Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Campus de Rio Claro

Codificação Espaço-Temporal

Thiago Tambasco Luiz

Dissertação apresentada ao Programa de Pós-Graduação – Mestrado Profissional em Matemática Universitária do Departamento de Matemática como requisito parcial para a obtenção do grau de Mestre

Orientadora
Profa. Dra. Carina Alves

2012

Tambasco Luiz, Thiago

Codificação Espaço-Temporal/ Thiago Tambasco Luiz- Rio Claro: [s.n.], 2012.

66 f.

Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas.

Orientadora: Carina Alves

1. Código de Ouro. 2. álgebras de divisão. 3. reticulados algébricos. 4. códigos perfeitos. I. Título

Ficha Catalográfica elaborada pela STATI - Biblioteca da UNESP
Campus de Rio Claro/SP

TERMO DE APROVAÇÃO

Thiago Tambasco Luiz

Codificação Espaço-Temporal

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação Mestrado Profissional em Matemática Universitária do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Profa. Dra. Carina Alves
Orientadora

Prof. Dr. Henrique Lazari
IGCE - Unesp - Rio Claro - SP

Prof. Dr. Antônio Aparecido De Andrade
IBILCE - Unesp - São José do Rio Preto - SP

Rio Claro, 31 de Agosto de 2012

Ao meus pais Waldir Vivacqua Luiz e Rosmary Tambasco Luiz
e à minha irmã Thaís Tambasco Luiz,
dedico

Agradecimentos

Após concluir este trabalho, agradeço:

A Deus.

À minha mãe, Rosmary Tambasco Luiz, mulher forte que sempre me incentivou aos estudos e me ensinou que a perseverança é a principal virtude que podemos ter.

Ao meu pai, Waldir Vivacqua Luiz, que sempre batalhou pelo bem da família a qual esteve em primeiro lugar em todas as suas decisões.

À minha irmã, Thaís Tambasco Luiz, por ser um grande exemplo de superação e esforço para fazer da vida não uma mera passagem, mas uma realização plena de seus sonhos.

A todos os meus familiares que com tanto carinho me apoiaram.

Aos meus amigos Eliézer, Kátia, Henrique e Braz por ficarem ao meu lado nos momentos mais difíceis dessa caminhada, e não me deixarem cair quando tropecei.

Aos amigos da Confraria por todas as risadas, viagens e noites de sexta-feira tão importantes e necessárias para que chegasse até aqui.

A todos os meus outros amigos e colegas de trabalho pelo apoio e força, sempre juntos.

À minha orientadora Profª Dra. Carina Alves pela amizade, dedicação extrema e ajuda incondicional na execução desse trabalho.

À banca examinadora pelas correções e sugestões.

À Secretaria da Educação do Estado de São Paulo pelo apoio fincaneiro.

A todos que contribuíram para o sucesso deste trabalho.

A coisa mais indispensável a um homem é reconhecer
o uso que deve fazer do seu próprio conhecimento.
Platão

Resumo

Neste trabalho nós abordamos alguns dos principais aspectos relacionados a codificação espaço-temporal e as ferramentas algébricas envolvidas na projeção de códigos baseados em álgebras de divisão cíclica. Apresentaremos também a construção do *Código de Ouro* ([9], [10]), que é um código espaço-temporal perfeito.

Palavras-chave: Código de Ouro, álgebras de divisão, reticulados algébricos, códigos perfeitos.

Abstract

In this work we discuss some main aspects related to space-time coding and algebraic tools involved in the design of codes based on cyclic division algebras. We also present the construction of the Golden Code ([9], [10]), which is a perfect space-time code.

Keywords: Golden Code, division algebras, algebraic lattice, perfect code.

Sumário

1 Introdução

Desde as primeiras transmissões de telégrafo, a transmissão de dados por meios elétricos tem revolucionado o modo com o qual as pessoas se comunicam e como a sociedade lida com a informação. Nos dias atuais, é inegável o fato de que a rotina do dia-a-dia se torna cada vez mais dependente dos meios de comunicação e demanda deles uma taxa de transmissão de dados cada vez mais alta. Desde os rádios comunicadores e passando pelo advento do telefone celular, as transmissões de dados sem fio tem ganhado importância significativa, e garantir a confiabilidade de sinal é um dos desafios de quem transmite esse tipo de sinal.

Ultimamente, além de apenas transmitir sinais de ligações telefônicas, novos tipos de dados passaram a ser transmitidos por esses aparelhos como músicas, fotos e etc, o que demanda uma rede que além alta qualidade de sinal tenha uma velocidade alta também na transmissão desses dados. Quando levamos em consideração redes 3G, 3G+ ou 4G, as taxas de transmissão são na ordem de Gigabits por segundo e conseguir aliar confiabilidade de sinal à tal velocidade é uma tarefa complexa.

Transmitir dados pelo meio atmosférico envolve muitos problemas inerentes a esse meio, como diferença de temperatura entre camadas da atmosfera, fenômenos meteorológicos, bloqueios causados por construções, pessoas, animais e outros objetos que estejam no caminho de propagação do sinal e fazem com que ele se enfraqueça, além da perda natural de energia que ocorre durante a propagação da onda. Para obter um bom resultado, uma opção seria utilizar uma faixa de freqüência grande, mas como as faixas de freqüências são escassas e caras, essa opção não é viável. Um tipo de sistema que tem sido bastante utilizado e visto como muito promissor é o MIMO - Multiple Input Multiple Output - que consiste no uso de múltiplas antenas para envio e recebimento de sinal. Os sistemas de comunicação MIMO estão sendo amplamente explorados principalmente por fornecer ganhos na transmissão de sinal.

Os problemas que envolvem a transmissão de um sinal sem fio aparecem independentemente do sistema utilizado pois são próprios do meio. Os efeitos nocivos do ambiente são referentes a desvanecimentos de larga escala e pequena escala. Desvanecimentos de larga escala estão associados à perda da qualidade do sinal devido à perda de potência do sinal conforme esse se propaga e à obstáculos que esse sinal pode enfrentar ao longo do percurso como edifícios, árvores, outras antenas, etc, ou seja, atuam na ordem de

vários comprimentos de onda do sinal. Os desvanecimentos de pequena escala são os que atuam na ordem de um comprimento de onda do sinal e se dão pelo fato de que o mesmo sinal pode chegar ao receptor por percursos diferentes, com fases diferentes e amplitudes diferentes. A sobreposição desses sinais é chamada de componente de multipercuso. Os multipercursos geram variações rápidas na amplitude do sinal recebido, uma vez que os sinais que chegam simultaneamente ao receptor combinam-se construtiva e/ou destrutivamente. Uma maneira de aumentar a confiabilidade do sinal é enviar o mesmo sinal através de múltiplas antenas, ou seja, usar a redundância como forma de aumentar a probabilidade de que pelo menos um dos sinais enviados chegue ao receptor sem desvanecimento ou interferência.

Se considerarmos que existem n_t antenas transmissoras e n_r antenas receptoras, haveria $n_t \cdot n_r$ ligações entre o transmissor e o receptor. Esse ganho obtido é chamado de ganho de diversidade e, neste caso, diz-se que há uma proteção de ordem $n_t \cdot n_r$ contra desvanecimentos do sinal, ou seja, as chances de pelo menos um sinal transmitido chegar a um receptor com qualidade é aumentada. A ordem do ganho de diversidade é definida como sendo o número de ligações independentes entre receptores e transmissores, sendo que são consideradas ligações independentes aquelas que não são redundantes, ou seja, não transmitem o mesmo sinal. Esse método, apesar de garantir tal aumento da qualidade do sinal, não otimiza a velocidade de transmissão da informação pois várias antenas enviam o mesmo sinal ao mesmo tempo, isto é, a informação demora mais para ser transmitida por completo do que demoraria se cada ligação transmitisse um sinal diferente. Por outro lado, se a informação for dividida em pequenos blocos e cada antena do sistema transmitir um desses blocos, todas as ligações entre transmissores e receptores tornam-se independentes e a velocidade de transmissão de dados aumenta muito, mas a probabilidade de que alguns sinais sejam perdidos ou incorretamente interpretados por um receptor devido à vários fatores presentes no meio de propagação é alta. Esse ganho obtido na velocidade de transmissão devido à independência das ligações é chamado de ganho de multiplexagem. O ganho de multiplexagem depende diretamente do número de antenas transmissoras do sistema já que quanto mais antenas, em mais blocos independentes a informação pode ser dividida e conseqüentemente mais rápido a informação será transmitida. Para maximizar os ganhos tanto de diversidade quanto de multiplexação foi introduzido o uso dos códigos espaço-temporais. Dessa forma, as antenas transmitem a mesma informação com uma pequena diferença de tempo entre as transmissões, de forma que haja redundância, garantindo a qualidade de sinal, mas que as ligações sejam independentes, aumentando a velocidade de transmissão. Dentre os tipos de codificação espaço-temporal destacam-se os códigos de bloco espaço-temporais (STBC) por sua facilidade de codificação/decodificação.

O objetivo deste trabalho é construir o Código de Ouro, que é um código que satisfaz todas as condições mencionadas acima. Uma álgebra de divisão é um objeto

algébrico que fornece naturalmente um conjunto linear de matrizes inversíveis e assim, o critério do posto é satisfeito. Dessa forma, organizamos o restante do nosso trabalho conforme delineamos na sequência.

No Capítulo 2, apresentamos o modelo do sistema MIMO, juntamente com alguns conceitos de teoria dos números algébricos que serviram de ferramenta para o desenvolvimento dos demais capítulos.

No Capítulo 3, apresentamos a teoria de reticulados algébricos.

No Capítulo 4, apresentamos as álgebras cíclicas e exploramos a sua relação com a construção de códigos espaço-tempo.

No Capítulo 5, apresentamos a construção do Código de Ouro que é um STBC perfeito.

Além disso, o trabalho visa mostrar uma aplicação prática da teoria dos números algébricos, teoria dos reticulados e álgebras cíclicas tratando didaticamente dos temas e possibilitando que pesquisas futuras se beneficiem das informações contidas aqui, indo de encontro com os ideais de formação de um matemático do Programa de Pós-Graduação em Matemática Universitária da UNESP - Rio Claro.

