada nas seções anteriores para melhor entendimento. Consideraram-se como referências (NAZER; GASTPAR, 2011a; OGGIER, VITERBO, 2004).

3.1 DEFINIÇÕES FUNDAMENTAIS

Definição 3.1. *Seja $v_1, \ldots, v_m$ um conjunto de vetores linearmente independentes em $\mathbb{R}^n$ (tal que $m \leq n$). O conjunto de pontos dado pela (27) é chamado um reticulado de posto m, e $\{v_1, \ldots, v_m\}$ é chamado uma base do reticulado.*

$$\Lambda = \left\{ x = \sum_{i=1}^{m} \lambda_i v_i \, , \lambda_i \in \mathbb{Z} \right\}. \tag{27}$$

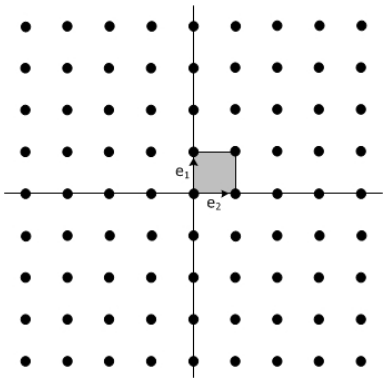
A base de um reticulado não é única, existem diferentes formas de escolher a base de um reticulado.

Definição 3.2. *O paralelepípedo formado pelos pontos satisfazendo (28); é chamado um paralelepípedo fundamental ou região fundamental do reticulado. Pode-se ver no Exemplo 3.1.*

$$\zeta_1 v_1 + \cdots + \zeta_m v_m, \; 0 \leq \zeta_i < 1 \tag{28}$$

Exemplo 3.1. *$\Lambda = \mathbb{Z}^2$ é um reticulado gerado pelos vetores $e_1 = (1,0)$ e $e_2 = (0,1)$ com região fundamental descrita na Figura 9:*

Figura 9 - Reticulado.



Fonte:Alves (2008)

Os vectores e_1 e e_2 são chamados base do reticulado.

Associado a um reticulado existe uma matriz geradora de ordem n, onde as n colunas são formadas por vetores base e as n linhas por coordenadas dos vetores base, o que nos leva à Definição 3.3.

Definição 3.3. *A matriz M (29); é chamada uma matriz geradora para o reticulado. A matriz $G = MM^t$ é chamada uma matriz de Gram para o reticulado, onde M^t denota a matriz transposta de M.*

$$M = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \cdots & v_{nn} \end{pmatrix} \tag{29}$$

Como M contém os vetores da base do reticulado $\{v_i\}_{i=1}^n$, a (i,j)-ésima entrada da matriz G é o produto interno $\langle v_i, v_j \rangle = v_i \cdot v_j^t$.

Os pontos do reticulado são formados por:

$$\Lambda = \{x = \lambda M \mid \lambda \in \mathbb{Z}^n\}. \tag{30}$$

Exemplo 3.2. *Considerando o reticulado do Exemplo 3.1., com os vetores base $e_1 = (1,0)$ e $e_2 = (0,1)$, tem-se como matriz geradora:*

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

O reticulado $\mathbb{Z}^2$ é identificado de forma natural com o anel dos inteiros de Gauss $\mathbb{Z}[i] =$

$\{x+iy \mid x,y \in \mathbb{Z}\}$, onde $i^2 = -1$. Cada elemento $(x,y) \in \mathbb{Z}^2$ corresponde de forma biunívoca a um único elemento $x+iy \in \mathbb{Z}[i]$. Conforme pode ser visto na Figura 9.

Definição 3.4. *O determinante do reticulado Λ é definido como sendo o determinante da matriz G.*

$$det(\Lambda) = det(G). \tag{31}$$

Desde que M seja uma matriz quadrada, obtemos que:

$$det(\Lambda) = (det(M))^2. \tag{32}$$

Definição 3.5. *Para reticulados de posto máximo, a raiz quadrada do determinante do reticulado é o volume do paralelepípedo fundamental, também chamado de volume do reticulado, e denotado por $vol(\Lambda)$.*

3.2 PROPRIEDADES GEOMÉTRICAS DOS RETICULADOS

Um empacotamento esférico é uma distribuição de esferas do mesmo raio em $\mathbb{R}^n$ de tal forma que a intersecção de quaisquer duas esferas tenha no máximo um ponto. Assim, pode-se descrever um empacotamento indicando apenas o conjunto do centro das esferas e o raio.

Um empacotamento reticulado é um empacotamento em que o conjunto dos centros das esferas formam um reticulado Λ em $\mathbb{R}^n$.

Definição 3.6. *O raio de empacotamento é o maior raio para o qual é possível distribuir esferas centradas nos pontos do reticulado Λ e o empacotamento é definido da seguinte forma:*

$$\rho = d_{min}/2, \tag{33}$$

onde d_{min} é:

$$d_{min} = min\{|\lambda| \; ; \; \lambda \in \Lambda, \; \lambda \neq 0\}. \tag{34}$$

Dado um empacotamento no $\mathbb{R}^n$, associado a um reticulado Λ com base $\{v_1, \ldots, v_n\}$ define-se a sua densidade de empacotamento de esferas de raio r como sendo a porção do espaço $\mathbb{R}^n$ coberta pela união das esferas.

Denotando por $\mathscr{B}(\rho)$ a esfera com centro na origem e raio ρ, temos que a densidade de empacotamento de Λ é igual ao volume da parte da região fundamental coberta pelas esferas

pelo volume da região fundamental dada por,

$$\Delta(\lambda) = \frac{Vol(\mathscr{B}(\rho))}{Vol(\Lambda)} = \frac{(Vol(\mathscr{B}(1))\rho^n)}{Vol(\Lambda)}, \tag{35}$$

onde $Vol(\mathscr{B}(1)) = \begin{cases} \frac{\pi^{(n/2)}}{\frac{n}{2}}, & \text{se n é par} \\ \frac{2^n \pi^{(n-1)/2}((n-1)/2)}{n}, & \text{se n é ímpar.} \end{cases}$

Portanto, o problema se reduz ao estudo de outro parâmetro, chamado de densidade de centro, que é dado por

$$\delta(\Lambda) = \frac{\rho^n}{Vol(\Lambda)}. \tag{36}$$

Definição 3.7. *Seja Λ um reticulado, β uma base de Λ e V o espaço vetorial gerado por esta base. Define-se a região de Voronoi de $v \in V(v)$ como sendo a região que contém todos os pontos de V que estão mais próximos de v do que qualquer outro ponto u do reticulado.*

$$V(v) = \{x \in V;\ \|x - v\| \leq \|x - u\|, \forall\, u \in \Lambda\}. \tag{37}$$

3.2.1 Sub-reticulados, reticulados equivalentes e reticulados aninhados

Seja Λ um reticulado em $\mathbb{R}^n$ e M a matriz geradora associada. A partir de Λ, pode-se obter outro reticulado $\Lambda^{'}$ no qual $\Lambda^{'}$ é um subreticulado de Λ. Como dada na Definição 3.8.

Definição 3.8. *Seja B uma matriz $n \times n$ com entradas inteiras. Um sub-reticulado de Λ é dado por:*

$$\Lambda^{'} = \{x = \lambda BM \mid \lambda \in \mathbb{Z}^n\}. \tag{38}$$

Num reticulado Λ de dimensão n em $\mathbb{R}^n$, tem-se naturalmente uma estrutura de anel induzida por $\mathbb{Z}^n$ e portanto, um grupo aditivo abeliano a ele associado (conforme a Definição 3.2 e 3.3). Desde que $\Lambda^{'}$ é um sub-reticulado (também possue uma estrutura de grupo associado); em particular $\Lambda^{'}$ é então um subgrupo de Λ, e faz sentido considerar o grupo quociente $\Lambda/\Lambda^{'}$.

Definição 3.9. *O índice do sub-reticulado $\Lambda^{'}$ é a cardinalidade do grupo quociente $\Lambda/\Lambda^{'}$ e é dado por:*

$$|\Lambda/\Lambda^{'}| = \frac{vol(\Lambda^{'})}{vol(\Lambda)} = \frac{\sqrt{det(\Lambda^{'})}}{\sqrt{det(\Lambda)}} = |det(B)|. \tag{39}$$

É sempre possível encontrar um sub-reticulado de um dado reticulado considerando sua versão escalonada por um fator inteiro definido da seguinte maneira:

Definição 3.10. *Dado um reticulado Λ, um reticulado escalonado $\Lambda^{'}$ pode ser obtido multiplicando os vetores do reticulado por uma constante:*

$$\Lambda^{'} = c \cdot \Lambda, \tag{40}$$

onde $c \in \mathbb{R}$. Assim, $\Lambda^{'}$ é um sub-reticulado de Λ quando $c \in \mathbb{Z}$.

Mais geralmente, tem-se a Definição 3.11.

Definição 3.11. *Se um reticulado pode ser obtido de outro por uma rotação, reflexão ou mudança de escalar, diz-se que estes reticulados são equivalentes.*

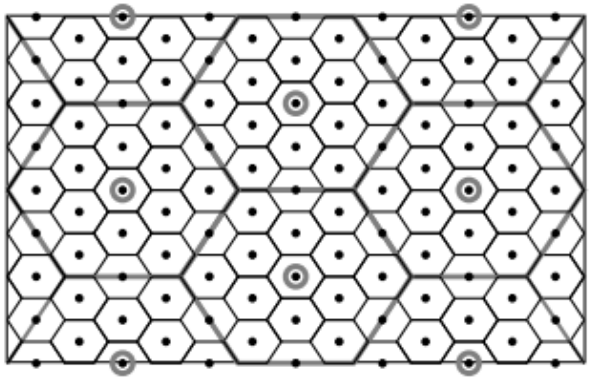
Consequentemente, duas matrizes geradoras M e $M^{'}$ definem reticulados equivalentes se, e somente se, eles são descritos por $M^{'} = cUMB$, onde c é uma constante não nula, U é uma matriz com entradas inteiras e determinante ± 1 e B é uma matriz real ortogonal. As correspondentes matrizes de Gram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

Assim, é importante destacar que o mesmo reticulado pode ser representado por algumas maneiras diferentes. Como consequência, dado uma matriz de Gram (ou geradora), não é fácil determinar qual é o reticulado correspondente. Invariantes, tais como a dimensão e o determinante poderão ajudar, mas um dos cuidados que deve-se ter é que tendo o mesmo determinante não é suficiente para garantir que dois reticulados são equivalentes.

Definição 3.12. *Um reticulado Λ_1 é chamado reticulado aninhado em um reticulado Λ se $\Lambda_1 \subseteq \Lambda$. De uma maneira mais geral uma sequência de reticulados $\Lambda, \Lambda_1, \ldots, \Lambda_L$ é aninhado se $\Lambda_L \subseteq \Lambda_{(L-1)} \subseteq \ldots \subseteq \Lambda_1 \subseteq \Lambda$.*

Dessa forma pode haver similaridade entre os sub-reticulados e os reticulados aninhados, a qual é que tem as mesmas propriedades com a diferença que quando se menciona um reticulado aninhado se faz referência a uma cadeia de reticulados. Uma maneira mais clara de entender os reticulados aninhados é via Figura 10.

Figura 10 - Reticulado aninhado.



Fonte: Nazer e Gastpar (2011a)

Os pontos pretos são os elementos do reticulado Λ e os círculos cinza são os pontos do reticulado aninhado Λ_1. A região de Voronoi para o reticulado está desenhada em preto e para o reticulado alinhado está desenhado em cinza.

3.3 TIPOS DE RETICULADOS

Neste capítulo apresentaremos dois tipos de reticulados:

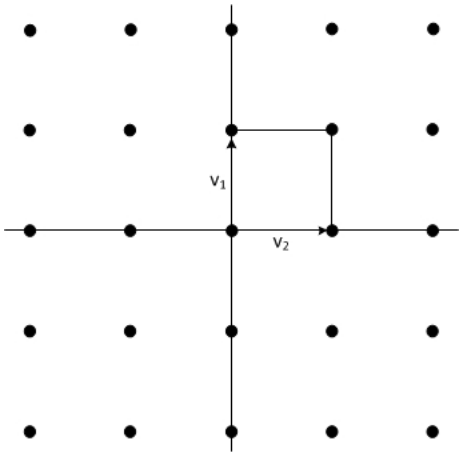
- Reticulados $\mathbb{Z}^n$

  São os reticulados mais simples, de forma general são:

$$\mathbb{Z}^n = \{(x_1, \ldots, x_n),\ x_i \in \mathbb{Z}\}. \tag{41}$$

  Para $n = 2$ tem-se uma associação à modulação QAM e a o anel $\mathbb{Z}[i]$, como apresentado na Figura 11.

Figura 11 - Reticulado $\mathbb{Z}^n$ $n = 2$.



Fonte: Oggier e Viterbo (2004)

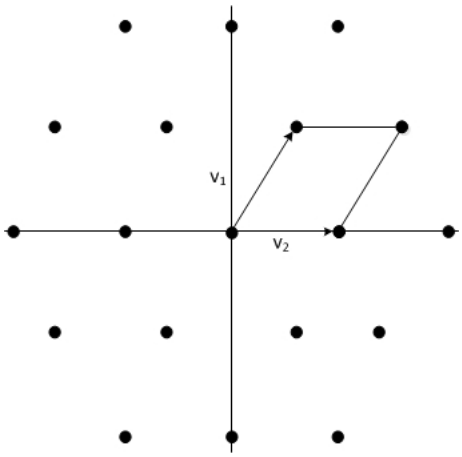
- Reticulados $\mathbb{A}_n$

  Em geral este reticulado pode ser definido como:

$$\mathbb{A}_n = \left\{ (x_0, x_1, \ldots, x_n) \in \mathbb{Z}^{n+1}, \sum_{i=0}^{n} x_i = 0 \right\} \tag{42}$$

  Este reticulado é bem conhecido em dimensão 2, onde $\mathbb{A}_2$ é chamado reticulado hexagonal e está associado à modulação HEX e o anel $\mathbb{Z}[\omega]$, como ilustrado na Figura 12.

Figura 12 - Reticulado A n=2



Fonte: Oggier e Viterbo (2004)

3.4 RETICULADOS COMPLEXOS

Define-se Λ como um reticulado complexo de grau N se Λ é um conjunto discreto de pontos dados por N-tuplas em um N espaço complexo $\mathbb{C}^N$ de dimensão N.

Os reticulados complexos de dimensão N tem uma estrutura aditiva de grupo. Todos os conceitos exposto neste capítulo sobre os reticulados sobre $\mathbb{Z}$ são válidos para os reticulados complexos sobre $\mathbb{Z}[\rho]$ para $\rho = i$ ou ω.

Definição 3.13. *O reticulado complexo pode ser representado por sua matriz geradora M*

$$\Lambda = \{x = \lambda M \mid \lambda \in \mathbb{Z}[\rho]^n\}, \tag{43}$$

onde $M \in M(\mathbb{C})$ e MM^H é a matriz Gram, onde H donata a transposta conjugada.

Definição 3.14. *Seja B uma matriz complexa de grau N, $\Lambda^{'}$ é um sub-reticulado complexo do reticulado complexo Λ se pode ser escrito como :*

$$\Lambda^{'} = \{x = \lambda BM \mid \lambda \in \mathbb{Z}[\rho]^n\}. \tag{44}$$

Desde que Λ tem uma estrutura de grupo aditivo pode se definir que $\Lambda^{'}$ tem uma estrutura de subgrupo de Λ, pode-se referir a um grupo quociente $\Lambda/\Lambda^{'}$ como partição de reticulados. A cardinalidade da partição de reticulados $\Lambda/\Lambda^{'}$ é chamado índice do subreticulado $\Lambda^{'}$. Este índice é calculado como:

$$|\Lambda/\Lambda^{'}| = \frac{vol(\Lambda^{'})}{vol(\Lambda)} = \frac{\sqrt{det(\Lambda^{'})}}{\sqrt{det(\Lambda)}} = |det(B)|. \tag{45}$$

Os reticulados complexos $\Lambda = \Lambda_{\mathscr{J}}$ podem ser obtidos do ideal correspondente $\mathscr{J} \subseteq \mathscr{O}_L$ via o mergulho complexo definido como o homomorfismo $\sigma : L \to \mathbb{C}^N$,

$$\sigma(x) = (\sigma_0(x) = id(x), \sigma(x), \ldots, \sigma_{N-1}(x)), \tag{46}$$

com $x = x_0 + x_1\theta + \cdots + x_{N-1}\theta^{N-1}$ onde $x_i \in \mathbb{Z}[\rho], \forall\, i = 0, \ldots, N-1$ e $\sigma_i \in Gal(L/F), \forall\, i = 0, \ldots, N-1$.