2 O Modelo do Sistema MIMO

É necessário criar um modelo adequado de canal MIMO que abranja as principais propriedades do canal sem fio. Neste sentido, descreveremos critérios para que a probabilidade de erro seja minimizada. Para maiores detalhes sobre a teoria abordada aqui, podem ser consultadas as referências [1], [3] e [9].

2.1 O modelo do sistema MIMO

Uma única antena transmissora durante um único intervalo de tempo envia um sinal que pode ser interpretado como um um número complexo $x \in \mathbb{C}$. Durante o percurso do sinal até a antena receptora, ele sofrerá alguma distorção que pode ser modelada pela multiplicação de x por um número complexo h chamado *coeficiente de desvanecimento*. Além disso, a antena receptora captará algum ruído presente no meio de propagação que pode ser modelado pela adição de um número complexo z. Assim, o sinal recebido será $y = hx + z$.

Supondo agora que haja n_t antenas transmitindo simultaneamente um sinal para uma única antena receptora. Seja $x_j \in \mathbb{C}$ o sinal enviado pela j-ésima antena ($1 \leq j \leq n_t$). Como elas transmitem simultaneamente, cada uma dessas antenas tem participação no sinal detectado no receptor. O sinal recebido $y \in \mathbb{C}$ será portanto alguma combinação linear de tais números complexos, mais um certo ruído:

$$y = h_1x_1 + h_2x_2 + ... + h_{n_t}x_{n_t} + z$$

onde $h_j \in \mathbb{C}$ é o coeficiente de desvanecimento entre a j-ésima antena transmissora e o receptor.

Aumentando agora o número de antenas receptoras para n_r, teremos os coeficientes de desvanecimento h_{ij} ($1 \leq i \leq n_r, 1 \leq j \leq n_t$), cada um correspondendo à transmissão entre a j-ésima antena transmissora e a i-ésima antena receptora; também haverá ruído captado por cada receptor, que será representado por $z_1, z_2, ..., z_{n_r} \in \mathbb{C}$. Para cada antena receptora $i \in \{1, \cdots, n_r\}$, teremos a equação

$$y_i = h_{i1}x_1 + h_{i2}x_2 + ... + h_{in_t}x_{n_t} + z_i.$$

Podemos, então, considerar o canal como um todo expressando as n_r equações através de uma equação matricial:

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{n_r} \end{pmatrix} = \begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1n_t} \\ h_{21} & h_{22} & \cdots & h_{2n_t} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n_r1} & h_{n_r2} & \cdots & h_{n_rn_t} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n_t} \end{pmatrix} + \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_{n_r} \end{pmatrix}$$

que pode ser escrita na forma abreviada

$$\vec{y} = H\vec{x} + \vec{z} \, .$$

O sistema MIMO pode ser usado para combater o desvanecimento usando técnicas de diversidade, isto é, diferentes réplicas do sinal são transmitidas redundantemente através de canais que sofrem desvanecimentos independentes, existindo desta forma uma alta probabilidade que pelo menos um dos canais não seja afetado pelo desvanecimento.

Visando fornecer diversidade, vários tipos de esquemas têm sido sugeridos. Um deles são os códigos de bloco espaço-tempo (STBC), os quais fornecem redundância em espaço, através do uso de múltiplas antenas, e redundância no tempo, através da codificação de canal.

O critério para modelar códigos espaço-tempo depende do tipo de receptor que é considerado. Duas principais classes de receptores tem sido consideradas na literatura: *coerente e não-coerente*. No primeiro caso, considerado neste, o receptor recupera a informação exata sobre o estado do canal (isto é também conhecido como perfeito estado de informação do canal (CSI). Na prática isto pode ser obtido introduzindo algum símbolo guia que permite uma estimativa precisa do canal, assim, podemos assumir que a matriz do canal H é conhecida no receptor. Para o caso não-coerente podem ser consultadas as referências [11] e [12].

Até agora aumentamos a confiabilidade e/ou taxa de transmissão adicionando antenas, proporcionando mais caminhos para levar a informação do transmissor ao receptor, podemos chamar isso de *diversidade espacial*. Outro ganho importante gerado pelo uso de códigos espaço-tempo pode ser chamado de *diversidade temporal*: como num código de bloco comum, consideremos que cada antena transmissora (sincronizada com as outras) envie uma *string* de T números complexos. Vamos tratar o tempo como discreto e um número complexo será transmitido durante cada intervalo de tempo. Portanto para cada tempo k no bloco $\{1, ..., T\}$, a j-ésima antena transmissora ($1 \leq j \leq n_t$) envia um símbolo $x_{jk} \in \mathbb{C}$; analogamente, cada tempo k, a i-ésima antena receptora ($1 \leq i \leq n_r$) captará um símbolo y_{ik}.

Podemos assumir que o canal é *quase-estático*; isto é, os coeficientes de desvanecimento h_j permanecem constantes durante o intervalo de tempo T que um bloco de informação leva para ser transmitido.

Se $\vec{y_k}$ denota o vetor $(y_{1k}, y_{2k}, ..., y_{n_r k})^T$ de símbolos recebidos no tempo k e analogamente $\vec{x_k} = (x_{1k}, x_{2k}, ..., x_{n_t k})^T$ denota o vetor de símbolos transmitido no tempo k, podemos escrever

$$\vec{y_k} = H\vec{x_k} + \vec{z_k},$$

onde $\vec{z_k}$ é o vetor de ruído no tempo k. Podemos então representar essas T equações numa única equação matricial

$$(\vec{y_1}\,\vec{y_2}\,\cdots\,\vec{y_T}) = H(\vec{x_1}\,\vec{x_2}\,\cdots\,\vec{x_T}) + (\vec{z_1}\,\vec{z_2}\,\cdots\,\vec{z_T});$$

que pode ser abreviada para

$$Y = H \cdot X + Z.$$

Lembrando que Y é uma matriz $n_r \times T$ na qual y_{ik} representa o símbolo recebido pela antena i no tempo k; a matriz do canal H tem dimensão $n_r \times n_t$ como antes; X é uma matriz $n_t \times T$ em que x_{jk} representa o símbolo transmitido pela antena j no tempo k; e a matriz de ruído Z tem dimensão $n_r \times T$. Neste trabalho, focaremos o caso onde $n_t = n_r = T = n$ e então podemos codificar n^2 símbolos de informação.

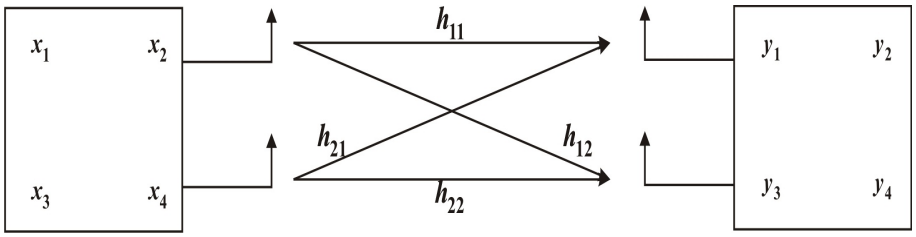


Figura 2.1: Exemplo de Canal MIMO 2×2

X : matriz de sinal transmitido $n_t \times T$
Y : matriz de sinal recebido $n_r \times T$
H : matriz de canal $n_r \times n_t$
Z : matriz ruído Gaussiana complexa $n_r \times T$

$$Y = HX + Z$$

Definição 2.1. *Um STBC é um conjunto finito $\mathcal{C}$ de $n_t \times T$ matrizes complexas X e é linear se*

$$\forall\, X,\, X' \in \mathcal{C} \Rightarrow X \pm X' \in \mathcal{C}.$$

2.2 Critérios para modelar códigos espaço-tempo

Sob a suposição de perfeito CSI, a decodificação por *máxima verossimilhança* (ML) corresponde a escolher uma palavra-código X que minimiza:

$$\min_{X \in \mathcal{C}} ||Y - HX||^2.$$

Uma estimativa da probabilidade de erro pode ser obtida usando a união limitada

$$P(e) \leq \frac{1}{|\mathcal{C}|} \sum_{x \in \mathcal{C}} \sum_{\hat{X} \neq X} P(X \longrightarrow \hat{X}) \tag{2.1}$$

onde $P(X \longrightarrow \hat{X})$ é a *probabilidade de erro ponto a ponto*, isto é, a probabilidade que, quando uma palavra-código X é transmitida, o receptor ML decide erroneamente em favor de outra palavra-código $\hat{X}$, assumindo que somente X e $\hat{X}$ estão no código.

No caso de desvanecimento Rayleigh independente ($h_{ij} \sim N_c(0,1)$), podemos escrever

$$P(X \longrightarrow \hat{X}) \leq \det \left[I_{n_t} + \frac{(X - \hat{X})(X - \hat{X})^\dagger}{4N_0} \right]^{-n_r}, \tag{2.2}$$

onde $\dagger$ denota a matriz transposta conjugada.

Denotando por r o posto da matriz diferença da palavra-código, se $r = n_t$ para todos os pares $(X, \hat{X})$, dizemos que o código tem *posto total*. Se denotarmos por λ_j, $j = 1, \cdots, r$ os autovalores não nulos da *matriz distância da palavra-código*

$$A = (X - \hat{X})(X - \hat{X})^\dagger \tag{2.3}$$

podemos reescrever (2.3) como

$$P(X \longrightarrow \hat{X}) \leq \prod_{j=1}^{r} \left(1 + \frac{\lambda_j}{4N_0} \right)^{-n_r}. \tag{2.4}$$

Para alta relação sinal-ruído (N_0 pequeno), temos

$$P(X \longrightarrow \hat{X}) \leq \delta^{-n_r} \left(\frac{1}{4N_0} \right)^{-rn_r}, \tag{2.5}$$

onde $\delta = \prod_{j=1}^{r} \lambda_j$. Então podemos escrever

$$P(X \longrightarrow \hat{X}) \leq \left(\frac{\delta^{1/r}}{4N_0} \right)^{-rn_r}. \tag{2.6}$$

No caso de códigos de posto máximo ($r = n_t$), temos $\delta = \det(A) = \prod_{j=1}^{n_t} \lambda_j \neq 0$ para todo A e dizemos que o código tem *diversidade total*. Isto significa que podemos explorar todos os $n_t n_r$ canais independentes disponíveis no sistema MIMO.