Consequentemente, se $\mathscr{J}$ é um ideal do anel $\mathscr{O}_L$ e desde que $\{1, \theta^1, \ldots, \theta^{N-1}\}$ é uma base-$\mathbb{Z}[\rho]$, a matriz geradora M dos reticulados complexos $\Lambda_{\mathscr{J}}$ se escreve como:

$$M = \begin{pmatrix} id(1) & \ldots & \sigma_{N-1}(1) \\ \vdots & & \vdots \\ id(\theta^{N-1}) & \ldots & \sigma_{N-1}(\theta^{N-1}) \end{pmatrix}. \tag{47}$$

4 QUANTIZAÇÃO DE CANAL BASEADO NA TEORIA DE NÚMEROS ALGÉBRICOS

Neste capítulo é proposto uma nova sugestão de quantificação de canal a partir de reticulados algébricos obtidos a partir de corpos de números $\mathbb{Q}(\zeta_{9.2^2})$. Para este propósito será apresentado a seguir as relações existentes entre a teoria de corpos algébricos, os reticulados e os problemas de modulação de codificação de canal.

A base deste capítulo são os trabalhos relacionados à codificação em ambientes de comunicação com interferência de multipercursos (DELFT; MAGNIFICUS, 2007; EREZ; ZAMIR, 2004; FORNEY, 1988; NAZER; GASTPAR, 2011)

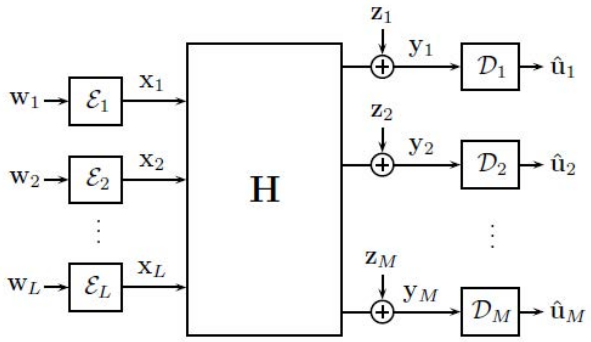
4.1 ESTRATÉGIA COMPUTER-AND-FORDWARD

A estratégia compute-and-forward foi proposta por (NAZER; GASTPAR, 2011a), permitindo decodificar equações lineares da mensagem transmitida usando combinações lineais ruidosas do canal. O receptor é capaz de recuperar (decodificar a mensagem transmitida) por meio de uma quantidade suficiente de combinações lineares.

A estratégia compute-and-forward traz uma mudança de paradigma na forma com que os problemas de interferência sempre foram tratados na literatura, já que a interferência sempre foi vista como um desvantagem em uma rede de comunicação. Já na estratégia compute-and-forward interferência é utilizada de forma favorável ao usuário.

A técnica basada em códigos reticulados aninhados, esses códigos apresentam uma estrutura linear, o que assegura que combinações lineares das palavras-código destes códigos também sejam uma palavra-código pertencente ao código. O esquema de codificador de canal na qual será feita a análise dos sinais transmitidas na rede de comunicação por meio das estruturas algébricas envolvidas está ilustrado na Figura 13.

Figura 13 - Sistema MIMO numa rede AWGN.



Fonte: Nazer e Gastpar (2011a)

Cada transmissor é equipado com um codificador de canal representado por blocos de diagrama que será denotado por ε_l; na sequência, cada palavra-código fonte, $\mathbf{w}_l$, de comprimento k, é mapeada a partir de $\mathbb{F}_p^k$ onde $\mathbb{F}_p$ denota um corpo finito de cardinalidade prima. O que determina uma codificação em $\mathbb{C}^n$, da forma $\varepsilon_l : \mathbb{F}_p^k \to \mathbb{C}^n$, gerando assim as palavras-códigos $\mathbf{x}_l = \varepsilon_l(w_l)$ que são elementos do código reticulado.

O modelo do canal é representado pela matriz $\mathbf{H} \in \mathbb{C}^{(M\times L)}$, de tal modo que a resposta do canal ao sinal transmitida é representada pela (48)

$$\mathbf{y}_m = \sum_{l=1}^{L} h_{ml}\mathbf{x}_l + \mathbf{z}_m, \tag{48}$$

onde $h_{ml} \in \mathbb{C}$ são os coeficientes do canal e $\mathbf{z}_m$ denota o ruído Gaussiano.

4.2 ESTRATÉGIA COMPUTE-AND-FORWARD BASEADA EM RETICULADOS SOBRE $\mathbb{Z}[\omega]$

Tunali (TUNALI et al., 2012) propôs um novo esquema para a estratégia de compute-and-forward baseado nos códigos reticulados definidos sobre $\mathbb{Z}[\omega]$.

Este resultado é obtido como consequência da Construção A para reticulados $\mathbb{Z}[\omega]$, e são reticulados obtidos pelo mergulho de corpos lineares $\mathbb{C}$ definidos sobre um corpo finito $\mathbb{F}_p$ em $\mathbb{R}^n$ ou $\mathbb{C}^{\frac{n}{2}}$, desde que n seja par.

A seguir é descrito alguns resultados básicos sobre os anéis $\mathbb{Z}[\omega]$ e dos reticulados definidos sobre $\mathbb{Z}[\omega]$.

Tem-se também que Λ_f é um reticulado alinhado de dimensão n sobre $\mathbb{Z}[\omega]$ e Λ um reticu-

lado de dimensão n sobre $\mathbb{Z}[\omega]$, Λ, é aninhado em Λ_f se $\Lambda \subseteq \Lambda_f$.

Outra importante observação é que Λ e Λ_f são reticulados escalonados, o que assegura que o segundo momento de Λ é igual a $P/2$. Finalmente, pode-se obter os códigos reticulados a partir de $\Lambda_f \bigcap V(\Lambda)$, onde $V(\Lambda)$ é a região associada de Voronoi associado ao reticulado Λ.

Seja $\mathscr{P}$ um ideal primo ou potência de um ideal primo no anel $\mathbb{Z}[\omega]$. Um fato bem conhecido na literatura é de que o grupo quociente $\mathbb{Z}[\omega]/\mathscr{P}\mathbb{Z}[\omega]$ é um isomorfismo a um corpo finitos $\mathbb{F}_q$, onde q determina a cardinalidade do corpo . Basta considerar um homomorfismo como descrito em (49), onde $\pi(a) \in \mathbb{F}_q$, $\forall\, a \in \mathbb{Z}[\omega]$.

$$\pi : \mathbb{Z}[\omega] \to \mathbb{Z}[\omega]/q\mathbb{Z}[\omega] \to \mathbb{F}_q. \tag{49}$$

Um reticulado de dimensão n sobre $\mathbb{Z}[\omega]$ em termos da matriz geradora complexa $M \in \mathbb{C}^{n\times k}$, pode ser expresso na forma:

$$\Lambda = \{\lambda = eM \ : \ e \in \mathbb{Z}[\omega]^k\} \tag{50}$$

A partir dos parâmetros dados pelos inteiros positivos, n, k, q satisfazendo a condição de que $k \leq n$, pode-se obter a matriz geradora M com elementos em $\mathbb{F}_q^n$ associada a código reticulados de dimensão n por meio da Construção A; para isto basta realizar a sequência de passos descritos a seguir:

1. O código discreto $\mathscr{C}$ é obtido como $\mathscr{C} = \{x = Gy : y \in \mathbb{F}_q^k\}$.
2. Gera-se um reticulado de dimensão n sobre $\mathbb{Z}[\omega]$ da forma $\Lambda_{\mathscr{C}} = \{\lambda \in \mathbb{Z}[\omega]^n : \pi(\lambda) \in \mathscr{C}\}$ através de π do código $\mathscr{C}$ sobre $\mathbb{C}^n$ de tal forma que tenha geometricamente o formato $\mathbb{Z}[\omega]^n$.
3. Escalar $\Lambda_{\mathscr{C}}$ com π^{-1} para obter $\Lambda = \pi^{-1}(\mathscr{C})$.

Os autores em (TUNALI et al., 2012) propuseram um procedimento similar a (NAZER; GASTPAR, 2011a) para obter reticulados sobre $\mathbb{Z}[\omega]$ da seguinte maneira:

i. HEX: Região fundamental de Voronoi do reticulado $\mathbb{Z}[\omega]^n$.

ii. $HEX\ \ GRID$: Os reticulados $q^{-1}\mathbb{Z}[\omega]^n$, onde q é primo ou potência de números primos no anel inteiro $\mathbb{Z}[\omega]$.

iii. $x^* = x \mod HEX = x \mod \mathbb{Z}[\omega]^n = x - [x]$, onde $x \in \mathbb{C}^n$ e $[.]$ identificam os vetores inteiros mais próxima x que pertencem a $\mathbb{Z}[\omega]^n$.

iv. $\mathscr{A} = \mathscr{A}^*$ mod HEX, onde $\mathscr{A}$ tomado em $\mathbb{C}^n$ e via a operação mod HEX realizada elemento por elemento.

v. $\mathscr{A}' = \mathscr{A} - \{0\}$, onde $\mathscr{A} \subset \mathbb{R}^n$, $\mathscr{A} \subset \mathbb{R}^n$ ou $\mathscr{A} \subset \mathbb{F}_q^n$.

vi. Λ: Um reticulado alinhado sobre $\mathbb{Z}[\omega]$ de dimensão n em $HEX\ GRID$, por exemplo, $\Lambda \subset HEX\ GRID$.

vii. $Vol(.)$ Volumem fechado em $\mathbb{C}^n$.

viii. $HEX\ GRID^*$: $HEX\ GRID \cap HEX$.

A partir destas considerações, Tunali (TUNALI et al., 2012) demonstra a existência de reticulados sobre $\mathbb{Z}[\omega]$ os quais são simultaneamente bons para problemas relacionados a quantificação e codificação de canal AWGN. Assim pode-se obter a partir de Construção A.

5 DESENVOLVIMENTO DA PROPOSTA

5.1 PARTE I: TEORIA DE CORPOS ALGEBRICOS

A teoria exposta nas seções 2.1, 2.2, 2.3 e 2.4 no capítulo 2, sobre a teoria dos números algébricos, já é suficiente para a construção dos reticulados algébricos que utilizaremos na estratégia compute-and-fordward para a quantização de canal.

Considerando os corpos ciclotômicos expostos na seção 2.4, definidos por $L = \mathbb{Q}(\zeta_{9.2^s})$, onde

$$\zeta_{9.2^s} = e^{\frac{2\pi i}{9.2^s}} = \cos\left(\frac{2\pi}{9.2^s}\right) + i\sin\left(\frac{2\pi}{9.2^s}\right), \tag{51}$$

baseado em (22), onde $\zeta_{9.2^s}$ denota a raíz 9.2^s-ésima da unidade, com $s \geq 2$.

Calculando o grau de $L/\mathbb{Q}$ pela (24) utilizando a função de Euler $\varphi(n)$ (ver detalhe (GIRAUD; BOUTILON; BELFIORE, 1997)),, tem-se que:

$$[L : \mathbb{Q}] = \varphi(n) = 3.2^s. \tag{52}$$

Dado que $\mathbb{Q}(\omega)/\mathbb{Q}$ é de grau 2 e a propriedade da função de Euler, se p e q são ambos primos tem-se que $\varphi(p \times q) = \varphi(p) \times \varphi(q)$. Logo o grau de $L/\mathbb{Q}(\omega)$ é dado por:

$$[L : \mathbb{Q}(\omega)] = N = \frac{\varphi(n)}{2} = 3.2^{s-1}. \tag{53}$$

Da extensão de Galois tem-se que

$$Gal(L/\mathbb{Q}) =< \sigma >= \{id, \sigma, \ldots, \sigma_{\varphi(n)-1}\} \text{ onde } \varphi(n) = 3.2^s, \tag{54}$$

onde σ denota algum homomorfismo $\sigma_j \in Gal(L/\mathbb{Q})$ que satisfaz a condição (55) de acordo com (25):

$$\sigma_j(\zeta_{9.2^s}) = \sigma_{9.2^s}^j \text{ onde } MDC(9.2^s, j) = 1. \tag{55}$$

A base integral de $\mathscr{O}_L = \mathbb{Z}[\zeta_{9.2^s}]$ de acordo com (26) é dada por

$$B = \{1, \zeta_{9.2^s}, \ldots, \zeta_{9.2^s}^{\varphi(n)-1}\} \text{ onde } \varphi(n) = 3.2^s. \tag{56}$$

A partir da família de corpos ciclotômicos $L_s = \mathbb{Q}(\zeta_{9.2^s})$ com $s \geq 2$, pode-se obter subcorpos

e relações entre a raiz da unidade como descrito a seguir:

Facilmente, verifica-se pelo (51) que:

$$\zeta_{9.2^s}^2 = \zeta_{9.2^{s-1}}. \tag{57}$$

O que faz sentido reescrever

$$L_s = L_{s-1}(\zeta_{9.2^s}) = \{w = x + y\zeta_{9.2^s} \mid x, y \in L_{s-1}\}. \tag{58}$$

Como consequência, obtém-se uma cadeia de extensões de corpos do tipo:

$$L_s/L_{s-1}/\cdots/L_3/L_2/L_0/F/K. \tag{59}$$

Figura 14 - Cadeia de Extensão de Corpos.

$$\begin{array}{c} L = L_s = \mathbb{Q}(\zeta_{9.2^s}) \\ | \\ L_{s-1} = \mathbb{Q}(\zeta_{9.2^{s-1}}) \\ | \\ \vdots \\ | \\ L_3 = \mathbb{Q}(\zeta_{9.2^3}) \\ | \\ L_2 = \mathbb{Q}(\zeta_{9.2^2}) \\ | \\ L_0 = \mathbb{Q}(\zeta_9) \\ | \\ F = \mathbb{Q}(\omega) \\ | \\ K = \mathbb{Q} \end{array}$$

Fonte: o próprio autor

Satisfazendo a relação de grau de (23), (24), (52) e (53) tem-se que

$$[L = L_s : L_{s-1}] = [L_{s-1} : L_{s-2}] = \cdots = [L_3 : L_2] = [L_2 : L_0] = 2,\ [L_0 : F] = 3,\ [F : K] = 2 \tag{60}$$

onde $F = \mathbb{Q}(\omega)$ e $K = \mathbb{Q}$.

Observe-se na Figura 15 que a extensão de corpos de $\mathbb{Q}(\omega)$ pode ser para dois corpos do mesmo grau, $\mathbb{Q}(\zeta_9)$ e $\mathbb{Q}(\zeta_{9.2})$, sendo os casos respectivos de $s = 0$ e $s = 1$ corpos isomorfos. Para nosso caso, se trabalha com a extensão de corpos $\mathbb{Q}(\zeta_9)$ para $s = 0$, como apresentado na Figura 15a.

Figura 15 - Grau da extensão de corpo.

(a) Grau extensão de corpo até $s = 3$; $\mathbb{Q}(\zeta_9)$ sobre $\mathbb{Q}(\omega)$

(b) Grau extensão de corpo até $s = 3$; $\mathbb{Q}(\zeta_{9.2})$ sobre $\mathbb{Q}(\omega)$

Fonte: o próprio autor

O polinômio minimal $p(x) \in L_{s-1}$ de acordo com a Definição 2.10 associado ao elemento primitivo de $\zeta_{9.2^s}$ considerando o Teorema 2.2 é escrito na forma:

$$p(x) = x^2 - \zeta_{9.2^{s-1}} \tag{61}$$

considerando (57), se reescreve (61) como

$$p(x) = x^2 - \zeta_{9.2^s}^2 = (x - \zeta_{9.2^s})(x + \zeta_{9.2^s}), \tag{62}$$

é a base de L_s sobre L_{s-1} é

$$\{1, \zeta_{9.2^s}\}. \tag{63}$$

Como consequência do Teorema 2.3 e (18), o grupo de Galois associado a extensão de corpos L_s/L_{s-1} é dado por:

$$Gal(L_s/L_{s-1}) = \{\sigma_1(\zeta_{9.2^s}), \sigma_2(\zeta_{9.2^s})\}, \tag{64}$$

com $\sigma_1(\zeta_{9.2^s}) = \zeta_{9.2^s} = id$, onde id é a identidade e $\sigma_2(\zeta_{9.2^s}) = -\zeta_{9.2^s}$ são as raízes do polinômio minimal dado por (62).

Agora, determina-se o grupo de Galois associado a extensão finita do corpo L_s sobre $\mathbb{Q}(\omega)$.

Seja L_s um corpo de extensão finita sobre $\mathbb{Q}(\omega)$ para $s \geq 2$. Como consequência, o grau da extensão de corpo L_s sobre $\mathbb{Q}(\omega)$ é dado por 3.2^{s-1} e $Gal\,(L_s/\mathbb{Q}(\omega))$ é cíclico com grau 3.2^{s-1}, então pode-se escrever $L_s = \mathbb{Q}(\omega)(\zeta_{9.2^s}) = F(\zeta_{9.2^s})$ onde, a base do corpo L_s visto como espaço vetorial sobre $\mathbb{Q}(\omega)$ de acordo com (26),é dada por

$$\{1, \zeta_{9.2^s}, \zeta_{9.2^s}^2, \ldots, \zeta_{9.2^s}^{N-1}\}, \tag{65}$$

onde $N = \varphi(n)/2 = 3.2^{s-1}$.