No caso de códigos com diversidade total, o termo dominante na união limitada (2.1) é dado pelo então chamado *determinante mínimo* do código,

$$\delta_{min} = \min_{X \neq \hat{X}} \det(A). \tag{2.7}$$

O termo $(\delta_{min})^{1/n_t}$ é conhecido como *ganho de codificação* [13].

No caso de códigos lineares a soma ou a diferença de qualquer par de palavras-código é uma palavra-código, portanto a união limitada reduz a

$$P(e) \leq \frac{1}{|\mathcal{C}|} \sum_{X \neq 0} P(0 \longrightarrow X) \tag{2.8}$$

e temos

$$\delta_{min} = \min_{X \neq 0_{n_t \times T}} \det(XX^{\dagger}). \tag{2.9}$$

Consequentemente, para minimizar a probabilidade de erro é necessário considerar dois critérios.

1. **O critério do posto:** de fato, para atingir a diversidade máxima $n_t n_r$, a matriz $(X - \hat{X})$ deve ter posto total para qualquer par de palavras-código X e $\hat{X}$. Códigos que atingem a diversidade máxima são chamados *totalmente diversos*.

2. **O critério do determinante**: se a diversidade de $n_t n_r$ é atingida, então o determinante mínimo de A tomado sobre todos os pares de palavras-código distintas deve ser maximizado.

Além disso, para melhorar o desempenho de códigos espaço-tempo, exigimos que as seguintes propriedades sejam satisfeitas:

- **Determinante não-nulo.** Dizemos que o código tem um *determinante não-nulo* se, antes da normalização SNR, existe um limitante inferior sobre o determinante mínimo que não depende do tamanho da constelação.

- **Forma.** Palavras-código e sinais podem ser representados por meio de esquemas compostos por pontos e vértices de grafos em espaços de curvatura constante. Ao conjunto de tais pontos chamamos indistintamente de *constelações de sinais*. Para otimizar a eficiência de energia dos códigos, uma forma sobre a constelação de sinais é introduzida. As constelações QAM ou HEX (estas podem ser vistas como subconjuntos de $\mathbb{Z}[i]$ ou $\mathbb{Z}[j]$, respectivamente, onde j é uma raiz terceira primitiva da unidade), ao serem enviadas são normalizadas de acordo com a capacidade do transmissor. Entretanto, como usamos STBCs lineares, o que é transmitido sobre cada camada é uma combinação linear de símbolos de informação, que podem mudar a energia do sinal. Cada camada pode ser escrita

como Mv, onde v é o vetor contendo os símbolos de informação QAM ou HEX, enquanto M é uma matriz que decodifica os símbolos dentro de cada camada. De modo a obter códigos com energia eficiente, exigimos que a matriz M seja unitária. Referimos a este tipo de forma de constelação como *forma cúbica*, pois uma matriz unitária aplicada sobre um vetor contendo valores discretos pode ser interpretada como pontos geradores do reticulado. Por exemplo, se usarmos símbolos QAM, obtemos o reticulado (cúbico) $\mathbb{Z}^n$.

- **Uniformidade média da energia transmitida por antena.** A i-ésima antena do sistema transmitirá um sinal x_{ik} para o tempo k. Nós exigimos que a energia de cada entrada da palavra-código seja constante, assim, temos uma repartição equilibrada da energia para o transmissor.

2.3 Teoria dos números algébricos

Definição 2.2. *Sejam L e K dois corpos. Dizemos que L é uma extensão de corpos se $K \subseteq L$, ou seja, K é subcorpo de L.*

Notação: L/K.

Definição 2.3. *Seja V um espaço vetorial sobre K. Se V admite uma base finita então chamamos de* ***dimensão*** *de V o número de elementos de tal base. Caso contrário, dizemos que a dimensão de V é infinita.*

Definição 2.4. *Seja L/K uma extensão de corpos. A dimensão do espaço vetorial de L sobre K é chamada* **grau da extensão** *de L sobre K e é denotada por $[L : K]$. Se $[L : K]$ é finito, dizemos que a extensão L/K é uma extensão finita.*

Notação: $[L : K] < \infty$.

Definição 2.5. *Uma extensão finita sobre o corpo dos números racionais, $\mathbb{Q}$, é chamada de* **corpo de números**.

Observação 2.1. Os corpos de números $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ e $\mathbb{Q}(j) = \{a + bj \mid a, b \in \mathbb{Q}\}$, onde j é a raiz terceira primitiva da unidade , isto é, $j^3 = 1$ e $j^n \neq 1, 1 \leq n \leq 2$) são de particular interesse. De fato, restringindo a e b em $\mathbb{Z}$ podemos obter o conjunto dos inteiros Gaussianos $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ e o conjunto dos inteiros de Eiseinstein $\mathbb{Z}[j] = \{a + bj \mid a, b \in \mathbb{Z}\}$.

Teorema 2.1. *(Teorema da multiplicatividade dos graus)*

Sejam K, M e L corpos tais que $K \subseteq M \subseteq L$ e $[L : K] < \infty$. Então, $[L : K] = [L : M] \cdot [M : K]$

Suponha $[L : M] = m$ e $[M : K] = n$. Sejam $B_1 = \{\alpha_1, \ldots, \alpha_m\}$ uma base de L sobre M e $B_2 = \{\beta_1, \ldots, \beta_n\}$ uma base de M sobre K.

Afirmação: $B = \{\alpha_i\beta_j, i = 1, \ldots, m \text{ e } j = 1, \ldots, n\}$ é uma base de L/K.

1. $[B] = L$.

   De fato: $\alpha \in L \Rightarrow \exists\, a_1, a_2, \cdots, a_m \in M$ tais que $\alpha = \sum_{i=1}^{m} a_i \alpha_i$.

   $a_i \in M \Rightarrow \exists\, b_{i1}, b_{i2}, \cdots, b_{in} \in K$ tais que $a_i = \sum_{j=1}^{n} b_{ij}\beta_j$. Logo, $\alpha = \sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}\alpha_i\beta_j$.

2. B é L.I.sobre K.

   De fato, $\sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}\alpha_i\beta_j = 0 \Rightarrow \sum_{i=1}^{m}\left(\sum_{j=1}^{n} b_{ij}\beta_j\right)\alpha_i$=0.

   Como B_1 é L.I. , temos $\sum_{j=1}^{n} b_{ij}\beta_j = 0$. Como B_2 é L.I. , temos $b_{ij} = 0, \forall i, j$.

   Portanto B é uma base de L/K com mn elementos. Pela Definição (2.3), $[L : K] = mn = [L : M].[M : K]$.

Exemplo 2.1. Queremos encontrar $\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\right]$.

Afirmação I : $\{1, \sqrt{2}\}$ é uma base de $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$.

De fato,

1. $\{1, \sqrt{2}\}$ gera $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$.

   Como $\mathbb{Q}(\sqrt{2}) = \{x \mid x = \alpha + \beta\sqrt{2}, \alpha, \beta \in \mathbb{Q}\}$, então $\forall x \in \mathbb{Q}(\sqrt{2}), x = \alpha.1 + \beta\sqrt{2}$, α, $\beta \in \mathbb{Q}$, ou seja, x é combinação linear de $\{1, \sqrt{2}\}$.

2. $\{1, \sqrt{2}\}$ é linearmente independente.

   Suponha que $\alpha.1 + \beta\sqrt{2} = 0, \alpha, \beta, \in \mathbb{Q}$. Se $\beta \neq 0$, então $\sqrt{2} = \dfrac{-\alpha}{\beta}$, o que é absurdo pois $\sqrt{2}$ é irracional. Portanto, $\beta = 0$ e daí temos que $\alpha.1 + 0.\sqrt{2} = 0 \Rightarrow \alpha = 0$. Dessa forma, $\{1, \sqrt{2}\}$ é uma base de $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$.

   Logo $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Afirmação II : $\{1, \sqrt{3}\}$ é uma base de $\mathbb{Q}(\sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$

1. De fato, $\{1, \sqrt{3}\}$ gera $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$.

   Como $\mathbb{Q}(\sqrt{3}, \sqrt{2}) = \{x \mid x = \alpha + \beta\sqrt{3}, \alpha, \beta \in \mathbb{Q}(\sqrt{2})\}$, então $\forall x \in \mathbb{Q}(\sqrt{3}, \sqrt{2}), x = \alpha.1 + \beta\sqrt{3}, \alpha, \beta \in \mathbb{Q}(\sqrt{2})$, ou seja, x é combinação linear de $\{1, \sqrt{3}\}$.

2. $\{1, \sqrt{3}\}$ é linearmente independente.

   Suponha que $\alpha.1 + \beta\sqrt{3} = 0, \alpha, \beta, \in \mathbb{Q}(\sqrt{2})$. Assim podemos reescrever a igualdade como

$$(p + q\sqrt{2}) + (r + s\sqrt{2})\sqrt{3} = 0,\ p, q, r \text{ e } s \in \mathbb{Q}.$$

Se $\beta = (r + s\sqrt{2}) \neq 0$, então $\sqrt{3} = \dfrac{-(p+q\sqrt{2})}{r+s\sqrt{2}} = \dfrac{-(p+q\sqrt{2})}{r+s\sqrt{2}}.\dfrac{r-s\sqrt{2}}{r-s\sqrt{2}} = \dfrac{-(pr-ps\sqrt{2}+qr\sqrt{2}-2qs)}{r^2-2s} = \dfrac{-pr+2qs+(ps-qr)\sqrt{2}}{r^2-2s} = \dfrac{-pr+2qs}{r^2-2s} + \dfrac{(ps-qr)\sqrt{2}}{r^2-2s} = a + b\sqrt{2}, a, b \in \mathbb{Q}$. Assim, temos que

$$\begin{aligned} (\sqrt{3})^2 &= (a+b\sqrt{2})^2 \\ 3 &= a^2 + 2ab\sqrt{2} + 2b^2 \\ 3 - a^2 - 2b^2 &= 2ab\sqrt{2} \\ \frac{3-a^2-2b^2}{2ab} &= \sqrt{2}, \end{aligned} \tag{2.10}$$

o que é absurdo pois $\sqrt{2}$ é irracional.

Portanto, $r+s\sqrt{2} = \beta = 0$ e daí temos que $p+q\sqrt{2}+0.\sqrt{3} = 0 \Rightarrow p+q\sqrt{2} = \alpha = 0$.