O polinômio minimal $p(x)$ sobre $\mathbb{Q}(\omega)$ de acordo com a Definição 2.10 associado ao elemento primitivo de $\zeta_{9.2^s}$ considerando o Teorema 2.2 é escrito na forma:

$$p(x) = \prod_{k=0}^{N-1} (x - \zeta_{9.2^s}^k). \tag{66}$$

O grupo de Galois associado a extensão de corpos $L_s/\mathbb{Q}(\omega)$ de acordo a Teorema 2.3 é dado por:

$$Gal(L_s/\mathbb{Q}(\omega)) = \{\sigma_1(\zeta_{9.2^s}), \sigma_2(\zeta_{9.2^s}), \ldots, \sigma_N(\zeta_{9.2^s})\}, \tag{67}$$

com

$$\sigma_1(\zeta_{9.2^s}) = \zeta_{9.2^s} = id, \sigma_2(\zeta_{9.2^s}) = \zeta_{9.2^s}^2, \ldots, \sigma_N(\zeta_{9.2^s}) = \zeta_{9.2^s}^{N-1}, \tag{68}$$

onde $\zeta_{9.2^s}^k$,$\forall\, k = 0, ..., N-1$ são as raízes do polinômio minimal dado por (66).

5.2 PARTE II: APROXIMAÇÂO DOS COEFICIENTES DO CANAL *H*

5.2.1 Construção de reticulados aninhados sobre $\mathbb{Z}[\omega]$

Nesta seção se propõe um novo esquema de codificação baseado em partição de cadeias de reticulados sobre $\mathbb{Z}[\omega]$ para quantificação dos coeficientes de canal.

Neste esquema é preciso saber apenas os coeficientes dos canais para cada transmissor neles mesmo. Por isso, considera-se a interferência do canal como um valor complexo dado por $a_{ml} \in \{\mathbb{Z} + \omega\mathbb{Z}\}$.

Em (TUNALI et al., 2012), os autores demonstram e garantiram a existência de códigos reticulados aninhados sobre $\mathbb{Z}[\omega]$ os quais apresentam um bom desempenho para problemas de quantificação e codificação de canais. Adicionalmente, mostrou-se a possibilidade de obter um canal equivalente induzido pela transformação de modulo-Λ. Neste modelo de canal "virtual"cada receptor analisa os pontos do reticulado dados pela combinação linear sobre $\mathbb{Z}[\omega]$ do tipo:

$$\mathbf{y_m} = \sum_{l=1}^{L} a_{ml}\mathbf{t_l} + \mathbf{z_{eq,m}}. \tag{69}$$

O modelo de canal "virtual"é um equivalente apresentado em (48). Desta maneira isto equivale aplicar U no vetor receptor (69):

$$\bar{y}_m = Uy_m = \sum_{l=1}^{L} a_{ml}Ut_l + Uz_{eq,m}. \tag{70}$$

Como $z_{eq,m}$ é ruido circular simétrico complexo Gaussiano i.i.d. e U é unitário, em (70). Tem-se o vetor da forma $a_{ml}Ut_l$, por simplicidade de notação, será denotado por:

$$\bar{x} = h \cdot U \cdot x \tag{71}$$

onde $x = t_l$ é o ponto de reticulado transmitido pelo usuário considerado e $h = a_{ml}$ é o coeficiente do canal. Reescrevendo (71), tem se:

$$\begin{pmatrix} h & 0 & \cdots & 0 \\ 0 & h & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h \end{pmatrix} \cdot U \cdot x = H \cdot U \cdot x. \tag{72}$$

Nesta etapa, tem-se como meta quantificar a matriz diagonal H pela matriz diagonal. Para isso, é preciso quantificar a matriz diagonal H pelo ruído gaussiano com U unitária que também deve satisfazer as expressões (69), (71) e (72).

A nossa contribuição neste trabalho é realizar a quantificação da matriz H por meio de matrizes unitárias contruídas via reticulados obtidos via Construção A.

Esta construção é baseada em resultados obtidos via códigos cíclicos sobre corpos finitos $\mathbb{F}_3$ como proposto por Forney (FORNEY, 1988b),, os autores em (GIRAUD; BOUTILON;BELFIORE, 1997) construíram famílias de reticulados complexos sobre $\mathbb{Z}[\omega]$, $\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]}$, que são isomorfos aos reticulados $\mathbb{Z}[\omega]^N$, onde $N = 3.2^{s-1}$.

Como consequência do inteiro positivo 3 ser totalmente ramificado na extensão $\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}$, construiremos cadeias de reticulados alinhados a partir de reticulados algébricos $\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]}$.

Neste sentido, consideremos famílias de anéis de inteiros de corpos ciclotômicos $\mathbb{Q}(\zeta_{9.2^s})$, com $s \geq 2$. Pode-se usar as ferramentas algébricas dos copos ciclotômicos $\mathbb{Q}(\zeta_{9.2^s})$ para obter a cadeia de reticulados aninhados sobre $\mathbb{Z}[\omega]$ a partir dos reticulados $\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]}$ isomorfos aos reticulados-$\mathbb{Z}[\omega]^N$.

Sabendo que $\{1, \zeta_{9.2^s}, \zeta_{9.2^s}^2, \ldots, \zeta_{9.2^s}^{N-1}\}$ da (65) é uma base sobre $\mathbb{Z}[\omega]$ para o anel de inteiros, então a matriz geradora M_0 do reticulado algébrico $\Lambda_{\mathbb{Z}_{\zeta_{9.2^s}}}$ descrito em (47) é dado por:

$$M_0 = \begin{pmatrix} id(1) & \sigma_2(1) & \ldots & \sigma_N(1) \\ id(\zeta_{9.2^s}) & \sigma_2(\zeta_{9.2^s}) & \ldots & \sigma_N(\zeta_{9.2^s}) \\ id(\zeta_{9.2^s}^2) & \sigma_2(\zeta_{9.2^s}^2) & \ldots & \sigma_N(\zeta_{9.2^s}^2) \\ \vdots & \vdots & & \vdots \\ id(\zeta_{9.2^s}^{N-1}) & \sigma_2(\zeta_{9.2^s}^{N-1}) & \ldots & \sigma_N(\zeta_{9.2^s}^{N-1}) \end{pmatrix} \tag{73}$$

Observação 5.1. *A matriz M_0 e M_0^T tem as mesmas propriedades, considerando que temos $M_0' = \frac{1}{\sqrt{N}} M_0$ pode-se ter que $(M_0')(M_0')^H$ é igual a matriz identidade, onde $(M_0')^H$ denota a transposta conjugada de M_0'. Então $M_0' = \frac{1}{\sqrt{N}} M_0$ é uma matriz unitária e usando as propriedades básicas é fácil de comprovar que $U = \frac{1}{\sqrt{N}} M_0^T$.*

(GIRAUD; BOUTILON; BELFIOIRE, 1997)

Com o modelo apresentado, considere $\mu = 1 + \zeta_{9.2^s}$ um elemento do ideal $\Im\mathbb{Z}[\zeta_{9.2^s}]$ no anel dos inteiros $\mathscr{O}_L = \mathbb{Z}[\zeta_{9.2^s}]$ do corpo ciclotômico $\mathbb{Q}(\zeta_{9.2^s})$, de grau finito N sobre $\mathbb{Q}(\omega)$, tal que, $\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]}$ é isomorfo ao reticulado-$\mathbb{Z}[\omega]^N$.

5.2.2 Construção da cadeia de reticulados aninhados sobre $\mathbb{Z}[\omega]$

Considerando ideais em $\mathbb{Z}[\zeta_{9.2^s}]$ da forma $\Im^k\mathbb{Z}[\zeta_{9.2^s}]$ obtidos como potência do ideal μ^k e suas correspondentes matrizes geradoras M_k dos reticulados algébricos $\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]}$ associados para todo $k \geq 2$.

Aproximando a matriz H com os mergulhos canônicos do gerador μ^k do $\Im^k$, onde $k \in \mathbb{Z}$, com base a Proposição 5.1:

Proposição 5.1. *Tem-se que $\{u_k, u_k\zeta_{9.2^s}, u_k\zeta_{9.2^s}^2, \ldots, u_k\zeta_{9.2^s}^{N-1}\}$ é a base sobre $\mathbb{Z}[\omega]$ de $u_k\mathbb{Z}[\zeta_{9.2^s}] = u_k\mathscr{O}_L$, onde $N = 3.2^{s-1}$, $\{1, \zeta_{9.2^s}, \zeta_{9.2^s}^2, \ldots, \zeta_{9.2^s}^{N-1}\}$ é a base sobre $\mathbb{Z}[\omega]$ de $\mathscr{O}_L$ e $u_k = \mu^k$ é o gerador do ideal $\Im^k$, com $k \in \mathbb{Z}$ e $\mu = 1 + \zeta_{9.2^s}$.*

Pela notação definida por $\zeta_{9.2^s} = \zeta$ e $\mu = 1 + \zeta_{9.2^s} = 1 + \zeta$, tem-se a matriz geradora M_k dos reticulados complexos associados a $\Lambda_{\mathbb{Z}_{\zeta_{9.2^s}}}$ na forma:

$$M_k = \begin{pmatrix} u_k & u_k\zeta & \cdots & u_k\zeta^{N-1} \\ \sigma_2(u_k) & \sigma_2(u_k\zeta) & \cdots & \sigma_2(u_k\zeta^{N-1}) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_N(u_k) & \sigma_N(u_k\zeta) & \cdots & \sigma_N(u_k\zeta^{N-1}) \end{pmatrix}$$

$$= \begin{pmatrix} u_k & 0 & \cdots & 0 \\ 0 & \sigma_2(u_k) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \sigma_N(u_k) \end{pmatrix} \cdot \begin{pmatrix} 1 & \zeta & \cdots & \zeta^{N-1} \\ 1 & \sigma_2(\zeta) & \cdots & \sigma_2(\zeta^{N-1}) \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \sigma_N(\zeta) & \cdots & \sigma_N(\zeta^{N-1}) \end{pmatrix} \tag{74}$$

A matriz H pode ser aproximada pela

$$M'_{u^k} = \begin{pmatrix} u_k & 0 & \cdots & 0 \\ 0 & \sigma_2(u_k) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \sigma_N(u_k) \end{pmatrix}. \tag{75}$$

Observe que:

$$M'_k M_0^T = \begin{pmatrix} u_k & 0 & \cdots & 0 \\ 0 & \sigma_2(u_k) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \sigma_N(u_k) \end{pmatrix} \cdot \begin{pmatrix} 1 & \zeta & \cdots & \zeta^{N-1} \\ 1 & \sigma_2(\zeta) & \cdots & \sigma_2(\zeta^{N-1}) \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \sigma_N(\zeta) & \cdots & \sigma_N(\zeta^{N-1}) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \zeta & \cdots & \zeta^{N-1} \\ 1 & \sigma_2(\zeta) & \cdots & \sigma_2(\zeta^{N-1}) \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \sigma_N(\zeta) & \cdots & \sigma_N(\zeta^{N-1}) \end{pmatrix} \cdot M_{\mu^k} = M_0^T M_{\mu^k}, \tag{76}$$

onde M_{μ^k} é uma matriz de ordem N com elementos pertencentes ao anel $\mathbb{Z}[\omega]$.

Isto significa que se $u_k = \mu^k$ gera o ideal $\mu^k \mathscr{O}_L$, então a matriz M_{μ^k} é a matriz geradora do reticulado obtido do mergulho canônico de $\Im^k$ em $\mathbb{C}^n$, e comparando as posições do reticulado-$\mathbb{Z}[\omega]^N$ é igual a k.

Para $k = 1$ tem-se:

$$\begin{pmatrix} \mu & 0 & \cdots & 0 \\ 0 & \sigma_2(\mu) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \sigma_N(\mu) \end{pmatrix} \cdot \begin{pmatrix} 1 & \zeta & \cdots & \zeta^{N-1} \\ 1 & \sigma_2(\zeta) & \cdots & \sigma_2(\zeta^{N-1}) \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \sigma_N(\zeta) & \cdots & \sigma_N(\zeta^{N-1}) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \zeta & \cdots & \zeta^{N-1} \\ 1 & \sigma_2(\zeta) & \cdots & \sigma_2(\zeta^{N-1}) \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \sigma_N(\zeta) & \cdots & \sigma_N(\zeta^{N-1}) \end{pmatrix} \cdot M_\mu = M_0^T M_\mu \tag{77}$$

pela indução, tem-se que para $k \geq 1$:

$$M'_1 M_0^T = M_0^T (M_\mu)^k,$$

tal que,

$$M_{\mu^k} = (M_\mu)^k$$

Os coeficientes do canal são aproximados pela matriz diagonal M'_{μ^k}, com elementos de m_{ii}, que são dados pelo $\sigma^k(\mu)^k$, e $\sigma \in Gal(\mathbb{Q}(\zeta)/\mathbb{Q}(\omega)$ onde $N = [\mathbb{Q}(\zeta) : \mathbb{Q}(\omega)]$.

Desde que $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}(\omega)$ é de ordem cíclica N, podendo-se obter $\sigma^k = \sigma^r$, onde $k = r \mod N$, $(0 \leq r < N)$.

Como consequência, é obtida uma cadeia infinita de reticulados definidos sobre $\mathbb{Z}[\omega]$ de forma periódica $\Lambda_{\mathfrak{J}^k}$, ou seja, existe $N \in \mathbb{N}$, tal que, a cadeia de reticulados sobre $\mathbb{Z}[\omega]$ satisfaz:

$$\begin{aligned} \Lambda_{\mathbb{Z}[\zeta]} = \Lambda_{\mathfrak{J}^0}, \Lambda_{\mathfrak{J}}, \ldots, \Lambda_{\mathfrak{J}^{N-1}}, \Lambda_{\mathfrak{J}^N} = \\ \Lambda_{\mathfrak{J}^0}, \Lambda_{\mathfrak{J}^{N+1}} = \Lambda_{\mathfrak{J}}, \ldots, \Lambda_{\mathfrak{J}^{N+N-1}} = \Lambda_{\mathfrak{J}^{N-1}} \ldots \end{aligned} \tag{78}$$

como também satisfaz:

$$\Lambda_{\mathbb{Z}[\zeta]} \supset \Lambda_{\mathfrak{J}} \ldots \supset \Lambda_{\mathfrak{J}^{N-1}} \tag{79}$$

Proposição 5.2.

1. *Cada reticulado complexo ideal $\Lambda_{\mathfrak{J}^r}$ é um sub-reticulado dos reticulados complexos $\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]}$, cujo índice associado nesta partição de reticulados é $[\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]} : \Lambda_{\mathfrak{J}^r}] = 3^r$, para cada $r = 1, \ldots, N-1$.*

2. *Cada reticulado complexo ideal $\Lambda_{\mathfrak{J}^{r-1}}$ é um sub-reticulado dos reticulados complexos $\Lambda_{\mathfrak{J}^r}$, cujo índice associado nesta partição de reticulados é dado por $[\Lambda_{\mathfrak{J}^r} : \Lambda_{\mathfrak{J}^{r-1}}] = 3$, para cada $r = 1, \ldots, N-1$.*

Prova 5.1.

1. *Observe que o fato $\Lambda_{\mathfrak{J}^r}$ deve ser um sub-reticulado dos reticulados complexos $\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]}$ é consequência direta da Observação 5.1. Quando o índice dos reticulados complexos $\Lambda_{\mathfrak{J}}$ é calculado pelo reticulados complexos $\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]}$, tem-se*

$$\mid \Lambda_{\mathbb{Z}[\zeta_{9.2^s}]} : \Lambda_{\mathfrak{J}^r} \mid = \frac{vol(\Lambda_{\mathfrak{J}^r})}{vol(\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]})}.$$

Considerando o reticulado real $\Lambda_{\mathfrak{J}^r}$ e $\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]}$ que foi obtido pelos reticulados algébricos dados por $\Lambda_{\mathfrak{J}^r}$ e $\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]}$, respetivamente, então para o caso $r = 1$, obtem-se:

$$3 = N(\mathfrak{I}) = \mid \mathbb{Z}[\zeta_{9.2^s}] : \mathfrak{I} \mid = \frac{vol(\Lambda_{\mathfrak{J}})}{vol(\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]})} = \mid \Lambda_{\mathbb{Z}[\zeta_{9.2^s}]} : \Lambda_{\mathfrak{J}} \mid .$$

Para o caso geral, usa-se a propriedade multiplicativa da norma relativa. Consequentemente, obtêm-se:

$$3^r = N(\Im^r) = \mid \mathscr{O}_L : \Im^r \mid = \frac{vol(\Lambda_{\Im^r})}{vol(\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]})}.$$

Por isso, $\mid \Lambda_{\mathbb{Z}[\zeta_{9.2^s}]} : \Lambda_{\Im^r} \mid = 3^r$*, a partir de* $3 = N(\Im)$.