Dessa forma, $\{1, \sqrt{3}\}$ é uma base de $\mathbb{Q}(\sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$.

Logo $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$.

Pelo Teorema da multiplicatividade dos graus,

$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})].[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.2 = 4$

e $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ é uma base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}$.

Definição 2.6. *Seja L/K uma extensão de corpos e $\alpha \in L$. Dizemos que α é **algébrico** sobre K se existe $f \in K[x]^* = K[x] \setminus 0$ ($K[x]$: conjunto dos polinômios sobre K na indeterminada x) tal que $f(\alpha) = 0$. Caso não exista f com tais condições, dizemos que α é **transcendente**.*

Observação 2.2. Se $K = \mathbb{Q}$, dizemos simplesmente que α é **algébrico** ou **transcendente**.

Exemplo 2.2. É fácil dar exemplos de números algébricos sobre $\mathbb{Q}$:

- todos os números racionais
- $\sqrt{2}$
- $\sqrt{2} + \sqrt{5}$
- i.

No entanto, é difícil dar exemplos de números transcendentes. Em 1873, Hermite demonstrou que o número

$$e = \lim_{n\to\infty} \left(1 + \frac{1}{n+1}\right)^{n+1}$$

é transcendente e em 1882 Lindemann demonstrou que π é transcendente [14].

Definição 2.7. *Uma extensão L sobre K é* ***algébrica*** *se todo $\alpha \in L$ é algébrico sobre K.*

Exemplo 2.3. Vamos verificar que a extensão $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$ é algébrica.

$\alpha \in \mathbb{Q}(\sqrt{2}) \Rightarrow \alpha = a + b\sqrt{2}, a, b \in \mathbb{Q}$.

$x = a + b\sqrt{2} \Rightarrow (x-a)^2 = 2b \Rightarrow x^2 - 2ax + a^2 - 2b = 0$.

Logo, α é raiz de $x^2 - 2ax + a^2 - 2b \in \mathbb{Q}[x]$ e, dessa forma, α é algébrico sobre $\mathbb{Q}$ e, portanto, a extensão $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ é algébrica.

Definição 2.8. *Dizemos que α é* ***inteiro algébrico*** *se existe $f(x) \in \mathbb{Z}[x]^* = \mathbb{Z}[x] \setminus 0$, mônico, tal que $f(\alpha) = 0$. O conjunto $\mathcal{O}_K = \{\alpha \in K \mid \alpha$ é inteiro algébrico $\}$ é um anel chamado* ***anel dos inteiros de K****.*

Exemplo 2.4. O elemento $\alpha = \sqrt{2} + \sqrt{3}$ é inteiro sobre $\mathbb{Z}$, pois é raiz do seguinte polinômio $x^4 - 10x^2 + 1 \in \mathbb{Z}[x]$.

Definição 2.9. *Seja L/K extensão de corpos de α algébrico sobre K. O polinômio $p(x) \in K[x]^*$, mônico e de menor grau tal que $p(\alpha) = 0$ é chamado* ***polinômio minimal*** *de α sobre K. Notação : $p = irr_\alpha \mid K$.*

Definição 2.10. *Seja $f(x) \in K[x]$ tal que $\partial f \geq 1$. Dizemos que $f(x)$ é um* ***polinômio irredutível*** *sobre K se toda vez que $f(x) = g(x).h(x), f(x), g(x) \in K[x]$, então $f(x) = a$ ou $h(x) = b$, $a, b \in K$, a, b constantes. Se $f(x)$ não é irredutível, dizemos que é* ***redutível*** *sobre K.*

Teorema 2.2. *(Critério de Eisenstein)*

Seja $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Se existir $p \in \mathbb{Z}$, p primo, tal que:

- $p \mid a_0, ..., a_{n-1}$
- $p \nmid a_n$
- $p^2 \nmid a_0$

Então $f(x)$ é irredutível em $\mathbb{Z}[x]$.

Lema 2.1. *(Lema de Gauss [15], p. 44) Seja $f(x) \in \mathbb{Z}[x]$ tal que $f(x)$ é irredutível sobre $\mathbb{Z}$. Então $f(x)$ é irredutível sobre $\mathbb{Q}$.*

Observação 2.3. Seja $p(x) \in K[x]^*$ e $\alpha \in K$ tal que $p(x)$ é o polinômio minimal de α sobre K . Então $p(x)$ é irredutível sobre K.

De fato: Suponha $p(x) = f(x).g(x)$, $f(x), g(x) \in K[x]^*$ e $\partial f(x) \geq 1$ e $\partial g(x) \geq 1$ Então, $p(\alpha) = 0 \Rightarrow f(\alpha).g(\alpha) = 0 \Rightarrow f(\alpha) = 0$ ou $g(\alpha) = 0$, o que contradiz a minimalidade do grau de $p(x)$. Logo, $p(x)$ é irredutível sobre K.

Exemplo 2.5. Seja $\alpha = \sqrt{2} + \sqrt{3}$ e $K = \mathbb{Q}$.

$\alpha = \sqrt{2}+\sqrt{3} \Rightarrow (\alpha-\sqrt{2})^2 = (\sqrt{3})^2 \Rightarrow \alpha^2-2\alpha\sqrt{2}+2 = 3 \Rightarrow (\alpha^2-1)^2 = (2\alpha\sqrt{2})^2 \Rightarrow (\alpha^2-1)^2 = 8\alpha^2 \Rightarrow \alpha^4 - 10\alpha^2 + 1 = 0$. Assim, $p(x) = x^4 - 10x^2 + 1 = 0$

Vamos verificar se $p(x)$ é irredutível sobre $\mathbb{Z}$.

Suponha que haja fator de grau 1, $(x-a)$, tal que $p = (x-a)(a_3x^3+a_2x^2+a_1x+a_0)$, $a_3, a_2, a_1, a_0 \in \mathbb{Z}$.

Aplicando a distributiva, temos que o termo constante $a.a_0 = 1$. Como $a \in \mathbb{Z}$ então $a = \pm 1$. Logo ± 1 seria raiz de $p(x)$, mas $p(\pm 1) \neq 0$, o que significa que não há fator de grau 1, e por consequência nem de grau 3, para $p(x)$.

Por outro lado, $p(x) = (x^2 - (-5 + 2\sqrt{6}))(x^2 + (5 + 2\sqrt{6}))$ e temos que cada fator não tem raiz em $\mathbb{Z}$ e, assim, $p(x)$ não possui fatores de grau 2 com raízes em $\mathbb{Z}$.

Dessa forma, $p(x)$ é irredutível sobre $\mathbb{Z}$ e, pelo Lema de Gauss, é irredutível sobre $\mathbb{Q}$.

Portanto, $p = irr_\alpha \mid \mathbb{Q}$.

Exemplo 2.6. Seja $\alpha = i \in \mathbb{C}$ e $K = \mathbb{R}$.

$\alpha = i \Rightarrow \alpha^2 = -1 \Rightarrow \alpha^2 + 1 = 0$.

Assim, seja $p(x) = x^2 + 1$. Vamos verificar se $p(x)$ é irredutível sobre $\mathbb{R}$.

Como $p(x) = (x + i)(x - i)$, temos que cada fator não tem raiz em $\mathbb{R}$ e assim, $p(x)$ é irredutível sobre $\mathbb{R}$. Portanto, $p(x) = irr_\alpha \mid \mathbb{R}$.

Teorema 2.3. *Seja L/K extensão de corpos e $\alpha \in L$ algébrico sobre K, com $p(x) = irr_\alpha \mid K$ tal que $\partial p = n$. Então $\{1, a, ..., a^{n-1}\}$ é base de $K(\alpha)$ sobre K e $[K(\alpha) : K] = \partial p = n$.*

Seja $K[\alpha] = K(\alpha) = \{f(\alpha) \mid f(x) \in K[x]\}$.

$f(x), p(x) \in K[x] \Rightarrow$existem $q(x), r(x) \in K[x]$ tais que $f(x) = p(x).q(x) + r(x)$ com $r(x) = 0$ ou $\partial r(x) < \partial p(x)$. Logo, existem $a_0, a_1, \cdots, a_{n-1} \in K$ tais que $r(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$.

Assim, se $f(\alpha) = p(\alpha)q(\alpha) + r(\alpha)$.

Como $p(\alpha) = 0$, $f(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \Rightarrow K[\alpha] = [1, a, \cdots, a^{n-1}]$.

Vamos verificar se $\{1, a, \cdots, a^{n-1}\}$ é linearmente independente.

De fato, $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0 \Rightarrow f(\alpha) = 0$, para $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$.

Pela minimalidade do grau de $p(x)$, $f(x) = 0$, ou seja, $a_0 = a_1 = \cdots = a_{n-1} = 0$. Logo, $\{1, a, ..., a^{n-1}\}$ é base de $K(\alpha)$ sobre K e $[K(\alpha) : K] = n$.

Exemplo 2.7. Seja $\alpha = \sqrt[3]{2}, p = x^3 - 2$. Aplicando o critério de Eiseinstein em $p(x)$ com o primo $p = 2$ temos que $p(x) = irr_\alpha \mid \mathbb{Q}$.

Assim, pelo Teorema (2.3), $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ e $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ é base de $\mathbb{Q}(\sqrt[3]{2})$ sobre $\mathbb{Q}$.

Teorema 2.4. *(Teorema do elemento primitivo)*

Se K é um corpo de números, então $K = \mathbb{Q}(\alpha)$ para algum inteiro algébrico α que é chamado ***elemento primitivo*** *de K.*

Exemplo 2.8. Considere o corpo de números $\mathbb{Q}(i,\sqrt{5})$. Mostraremos que $\mathbb{Q}(i,\sqrt{5}) = \mathbb{Q}(i+\sqrt{5})$.

É claro que $\mathbb{Q}(i+\sqrt{5}) \subseteq \mathbb{Q}(i,\sqrt{5})$.

Agora, $(1+\sqrt{5})^3 = 14i + 2\sqrt{5} \in \mathbb{Q}(i+\sqrt{5})$.