2. *O índice dos reticulados complexos ideais* $\Lambda_{\Im^r}$ *pelos reticulados complexos* $\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]}$ *é dado por:*

$$\mid \Lambda_{\Im^r} : \Lambda_{\Im^{r-1}} \mid = \frac{\frac{vol(\Lambda\Im^r)}{vol(\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]})}}{\frac{vol(\Lambda_{\Im^{r-1}})}{vol(\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]})}} = \frac{3^r}{3^{r-1}} = 3.$$

Observe que cada ideal em $\mathbb{Z}[\zeta_{9.2^s}]$ integrado pelo elementos dados $\Im^k$ por $k = 0, 1, \ldots, N-1$, se obtêm da partição de reticulados sobre $\mathbb{Z}[\omega]$ dados por (81)

$$\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]} / \Lambda_{\Im} / \Lambda_{\Im^2} / \ldots / \Lambda_{\Im^{N-2}} / \Lambda_{\Im^{N-1}}, \tag{80}$$

onde $\mid \Lambda_{\Im^r} / \Lambda_{\Im^r} \mid = 3, \forall r = 1, \ldots, N-1$ satisfaz (78):

$$\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]} \supset \Lambda_{\Im} \ldots \supset \Lambda_{\Im^{N-1}}. \tag{81}$$

É por isso que por cada índice $k \geq N$, se obtém:

$$\Lambda_{\mathbb{Z}[\zeta]} = \Lambda_{\Im^0}, \Lambda_{\Im}, \ldots, \Lambda_{\Im^{N-1}}, \Lambda_{\Im^N} = \Lambda_{\Im^0}, \Lambda_{\Im^{N+1}} = \Lambda_{\Im}, \ldots, \Lambda_{\Im^{N+N-1}} = \Lambda_{\Im^{N-1}} \ldots \tag{82}$$

Observação 5.2.

1. *Pode-se obter,* $\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]}$ *isomorfismo dos reticulados sobre* $\mathbb{Z}[\omega]^N$*. Pela Observação 5.1 é preciso só normalizar N, onde* $N = 3.2^{s-1}$.

2. *Para obter a matriz geradora associada a* $\Lambda_{\Im^k}$ *a transformação necessária na (79), é preciso normalizar a matriz geradora associada para os reticulados sobre* $\mathbb{Z}[\omega]$ *por* $1/N3^k$ *para cada* $k = 0, \ldots, N-1$.

6 CONCLUSÕES

Quando se fala a respeito de mensagens, pode-se entender símbolos ou letras que se pretende transmitir; para que a transmissão seja realizada com êxito é preciso quantificar a informação que contêm a mensagem, assim Shannon define esta quantidade como uma relação logarítmica da probabilidade de cada um dos símbolos que contém a mensagem. Mas o transporte da mensagem é obstáculo enfrentado em diferentes tipos de interferência presentes no ambiente, por isso acaba afetando os parâmetros de energia do sinal que se quer transmitir, fazendo uso do modelo de Costa (COSTA, 1985) o sistema de transmissão é desenhado. A proposta enfoca na codificação de canal para alcançar a comunicação sem fio com sucesso para o sistema MIMO.

Em modulação codificada, isto é, na codificação do canal os sinais são representados por palavras-código, desta maneira os sistemas de comunicação podem ser representados matematicamente através de ferramentas algébricas da teoria dos números algébricos. As vantagens da representação das palavras-código sobre corpos são as propriedades de linearidade, associativas e comutativas em suas operações aditivas e multiplicativas, permitindo um desempenho eficiente de códigos; simplificando os cálculos que são necessários para desenvolver métodos de detecção e correção de erros no canal.

Os reticulados provenientes de corpos de números possuem propriedades geométricas que são adaptadas às constelações dos sinais modulados, onde se podem identificar parâmetros tais como densidade, raios e áreas limitantes para as decisões de palavras-código no processo de demodulação. De acordo com os parâmetros mencionados, procura-se encontrar reticulados com maior densidade, dependendo das áreas de empacotamento, associados aos corpos utilizados.

Com a estratégia apresentada por (NAZER; GASTPAR, 2011a) pode-se utilizar o ruído de forma benéfica para realizar a quantificação da mensagem a transmitir, por meio de sistemas lineares. Associando com os reticulados pela Construção A, definindo desta maneira códigos de reticulados aninhados $\mathbb{Z}[\rho]$ onde $\rho = i$ ou ω.

A partir da garantia da existência dos códigos reticulados alinhados sobre $\mathbb{Z}[\omega]$ proposto por (TUNALI et al., 2012) é apresentado o esquema para definir a partição da cadeia de reticulados dos coeficientes do canal pelo esquema de (TRINCA, 2013) pelo sua matriz geradora formada pelo elemento ideal $\zeta_{9.2^s}$. Com os códigos reticulados alinhados $\mathbb{Z}[\omega]$ dos subreticulados de

$\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]}$ tem-se melhor quantificação com eles, obtendo uma partição dupla de cadeia infinita de reticulados.

Como trabalhos futuros pode-se calcular a cadeia de reticulados complexos aninhados sobre $\Lambda_{\mathbb{Z}[\zeta_{9.2^s}]}$ apresentando seu índice de erro quadrático mínimo (MMSE, minimum mean square error).

REFERÊNCIAS

ALVES, C. *Reticulados e códigos.* 2008. 133 f. Tese (Doutorado) - Departamento de Matemática, Universidade Estadual de Campinas, São Paulo, 2008.

BORADDE, S.; ZHENG, L.; GALLAGER, R. Amplify-and forward in wireless realy networks: rate, diversity and network size *IEEE Trans Inform. Theory*, New York, v. 53, n. 10, p. 3302-3318, Oct. 2007.

CARLEIAL, A. B. A case where interference does not reduce capacity. *IEEE Trans. Inform. Theory*, New York, v.21, n.5, p.596-597, Sep. 1975.

COSTA, H. M. On the gaussian interference channel,. *IEEE Trans Inform. Theory*. New York, IT-31,n. 5,p. 607-615, Jan. 1985.

EREZ, U.; LITSYN, S.; ZAMIR, R. Lattices which are good for (almost) everything. *IEEE Trans. Inform. Theory*, New York, v. 51, n. 10, p. 3401-3416, Oct. 2005.

FORNEY, G. D. Coset codes. i. introduction and geometrical classification. *IEEE Trans. Inform. Theory*, New York, v. 34, n. 5, p. 1123-1151, Sep. 1988.

FORNEY, G. D. Coset codes. ii. introduction and geometrical classification. *IEEE Trans. Inform. Theory*, New York, v. 34, n. 5, p. 1152-1187, Sep. 1988.

GIRAUD, X.; BOUTILON, E.; BELFIORE, J. Algebraic tools to build modulation schemes for fading channels. *IEEE Trans. Inform. Theory*, New York, v. 43, n. 3, p. 938-952, May. 1997.

HAN, T. S.; KOBAYASHI, K. A new achievable rate region for interference channel. *IEEE Trans. Inform. Theory*, New York, it-27, n. 1, p. 49-61, Jan. 1981.

KRAMER, G.; GASTPAR, M.; P., G. Cooperative strategies and capacity theorems for relay networks. *IEEE Trans. Inform. Theory*, New York, v. 51, n. 9, p. 3037-3063, Sep. 2005.

LANEMANL, J. N.; C., T. N.; W., W. Cooperative diversity in wireless networks: efficient protocols and outage behavior. *IEEE Trans. Inform. Theory*, New York, v. 50, n. 12, p. 3062-3080, Dic. 2004.

NAZER, B.; GASTPAR, M. Compute-and-forward: harnessing interference through structured codes. *IEEE Trans. Inform. Theory*, New York, v. 57, n. 10, p. 6463-6486, Oct. 2011.

NAZER, B.; GASTPAR, M. Reliable physical layer network coding. *Proceedings of the IEEE*, New York, v. 99, n. 3, p. 438-6486, Mar. 2011.

OGGIER, F.; BELFIORE, J. C.; VITERBO, E. Cyclic division algebras: a tool for space-time coding. *Foundations and Trends in Communications and Information Theory*, Princeton, v. 4, n. 1, p. 1-95, Jan. 2007.

OGGIER, F.; VITERBO, E. Algebraic number theory and code design for rayleigh fading channels. *Foundations and Trends in Communications and Information Theory*, Princeton, v. 1, n. 3, p. 1-88, Jan. 2004.

PALAZZO, R. *Fundamentos algébricos e geométricos dos códigos corretores de erros*. São Paulo: Universidade Estatual de Campinas, 2003.

RAPPAPORT, T. S. *Comunicações sem fio, princípios e práticas.* 2. ed. [S.l.: s.n.], 2009. p. 432.

SATO, H. The capacity of gaussian interference channel under strong interference. *IEEE Trans. Inform. Theory*, IT-27, n. 6, p. 786-788, Nov. 1981.

SHANMUGAM, K. S. *Digital and analog communication systems.* New York: Jhon Wiley and Sons, 1979. p. 600.

SHANNON, C. E. A mathematical theory of communication. *Bell System Technical Journal*, New York, v. 27, n. 1, p. 379-423;623-656, Jul, Oct 1948.

TRINCA, C. C. *A contribution to the study of channel communication systems.* 2013. 178 f. Tese (Doutorado) - Faculdade de Engenheria Elétrica, Universidade Estadual Paulista, São Paulo, 2013.

TUNALI, N. E.; NARAYANAN, K. R.; J., B. J.; HUANG, Y. C. Lattices over eisentein integer for compute-and-forward. In: CONFERENCE ALLERTON HOUSE, 51., 2012, Illnois. Annual Allerton Conference on Communication, Control, and Computing. Illinois: [s.n.], 2012. v. 51, p. 33-40.