Ainda, $(1+\sqrt{5})^3 - 2(i+\sqrt{5}) = 12i \in \mathbb{Q}(i+\sqrt{5})$ e, portanto, $i \in \mathbb{Q}(i+\sqrt{5})$ e por consequência $\sqrt{5}$ também. Pelo Teorema (2.3), uma base de $\mathbb{Q}(i,\sqrt{5})/\mathbb{Q}$ pode ser dada por $\{1, i+\sqrt{5}, (i+\sqrt{5})^2, (i+\sqrt{5})^3\}$

Vejamos agora como um corpo de números K pode ser representado, dizemos na verdade **mergulhado** em $\mathbb{C}$.

Lembremos que dados A e B anéis, um **homomorfismo de anéis** é uma função $\varphi : A \to B$ que satisfaz, para todo $a, b \in A$:

- $\varphi(a+b) = \varphi(a) + \varphi(b)$
- $\varphi(a.b) = \varphi(a).\varphi(b)$
- $\varphi(1) = 1$

Definição 2.11. *Sejam L/K e $K/\mathbb{Q}$ extensões de corpos.*

Dizemos que $\varphi : K \to L$ é um $\mathbb{Q}$**-homomorfismo** *se φ satisfaz $\varphi(a) = a, \forall a \in \mathbb{Q}$, ou seja, fixa $\mathbb{Q}$.*

Definição 2.12. *Um $\mathbb{Q}$-homomorfismo de anéis $\varphi : K \to \mathbb{C}$ é chamado um* ***mergulho*** *de K em $\mathbb{C}$.*

Teorema 2.5. *([18] p. 33) Seja $K = \mathbb{Q}(\theta)$ um corpo de números e $[\mathbb{Q}(\theta) : \mathbb{Q}] = n$. Existem exatamente n mergulhos distintos de K em $\mathbb{C}$,*

$$\begin{array}{rccl} \sigma_i : & K & \to & \mathbb{C} \\ & \theta & \mapsto & \sigma_i(\theta) = \theta_i,\ i = 1, ..., n, \end{array}$$

onde θ_i são as raízes distintas do polinômio minimal de θ sobre $\mathbb{C}$.

Notemos que um dos σ_i, que denotamos por σ_1, é a função identidade, isto é, $\sigma_1(x) = x, \forall x \in K$.

Quando aplicamos o mergulho σ_i num elemento qualquer $x \in K$, $x = \sum_{k=1}^{n} a_k\theta^k, a_k \in \mathbb{Q}$, temos, pelas propriedades dos $\mathbb{Q}$-homomorfismos,

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

Exemplo 2.9. Considere o corpo $\mathbb{Q}(\sqrt[3]{2})$ e o polinômio minimal $p(x) = x^3 - 2$.

Como as raízes n-ésimas de um número complexo não nulo podem ser obtidas como o produto de uma de suas raízes particulares pelas raízes n-ésimas da unidade $1, \omega, ..., \omega^{n-1}$, onde $\omega = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$, temos que as raízes de $p(x)$ são

$\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$. De acordo com a obervação (2.1), para $n = 3$, temos que $w = j$. Logo,

$$(x^3 - 2) = (x - \sqrt[3]{2})(x - j\sqrt[3]{2})(x - j^2\sqrt[3]{2}).$$

Assim temos três mergulhos:

$$\begin{array}{rccc} \sigma_1(x): & \mathbb{Q}(\sqrt[3]{2}) & \longmapsto & \mathbb{C} \\ & \sqrt[3]{2} & \longrightarrow & \sqrt[3]{2} \end{array}$$

$$\begin{array}{rccc} \sigma_2(x): & \mathbb{Q}(\sqrt[3]{2}) & \longmapsto & \mathbb{C} \\ & \sqrt[3]{2} & \longrightarrow & j\sqrt[3]{2} \end{array}$$

$$\begin{array}{rccc} \sigma_3(x): & \mathbb{Q}(\sqrt[3]{2}) & \longmapsto & \mathbb{C} \\ & \sqrt[3]{2} & \longrightarrow & j^2\sqrt[3]{2} \end{array}$$

Definição 2.13. *Sejam K um corpo de números e $x \in K$.*

Os elementos $\sigma_1(x), \sigma_2(x), \cdots, \sigma_n(x)$ são chamados ***conjugados*** *de x e*

$$N(x) = \prod_{i=1}^{n} \sigma_i(x) \text{ é chamado de } \textbf{\textit{Norma}} \text{ de } x \text{ e}$$

$$Tr(x) = \sum_{i=1}^{n} \sigma_i(x) \text{ é chamado de } \textbf{\textit{Traço}} \text{ de } x.$$

Teorema 2.6. *([18] p. 38) Seja K corpo de números. Para todo $x \in K$, temos $N(x) \in \mathbb{Q}$ e $Tr(x) \in \mathbb{Q}$. Se $x \in \mathcal{O}_K$, temos $N(x) \in \mathbb{Z}$ e $Tr(x) \in \mathbb{Z}$.*

Definição 2.14. *Seja K um corpo de números algébrico de grau n sobre $\mathbb{Q}$ e $\mathcal{O}_K$ seu anel dos inteiros. Dizemos que $w_1, w_2, ..., w_n$ é uma* ***base integral*** *de K se $w_i \in K, \forall\, i,\ i = 1, ...n$ e $\mathcal{O}_K = \mathbb{Z}w_1 + \mathbb{Z}w_2 + ... + \mathbb{Z}w_n$.*

Exemplo 2.10. Seja $K = \mathbb{Q}(\sqrt{2})$ um corpo de números.

O polinômio minimal de $\sqrt{2}$ sobre $\mathbb{Q}$ é $x^2 - 2$ e suas raízes são $\theta_1 = \sqrt{2}$ e $\theta_2 = -\sqrt{2}$. Assim,

$$\sigma_1(\sqrt{2}) = \sqrt{2} \text{ e } \sigma_2(\sqrt{2}) = -\sqrt{2}.$$

Para $x \in \mathbb{Q}(\sqrt{2})$, temos $x = a + b\sqrt{2}$, $a, b \in \mathbb{Q}$.

$$\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2} \text{ e } \sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}$$

A norma de x é:

$$N(x) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 \in \mathbb{Q}.$$

Já o traço de x é:

$$N(x) = (a + b\sqrt{2}) + (a - b\sqrt{2}) = 2a \in \mathbb{Q}.$$

Para extensões do tipo L/K temos o seguinte teorema:

Teorema 2.7. *Seja L/K uma extensão de corpos. Para todo $x \in L$, temos $N_{L/K}(x) \in K$ e $Tr_{L/K}(x) \in K$. Se $x \in \mathcal{O}_L$ temos que $N_{L/K}(x) \in \mathcal{O}_K$ e $N_{L/K}(x) \in \mathcal{O}_K$.*

Definição 2.15. *Seja $\{w_1, w_2, ..., w_n\}$ uma base integral de K.*
*O **discriminante** de K é definido por*

$$d_K = det[\sigma_j(w_i)]^2, \;\; i, j = 1, 2, ..., n.$$

Teorema 2.8. *O discrimintante de um corpo de números pertece a $\mathbb{Z}$.*

Definição 2.16. *Um* **ideal** $\mathcal{I}$ *de um anel comutativo A é um subgrupo aditivo de A que é fechado em relação a multiplicação por A, isto é, $a\mathcal{I} \subseteq \mathcal{I}$ para todo $a \in A$.*

Entre todos os ideais de um anel, alguns deles tem a propriedade especial de serem gerados por somente um elemento. Estes serão de particular interesse neste trabalho.

Definição 2.17. *Um ideal $\mathcal{I}$ é principal se ele é da forma*

$$\mathcal{I} = \langle x \rangle A = \{xy, y \in A\}, \; x \in \mathcal{I}.$$

e podemos escrever $\mathcal{I} = \langle x \rangle$.

Exemplo 2.11. $n\mathbb{Z}$ é um ideal principal de $\mathbb{Z}$ para todo n.

Definição 2.18. *Um domínio A é um **domínio de ideais principais** se todo ideal de A é principal.*

Definição 2.19. *Um anel A é chamado **integralmente fechado** se todo elemento do seu corpo de frações que é inteiro sobre A está em A.*

Proposição 2.1. *Se A é um domínio de ideais principais então A é integralmente fechado.*

Exemplo 2.12. O anel $\mathbb{Z}$ dos números inteiros é integralmente fechado, pois é um domínio de ideais principais.

Podemos definir a **norma** de um ideal. No caso de um ideal principal, isso está diretamente relacionado com a norma do gerador do ideal, definido em (2.13).

Definição 2.20. *Seja $\mathcal{I} = \langle x \rangle \mathcal{O}_L$ um ideal principal de $\mathcal{O}_L$. Sua* **norma** *é definida por $N(\mathcal{I}) = |N(x)|$.*

2.4 Corpos Quadráticos

Nosso objetivo aqui é determinar o anel dos inteiros algébricos, base integral e discriminante dos corpos quadráticos.

Definição 2.21. *Uma extensão de corpos de grau 2 sobre o corpo $\mathbb{Q}$ é chamado um* ***corpo quadrático****.*

Proposição 2.2. *Todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, sendo d um inteiro livre de quadrados, isto é, d não é divisível pelo quadrado de nenhum inteiro maior que 1.*

Sejam $K = \mathbb{Q}(\theta)$ um corpo quadrático e $f(x) = x^2 + ax + b$, com $a, b \in \mathbb{Q}$, o polinômio minimal de $\theta \in K$. Resolvendo a equação quadrática $\theta^2 + a\theta + b = 0$, temos que $\theta = \dfrac{-a \pm \sqrt{a^2 - 4b}}{2}$ são as raízes de $f(x)$. Como $2\theta \pm a = \sqrt{a^2 - 4b}$, segue que $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{a^2 - 4b})$.

Por outro lado, $a^2 - 4b$ é um número racional que podemos escrever como $a^2 - 4b = \dfrac{u}{v} = \dfrac{uv}{v^2}$, com $u, v \in \mathbb{Z}$ e $mdc(u, v) = 1$ e de forma que u e v não sejam quadrados perfeitos, pois caso contrário teríamos $\mathbb{Q}(\theta) = \mathbb{Q}$. Assim, $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{a^2 - 4b}) = \mathbb{Q}\left(\sqrt{\dfrac{u}{v}}\right) = \mathbb{Q}\left(\sqrt{\dfrac{uv}{v^2}}\right) = \mathbb{Q}(\sqrt{uv})$. Suponhamos que $uv = k^2 d$, com $k, d, \in \mathbb{Z}$, e d livre de quadrados. Logo, $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{uv}) = \mathbb{Q}(\sqrt{k^2 d}) = \mathbb{Q}(\sqrt{d})$.

Observação 2.4. Se $d > 0$, a extensão $\mathbb{Q}(\sqrt{d})$ é dita **real** e se $d < 0$, a extensão $\mathbb{Q}(\sqrt{d})$ é dita **imaginária**.

Proposição 2.3. *Seja $K = \mathbb{Q}(\sqrt{d})$, com d um inteiro livre de quadrados, um corpo quadrático. Se um elemento $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ é um inteiro algébrico, então $2a$ e $a^2 - db^2$ são números inteiros.*

Demonstração: Seja $\alpha \in K$ um inteiro algébrico. Então existem $a_0, \cdots, a_{n-1} \in \mathbb{Z}$ tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Assim, considerando σ um automorfismo de K tal que $\sigma(\sqrt{d}) = -\sqrt{d}$, segue que, $\sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \cdots + a_1\sigma(\alpha) + a_0 = 0$, ou seja, $\sigma(\alpha)$ também é um inteiro algébrico de K. Temos que $\alpha + \sigma(\alpha)$ e $\alpha\sigma(\alpha)$ também são inteiros algébricos de K. Além disso, se $\alpha = a + b\sqrt{d}$, com a, $b \in \mathbb{Q}$, então $\alpha + \sigma(\alpha) = 2a \in \mathbb{Q}$ e $\alpha\sigma(\alpha) = a^2 - db^2 \in \mathbb{Q}$. Como $\mathbb{Z}$ é integralmente fechado segue que $2a$ e $a^2 - db^2$ são números inteiros.

A seguir determinaremos o anel dos inteiros algébricos de um corpo quadrático $K = \mathbb{Q}(\sqrt{d})$, com d um inteiro livre de quadrados.

Teorema 2.9. *Se $K = \mathbb{Q}(\sqrt{d})$ é um corpo quadrático com $d \in \mathbb{Z}$ livre de quadrados, então o anel dos inteiros algébricos $\mathcal{O}_K$ de $\mathbb{Q}(\sqrt{d})$ é dado por:*
a) $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ *se* $d \equiv 2$ *ou* $d \equiv 3 (mod\, 4)$ *e*
b) $\mathcal{O}_K = \mathbb{Z}\left[\dfrac{1 + \sqrt{d}}{2}\right]$ *se* $d \equiv 1 (mod\, 4)$.

Demonstração: Seja $\alpha = a+b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, com $a,\ b \in \mathbb{Q}$, um inteiro algébrico sobre $\mathbb{Z}$. Se $b = 0$ então o polinômio minimal de α sobre $\mathbb{Q}$ é dado por $p = irr_\alpha \mid \mathbb{Q} = x - a$, e como α é um inteiro algébrico sobre $\mathbb{Z}$, segue que $a \in \mathbb{Z}$. Se $b \neq 0$, então o polinômio minimal $p = irr_\alpha \mid \mathbb{Q}$ tem grau 2 e é obtido do seguinte modo:

$$\alpha = a + b\sqrt{d} \Longrightarrow \alpha - a = b\sqrt{d} \Longrightarrow (\alpha - a)^2 = b^2 d \Longrightarrow \alpha^2 - 2a\alpha + a^2 = b^2 d \Longrightarrow$$
$$\alpha^2 - 2a\alpha + (a^2 - b^2 d) = 0.$$

Logo $m(x) = x^2 - 2ax + a^2 - db^2$. Pela Proposição (2.3) temos que $2a,\ a^2 - db^2 \in \mathbb{Z}$. Assim, $(2a)^2 - d(2b)^2 \in \mathbb{Z}$ e daí $d(2b)^2 \in \mathbb{Z}$, pois $2a \in \mathbb{Z}$. Ainda temos que $2b \in \mathbb{Z}$, pois, caso contrário, no seu denominador existiria um fator primo p que apareceria na forma p^2 no denominador de $(2b)^2$ e como d é livre de quadrados teríamos que $d(2b)^2 \notin \mathbb{Z}$, o que é um absurdo. Logo, $2b \in \mathbb{Z}$. Assim, podemos escrever:

$$a = \frac{u}{2},\ b = \frac{v}{2},\quad com\, u,\ v \in \mathbb{Z}. \tag{2.11}$$

Além disso, temos que

$$(2a)^2 - d(2b)^2 \in 4\mathbb{Z}. \tag{2.12}$$

Substituindo a por $\dfrac{u}{2}$ e b por $\dfrac{v}{2}$, obtemos $u^2 - dv^2 \in\ 4\mathbb{Z}$.

a) Se $d \equiv 2$ ou $3(mod\,4)$, temos que u e v são pares, pois se v fosse ímpar teríamos $v^2 \equiv 1(mod\,4)$. Assim, como $u^2 - dv^2 \in 4\mathbb{Z}$ temos que $u^2 \equiv dv^2 \equiv d(mod\,4)$, ou seja, $d \equiv 0(mod\,4)$ ou $d \equiv 1(mod\,4)$, o que é um absurdo. Portanto, concluímos que v é par, isto é, $v^2 \equiv 0(mod\,4)$ e assim, $u^2 \equiv dv^2 \equiv 0(mod\,4)$ o que implica que u é par. Logo, se $\alpha = a + b\sqrt{d} \in \mathcal{O}_K$ temos que $\alpha \in \mathbb{Z}[\sqrt{d}]$ e assim, $\mathcal{O}_K \subset \mathbb{Z}[\sqrt{d}]$. Por outro lado, tomando $\alpha \in \mathbb{Z}[\sqrt{d}]$, temos que α é raiz do polinômio $x^2 - 2ax + a^2 - db^2 \in \mathbb{Z}[x]$, pois pela Proposição (2.3), temos que $2a,\ a^2 - db^2 \in \mathbb{Z}$. Logo, $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_K$. Portanto, $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.

b) Se $d \equiv 1(mod\,4)$, temos que $u^2 - dv^2 \in 4\mathbb{Z}$, e que u e v são de mesma paridade, isto é, são ambos pares ou ímpares. Se u e v são pares então $a,\ b \in \mathbb{Z}$. Logo, $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Se u e v são ímpares, então $\alpha = a + b\sqrt{d} = u/2 + (v/2)\sqrt{d} = (u - v)/2 + v((1 + \sqrt{d})/2) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Portanto, $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, ou seja, $\mathcal{O}_K \subset \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Por outro lado, se $\alpha = a + b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, com $a,\ b \in \mathbb{Z}$, temos que $2a + b \in \mathbb{Z}$ e $(a + b/2)^2 - d(b/2)^2 = a^2 + ab + (1 - d)b^2/4 \in \mathbb{Z}$, pois $d \equiv 1(mod\,4)$. Logo, $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subset \mathcal{O}_K$, pois os coeficientes do polinômio minimal de α, que é $m(x) = x^2 - (2a + b)x + a^2 + ab + (1 - d)b^2/4$ estão em $\mathbb{Z}$. Portanto, $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathcal{O}_K$.

Exemplo 2.13. Seja K o corpo quadrático $\mathbb{Q}(\sqrt{-1})$. O anel dos inteiros algébricos de K é dado por $\mathcal{O}_K = \mathbb{Z}[i] = \{a + bi :\ a, b \in \mathbb{Z}\}$, onde $i = \sqrt{-1}$ pois $d = -1 \equiv 3(mod\,4)$. O anel dos inteiros algébricos do corpo quadrático $\mathbb{Q}(\sqrt{-3})$ é $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ pois $d = -3 \equiv 1(mod\,4)$.

Como os $\mathbb{Q}$-monomorfismos de $K = \mathbb{Q}(\sqrt{d})$ em $\mathbb{C}$, com $d \in \mathbb{Z}$ livre de quadrados, são σ_1 e σ_2, onde $\sigma_1(\sqrt{d}) = \sqrt{d}$ e $\sigma_2(\sqrt{d}) = -\sqrt{d}$, segue que o discriminante de um

corpo quadrático é obtido do seguinte modo:
i) se $d \equiv 1(mod\,4)$, então

$$D_K = D_{K/\mathbb{Q}}\left(1, \frac{1+\sqrt{d}}{2}\right) = \left(\det\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1\left(\frac{1+\sqrt{d}}{2}\right) & \sigma_2\left(\frac{1+\sqrt{d}}{2}\right) \end{pmatrix}\right)^2 =$$
$$= \left(\det\begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{d}}{2} & \frac{1-\sqrt{d}}{2} \end{pmatrix}\right)^2 = d.$$

ii) se $d \equiv 2$ ou $3(mod\,4)$ então

$$D_K = D_{K/\mathbb{Q}}\left(1, \sqrt{d}\right) = \left(\det\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\sqrt{d}) & \sigma_2(\sqrt{d}) \end{pmatrix}\right)^2 = \left(\det\begin{pmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{pmatrix}\right)^2 = 4d.$$

Exemplo 2.14. Dado $K = \mathbb{Q}(\sqrt{5})$, tem-se $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, isto é, $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ é uma base integral de $\mathcal{O}_K$ e o discriminante de K é

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

Os monomorfismos de K em $\mathbb{C}$ são σ_1 a inclusão e σ_2 a conjugação complexa, isto é, $\sigma_1(a+b\sqrt{5}) = a+b\sqrt{5}$ e $\sigma_2(a+b\sqrt{5}) = a-b\sqrt{5}$. Logo, $Tr_{K/\mathbb{Q}}(a+b\sqrt{5}) = \sum_{i=1}^{2}\sigma_i(a+b\sqrt{5}) = 2a$ e $\mathcal{N}_{K/\mathbb{Q}}(a+b\sqrt{5}) = \prod_{i=1}^{2}\sigma_i(a+b\sqrt{5}) = a^2-5b^2$.