APÊNDICE A - IDEAIS PRIMOS TOTALMENTE RAMIFICADOS NA EXTENSÃO $\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(\omega)$

Seja L um corpo ciclotômico, tal que L é uma extensão algébrica finita sobre $\mathbb{Q}(\omega)$.

Cada ideal $\mathscr{I}$ do anel de inteiros $\mathscr{O}_L$ tem uma fatoração em um produto único de ideais primos dados na forma:

$$\mathscr{I}\mathscr{O}_L = \mathfrak{I}_1^{e_1}\mathfrak{I}_2^{e_2}\ldots\mathfrak{I}_n^{e_n}. \tag{83}$$

A potência de qualquer ideal $\mathfrak{I}_i$ faz parte da fatoração $\mathscr{P}\mathscr{O}_L$ a qual é chamada de grau de ramificação de $\mathfrak{I}_i$ sobre $\mathscr{P}\mathbb{Z}[\omega]$ e é denotado pelo $e(\mathfrak{I}_i|\mathscr{P}) = e_i$.

Se $e_i \geq 2$, pode-se dizer que $\mathscr{P}$ é ramificado em $\mathscr{O}_L$. Do mesmo modo, se $\mathscr{P}\mathscr{O}_L = \mathfrak{I}^n$, pode-se dizer que $\mathscr{P}$ é totalmente ramificado em $\mathscr{O}_L$.

No trabalho tem interesse em encontrar ideais em $\mathscr{O}_L$, tal que, para algum inteiro primo $\mathscr{P}$, pode-se escrever o ideal $\mathscr{P}$ como $\mathscr{P}\mathscr{O}_L = \mathfrak{I}^N\mathscr{O}_L$, onde $\mathfrak{I}$ é um ideal primo em $\mathscr{O}_L$ e N é a dimensão da extensão do corpo $L/\mathbb{Q}(\omega)$.

Seja $\mathscr{P}$ e $\mathfrak{I}$, onde $\mathscr{P} = (1-\omega)\mathbb{Z}[\omega]$ e $\mathfrak{I} = (1-\zeta_{9.2^s})\mathscr{O}_L$ são ideais que pertencem aos anéis $\mathbb{Z}[\omega], \mathscr{O}_L$, respectivamente. Se demostrara que o ideal $\mathfrak{I}$ é totalmente ramificado na extensão de corpos $L/\mathbb{Q}(\omega)$.

Proposição A.1. *Seja $\zeta_{9.2^s}$ a 9.2^s-ésima raiz da unidade, para $s \geq 2$ e $L = \mathbb{Q}(\zeta_{9.2^s})$. Tem-se os seguintes resultados:*

1. *$\mathscr{P} = (1-\omega)\mathbb{Z}[\omega]$ é um ideal primo no anel de inteiros $\mathbb{Z}[\omega]$.*
2. *A norma relativa é dada por:*

$$N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(9.2^{s-1})}(1-\zeta_{9.2^s}) = 1-\zeta_{9.2^{s-1}}. \tag{84}$$

Prova A.1.

1. *Note-se que quando é aplicada a norma relativa $N_{\mathbb{Q}(\omega)/\mathbb{Q}}$ sobre $1-\omega$ (o elemento gerador do ideal $\mathscr{P}$), tem-se:*

$$N_{\mathbb{Q}(\omega)/\mathbb{Q}}(1-\omega) = id(1-\omega)\sigma(1-\omega) = 1-\omega^2 = 3. \tag{85}$$

Portanto, $\mathscr{P} = (1-\omega)\mathbb{Z}[\omega]$ é ideal primo em $\mathbb{Z}[\omega]$.

2. *Aplicando a norma relativa $N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(\zeta_{9.2^{s-1}})}$ sobre $1-\zeta_{9.2^s}$,tem-se*

$$N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(\zeta_{9.2^{s-1}})}(1-\zeta_{9.2^s}) = id(1-\zeta_{9.2^s})\sigma_r(1-\zeta_{9.2^s})$$
$$= (1-\zeta_{9.2^s})(1+\zeta_{9.2^s}) = 1-\zeta_{9.2^s}^2 = 1-\zeta_{9.2^{s-1}}. \quad (86)$$

Proposição A.2. *A norma relativa $N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(\omega)}$ aplicada sobre o elemento $1-\zeta_{9.2^s}$ é dada pelo $N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(\omega)}(1-\zeta_{9.2^s}) = 1-\omega, \forall s > 2$.*

Prova A.2.

1. *Para $s = 0$, tem-se que*

$$N_{\mathbb{Q}(\zeta_9)/\mathbb{Q}(\omega)}(1-\zeta_9) = id(1-\zeta_9)\sigma_3(1-\zeta_9) = (1-\zeta_9)(1+\zeta_9) = 1-\zeta_9^2 = 1-\omega. \quad (87)$$

2. *Pelo indução, sobre $s-1$, tem-se que*

$$N_{\mathbb{Q}(\zeta_{9.2^{s-1}})/\mathbb{Q}(\omega)}(1-\zeta_{9.2^{s-1}}) = 1-\omega. \quad (88)$$

Note

$$N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(9.2^{s-1})}(1-\zeta_{9.2^s}) = (1-\zeta_{9.2^s})(1+\zeta_{9.2^s}) = 1-\zeta_{9.2^s}^2 = 1-\zeta_{9.2^{s-1}}. \quad (89)$$

Pelo propriedades da norma relativa do extensão finita de corpos, tem-se que

$$N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(\omega)}(1-\zeta_{9.2^s}) = N_{\mathbb{Q}(\zeta_{9.2^{s-1}})/\mathbb{Q}(\omega)}(N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(9.2^{s-1})}(1-\zeta_{9.2^s})). \quad (90)$$

Como consequência do ponto (2) da Proposição A.1, conclui-se

$$N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(\omega)}(1-\zeta_{9.2^s}) = 1-\omega. \quad (91)$$

Proposição A.3. *A norma relativa $N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}}(1-\zeta_{9.2^s}) = 3, \forall s > 2$.*

Prova A.3.

1. *Para $s = 0$, tem-se que $\mathcal{O}_L = \mathbb{Z}[\zeta_9]$. Como consequência da propriedade da norma relativa da extensão finita de corpos e da prova do ponto (1) da Proposição A.2, tem-se que:*

$$N_{\mathbb{Q}(\zeta_9)/\mathbb{Q}}(1-\zeta_9) = N_{\mathbb{Q}(\omega)/\mathbb{Q}}(N_{\mathbb{Q}(\zeta_9)/\mathbb{Q}(\omega)}(1-\zeta_9) = N_{\mathbb{Q}(\omega)/\mathbb{Q}}(1-\omega) = 3. \quad (92)$$

2. *Pelo indução, sobre* $s-1$, *tem-se que*

$$N_{\mathbb{Q}(\zeta_{9.2^{s-1}})/\mathbb{Q}}(1-\zeta_{9.2^{s-1}}) = 3. \tag{93}$$

Note que tem-se

$$N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}}(1-\zeta_{9.2^s}) = N_{\mathbb{Q}(\zeta_{9.2^{s-1}})/\mathbb{Q}}(N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(9.2^{s-1})}(1-\zeta_{9.2^s})). \tag{94}$$

Note também que

$$N_{\mathbb{Q}(\zeta_{9.2^{s-1}})/\mathbb{Q}}(1-\zeta_{9.2^{s-1}}) = 1-\zeta_{9.2^{s-1}}. \tag{95}$$

Pelo consequência da indução sobre $s-1$, *se obtém que*

$$N_{\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}}(1-\zeta_{9.2^s}) = N_{\mathbb{Q}(\zeta_{9.2^{s-1}})/\mathbb{Q}}(1-\zeta_{9.2^{s-1}}) = 3. \tag{96}$$

Proposição A.4. *O ideal* $\mathscr{P}$ *é totalmente ramificado na extensão Galois* $\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(\omega)$.

Prova A.4. *A Proposição A.4 estabelece que o elemento* $1-\zeta_{9.2^s}$ *é primo em* $\mathbb{Z}[\zeta_{9.2^s}]$. *Consequentemente, o ideal* $\mathscr{P}$ *é um ideal primo em* $\mathbb{Z}[\zeta_{9.2^s}]$.

Como consequência da prova do Proposição A.4, pode-se reescrever o ideal $\mathscr{P}$ como $\mathscr{P} = \mathfrak{I}^N$, onde N é o grau da extensão do corpo $\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(\omega)$.

Pode-se concluir que $\mathscr{P}$ é totalmente ramificado na extensão finita de corpos $\mathbb{Q}(\zeta_{9.2^s})/\mathbb{Q}(\omega)$.