Exemplo 2.15. Dado $K = \mathbb{Q}(i)$ então $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$, isto é, $\{1, \sqrt{-1}\}$ é uma base integral para $\mathcal{O}_K$ e o discriminante absoluto de K é

$$d_K = \det\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\sqrt{-1}) & \sigma_2(\sqrt{-1}) \end{pmatrix}^2 = \det\begin{pmatrix} 1 & 1 \\ \sqrt{-1} & -\sqrt{-1} \end{pmatrix}^2 = -4.$$

Os monomorfismos de K em $\mathbb{C}$ são σ_1 a inclusão e σ_2 a conjugação complexa, isto é, $\sigma_1(a+b\sqrt{-1}) = a+b\sqrt{-1}$ e $\sigma_2(a+b\sqrt{-1}) = a-b\sqrt{-1}$. Logo, $Tr_{K/\mathbb{Q}}(a+b\sqrt{-1}) = \sum_{i=1}^{2}\sigma_i(a+b\sqrt{-1}) = 2a$ e $\mathcal{N}_{K/\mathbb{Q}}(a+b\sqrt{-1}) = \prod_{i=1}^{2}\sigma_i(a+b\sqrt{-1}) = a^2+b^2$.

Exemplo 2.16. Seja $L = \mathbb{Q}(i, \sqrt{5}), M = \mathbb{Q}(i)$ e $K = \mathbb{Q}(\sqrt{5})$.

Temos que:

1. $\mathcal{O}_K = \left\{a + b\left(\frac{1+\sqrt{5}}{2}\right) \mid a, b \in \mathbb{Z}\right\}$, $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ é uma $\mathbb{Z}$ - base para $\mathcal{O}_K$ e o polinômio minimal de $K/\mathbb{Q}$ é $p(x) = x^2 - x - 1 \in \mathbb{Z}[x]$.
2. $\mathcal{O}_L = \left\{a + b\left(\frac{1+\sqrt{5}}{2}\right) \mid a, b \in \mathbb{Z}[i]\right\}$, $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ é uma $\mathbb{Z}[i]$ - base para $\mathcal{O}_M$ e o polinômio minimal de L/M é $p(x) = x^2 - x - 1 \in \mathbb{Z}[i][x]$.

As raízes de $p(x) = x^2 - x - 1$ são: $\theta = \dfrac{1+\sqrt{5}}{2}$ e $\dfrac{1-\sqrt{5}}{2}$.
Logo,

$$\sigma_1(\theta) = \frac{1+\sqrt{5}}{2} \text{ e } \sigma_2(\theta) = \frac{1-\sqrt{5}}{2}.$$

Assim temos:

$$\begin{aligned} x^2 - x - 1 &\overset{Teo.(2.5)}{=} (x - \sigma_1(\theta))(x - \sigma_2(\theta)) \\ &= x^2 - x(\sigma_1(\theta) + \sigma_2(\theta)) + \sigma_1(\theta)\sigma_2(\theta) \\ &\overset{Def.(2.13)}{=} x^2 - Tr(\theta)x + N(\theta). \end{aligned} \tag{2.13}$$

2.5 Módulos

Nesta seção apresentamos alguns conceitos que serão usados no próximo capítulo.

Definição 2.22. *Seja A um anel. Um A-***módulo** *M é um grupo abeliano (aditivo) munido de uma aplicação $A \times M \longrightarrow M$, denotada por $(a, m) \longrightarrow am$, tal que, para quaisquer $a, b \in A$ e $x, y \in M$, tem-se:*
i) $a(x + y) = ax + ay$;
ii) $(a + b)x = ax + bx$;
iii) $(ab)x = a(bx)$;
iv) $1x = x$.

Definição 2.23. *Sejam A um anel e M um A-módulo. Um subconjunto $N \subset M$ não vazio é um A-***submódulo** *de M se, com as operações herdadas de M, também é um A-módulo.*

Um A-módulo que possui uma base é chamado de um A-**módulo livre** e o número de elementos da base é chamado de **posto** de M.

2.6 Números p-ádicos e anel de valorização

Os resultados dessa seção serão de grande importância para um melhor entendimento da construção que faremos no Capítulo 5.

Definição 2.24. *Seja B um domínio de integridade e denotemos por K seu corpo de frações. Dizemos que B é um* **anel de valorização** *de K se, para cada $x \neq 0$ ou $x \in B$ ou $x^{-1} \in B$ (ou ambos).*

Definição 2.25. *Seja $p \in \mathbb{N}$ um primo qualquer e escreva $x \in \mathbb{Z}$ como $x = p^m b$, onde $m \in \mathbb{N} \cup \{0\}$ e o máximo divisor comum entre b e p é 1. A valorização p-ádica de x é definida pela função $v_p(x) = m$, onde m é a maior potência de p que divide x.*

Exemplo 2.17. $v_5(10) = 1$, $v_{11}(16) = 0$, $v_3(54) = 3$.

Propriedades:

1. $v_p(a) \geq 0$;
2. $v_p(ab) = v_p(a) + v_p(b)$;
3. $v_p(a + b) \geq min(v_p(a), v_p(b))$.

Para todo $x \in \mathbb{Q}$ a norma p-ádica de x é dada por

$$|x|_p = \begin{cases} p^{-v_p(x)} & se \quad x \neq 0 \\ p^{-\infty} = 0 & se \quad x = 0. \end{cases}$$

Proposição 2.4. *A função* $|\ |_p : \mathbb{Q} \to \mathbb{R}^+$ *tem as tem as seguintes propriedades:*

1. $|x|_p = 0$ *se, e somente se,* $x = 0$;
2. $|xy|_p = |x|_p|y|_p$;
3. $|x + y| \leq max\{|x|_p, |y|_p\}$ *e a igualdade ocorre se,* $|x|_p \neq |y|_p$.

O corpo de valorização dos números p-ádicos é o completamento $\hat{\mathbb{Q}}$ de $\mathbb{Q}$ com respeito a norma $|\ |_p$ e é denotado por $\mathbb{Q}_p$. A norma em $\mathbb{Q}_p$ será denotada por $|\ |_p$ e o conjunto $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v_p(x) \geq 0\}$ é o seu anel de valorização.

3 Reticulados Algébricos

Neste capítulo apresentamos um método para a geração de reticulados no $\mathbb{R}^n$. A vantagem de obter reticulados por este método é que podemos identificar os pontos do reticulado no $\mathbb{R}^n$ como os elementos de um corpo de números.

Definição 3.1. *Sejam* $\{v_1, v_2, ..., v_m\}$ *vetores linearmente independentes do* $\mathbb{R}^n$ *(logo,* $m \leq n$*). O conjunto de pontos*

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

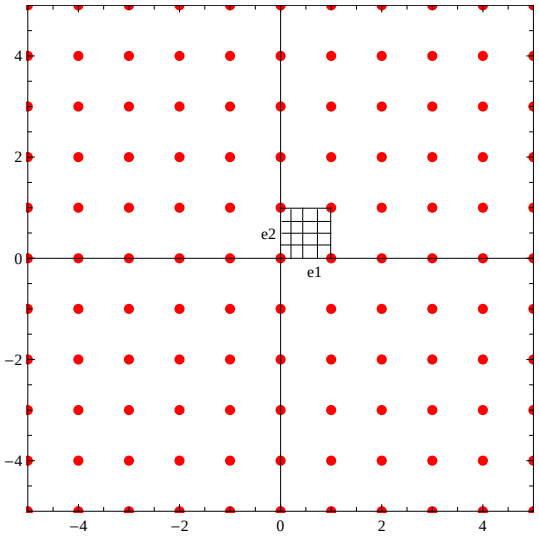
é chamado ***reticulado*** *de dimensão* m *e* $\{v_1, v_2, ..., v_m\}$ *é chamado de* ***base*** *do reticulado.*

Definição 3.2. *O paralelepípedo formado pelos pontos*

$$\theta_1 v_1 + \cdots + \theta_m v_m, \ 0 \leq \theta_i < 1$$

é chamado um **paralelepípedo fundamental** *ou* **região fundamental** *do reticulado.*

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 abaixo.



Definição 3.3. *Seja* $\{v_1, \ldots, v_m\}$ *uma base de* Λ. *Se* $v_i = (v_{i1}, \ldots, v_{in})$, *para* $i = 1, \cdots, m$, *a matriz*

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

é chamada uma ***matriz geradora*** *para o reticulado. A matriz* $G = MM^t$ *é chamada uma* ***matriz de Gram*** *para o reticulado, onde* t *denota a transposição.*

Assim, os pontos do reticulado são formados por

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

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

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

o mesmo reticulado pode ser representado em algumas diferentes maneiras. Como uma 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 temos que ter é que tendo o mesmo determinante não é suficiente para garantir que dois reticulados são equivalentes. Essas considerações serão importantes mais tarde, quando construiremos constelações de reticulados algébricos onde a orientação do reticulado no espaço euclidiano se torna importante.

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

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

Definição 3.5. *Seja* B *uma matriz* $n \times n$ *com coeficientes em* $\mathbb{Z}$. *Um* ***subreticulado*** *de* Λ *é dado por*

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

Definição 3.6. *Dado um reticulado* Λ, *um reticulado* ***escalonado*** Λ' *pode ser obtido multiplicando todos os vetores do reticulado por uma constante, isto é,*

$$\Lambda' = c\Lambda,\ c \in \mathbb{R}.$$

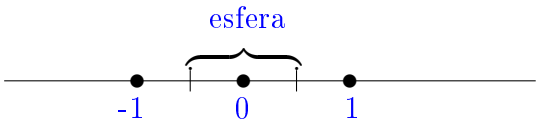
Ainda, Λ' *é um sub-reticulado de* Λ *quando* $c \in \mathbb{Z}$.

É importante observar que o mesmo reticulado pode ser representado de diferentes maneiras e como uma 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 temos que ter é que tendo o mesmo determinante não é suficiente para garantir que dois reticulados são equivalentes.

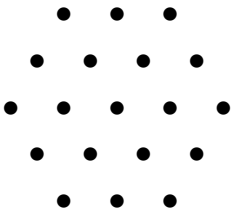
Definição 3.7. *Um* **empacotamento esférico**, *ou simplesmente um empacotamento no* $\mathbb{R}^n$, *é uma distribuição de esferas de mesmo raio no* $\mathbb{R}^n$ *de forma que a intersecção de quaisquer duas esferas tenha no máximo um ponto. Pode-se descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio.*

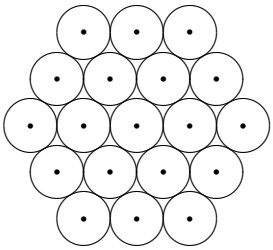
Um dos problemas de empacotamento esférico de um reticulado no $\mathbb{R}^n$ é encontrar um empacotamento com maior densidade. A seguir, daremos exemplos em dimensões 1, 2 e 3. Para maiores detalhes, consultar [5].

Em dimensão um, temos que os pontos de coordenadas inteiras da reta formam um $\mathbb{Z}$-reticulado cuja a densidade de empacotamento é a melhor possível dada por $\Delta = 1$. Neste caso, as "esferas" são intervalos como podemos ver na figura abaixo.



Para dimensão dois o reticulado hexagonal A_2 (favo de mel) é o de maior densidade, dada por $\Delta = \dfrac{\pi}{\sqrt{12}} \approx 0,9069$. O empacotamento deste reticulado com base $\beta = \left\{(1,0), (-\frac{1}{2}, \frac{\sqrt{3}}{2})\right\}$ é dado por





Em dimensão o reticulado conhecido como fcc, (*face centered cubic*) é o empacotamento com maior densidade (pirâmides de laranjas), sendo essa $\Delta = \dfrac{\pi}{\sqrt{18}} \approx 0,7405$.

Definição 3.8. *Seja $\sigma_1, \cdots, \sigma_n$ os n mergulhos de um corpo de números K de grau n, e vamos ordenar os σ_i's de modo que, para todo $x \in K$, $\sigma_i(x) \in \mathbb{R}$, $1 \leq i \leq r_1$, e $\sigma_{j+r_2}(x)$ é o conjugado complexo de $\sigma_j(x)$ para $r_1 + 1 \leq j \leq r_1 + r_2$. Note que $r_1 + 2r_2 = n$. Chamamos de* **mergulho canônico** *$\sigma : K \longrightarrow \mathbb{R}^{r_1+2r_2}$ o isomorfismo definido por*

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

onde $\Re$ e $\Im$ denotam as partes real e imaginária, respectivamente.

Podemos definir um mergulho similar se considerarmos, ao invés da extensão $K/\mathbb{Q}$, uma extensão mais geral L/K:

$$\begin{array}{rccl} \sigma: & L & \longmapsto & \mathbb{C}^n \\ & x & \longrightarrow & \sigma(x) = (\sigma_1(x), ..., \sigma_n(x)) \end{array}$$

onde $\sigma_1(x), ..., \sigma_n(x)$ são mergulhos relativos de L sobre K isto é, $\sigma_i(x)$ fixa K para todo $i = 1, ..., n$.

Exemplo 3.2. Sejam o corpo quadrático $K = \mathbb{Q}(i)$, onde $i = \sqrt{-1}$, e $\{\sigma_1, \sigma_2\}$ o grupo dos $\mathbb{Q}$-monomorfismos de K em $\mathbb{C}$, onde σ_1 é a aplicação identidade e $\sigma_2(a+bi) = a-bi$, com $a, b \in \mathbb{Q}$. Neste caso, $r_1 = 0$ e $r_2 = 1$. Para $x = a + bi \in K$, com $a, b \in \mathbb{Q}$, temos $\sigma(x) = (\Re\sigma_1(x), \Im\sigma_1(x)) = (a, b)$.

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

Teorema 3.1. *Sejam $\{w_1, \cdots, w_n\}$ uma base integral de K e $\sigma : K \to \mathbb{C}$ o mergulho canônico. Os n vetores $\mathbf{v_i} = \sigma(w_i) \in \mathbb{R}^n$, $i = 1, \cdots, n$ são linearmente independentes e definem um reticulado em $\mathbb{R}^n$, denominado* **reticulado algébrico** *de posto máximo, $\Lambda = \sigma(\mathcal{O}_K)$.*

Proposição 3.1. *Seja K um corpo de números de grau n e B um $\mathbb{Z}$-submódulo livre de K de posto n. Se $(x_i)_{1\leq i\leq n}$ é uma $\mathbb{Z}$-base de B, então $\sigma(B)$ é um reticulado em $\mathbb{R}^n$.*

Concluímos assim, que o ingrediente chave para a construção de reticulados algébricos tem sido a existência de uma $\mathbb{Z}$-base livre em K. Como $\mathcal{O}_K$ e seus ideais são $\mathbb{Z}$-módulos livres de posto n, podemos mergulhá-los em $\mathbb{R}^n$ para obter um reticulado algébrico.

A matriz geradora M de um reticulado algébrico, isto é, de um reticulado construído usando o mergulho canônico de K, é dada por

$$\begin{pmatrix} \sigma_1(w_1) & \cdots & \sigma_{r_1}(w_1) & \Re\sigma_{r_1+1}(w_1) & \cdots & \Im\sigma_{r_1+r_2}(w_1) \\ \vdots & & & & \vdots & \\ \sigma_1(w_n) & \cdots & \sigma_{r_1}(w_n) & \Re\sigma_{r_1+1}(w_n) & \cdots & \Im\sigma_{r_1+r_2}(w_n) \end{pmatrix},$$

onde $\{w_1, \cdots, w_n\}$ é aqui uma base de $\mathcal{O}_K$. Isto dá um reticulado real.

Analogamente, um reticulado complexo Λ^c é dado por

$$\Lambda^c = \{x = \lambda M \in \mathbb{C}^n \mid \lambda \in \mathbb{Z}[i]^n \text{ ou } \mathbb{Z}[j]^n\}.$$

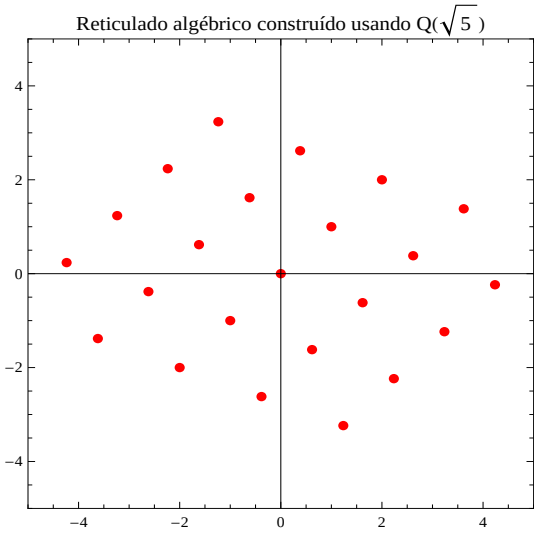
Agora sua matriz geradora é dada, usando o mergulho $\sigma(x) = (\sigma_1(x), \cdots, \sigma_n(x))$, por

$$\begin{pmatrix} \sigma_1(w_1) & \sigma_2(w_1)\cdots & \sigma_n(w_1) \\ \sigma_1(w_2) & \sigma_2(w_2)\cdots & \sigma_n(w_2) \\ \vdots & & \vdots \\ \sigma_1(w_n) & \sigma_2(w_n)\cdots & \sigma_n(w_n) \end{pmatrix}, \tag{3.1}$$

onde $\{w_1, \cdots, w_n\}$ é uma base de $\mathcal{O}_L$ sobre K, e $\sigma_1, \cdots, \sigma_n$ são mergulhos relativos de L/K.

Exemplo 3.3. Seja $K = \mathbb{Q}(\sqrt{5})$. A base integral de K é $\{1, \frac{1+\sqrt{5}}{2}\}$ e $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. Pelo Teorema (3.1), $\Lambda = \sigma(\mathcal{O}_K)$ é um reticulado no $\mathbb{R}^2$. Os dois mergulhos são $\sigma_1(\sqrt{5}) = \sqrt{5}$, $\sigma_2(\sqrt{5}) = -\sqrt{5}$ e a matriz geradora do reticulado é

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

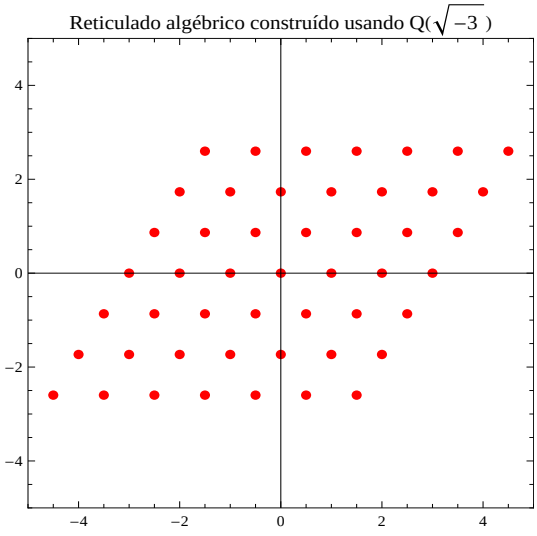


Exemplo 3.4. Seja $K = \mathbb{Q}(\sqrt{-3})$. A base integral de K é $\{1, \frac{1+\sqrt{-3}}{2}\}$ e $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. Pelo Teorema (3.1), $\Lambda = \sigma(\mathcal{O}_K)$ é um reticulado no $\mathbb{R}^2$. Os dois mergulhos são $\sigma_1(\sqrt{-3}) = \sqrt{-3}$, $\sigma_2(\sqrt{-3}) = -\sqrt{-3}$. Neste caso, $r_1 = 0$ e $r_2 = 2$, assim, a matriz geradora do reticulado é

$$M = \begin{pmatrix} \Re\sigma_1(1) & \Im\sigma_1(1) \\ \Re\sigma_1\left(\frac{1+\sqrt{-3}}{2}\right) & \Im\sigma_1\left(\frac{1+\sqrt{-3}}{2}\right) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix},$$

.

Observe que via $\mathbb{Q}(\sqrt{-3})$ obtivemos o reticulado hexagonal A_2.



Até então usamos o anel dos inteiros $\mathcal{O}_K$ para construir reticulados algébricos, mas veremos que tais reticulados podem ser obtidos de maneira mais geral, considerando ideais de $\mathcal{O}_K$ ou considerando ideais em $\mathcal{O}_L$, onde L é uma extensão finita de K.

Um reticulado algébrico Λ' construído a partir de um ideal $\mathcal{I} \subset \mathcal{O}_L$ da um subreticulado do reticulado algébrico Λ construído de $\mathcal{O}_L$. Se $\mathcal{I} = \alpha\mathcal{O}_L$, então a matriz geradora M é dada por

$$M = \begin{pmatrix} \sigma_1(\alpha w_1) & \sigma_2(\alpha w_1) \cdots & \sigma_n(\alpha w_1) \\ \sigma_1(\alpha w_2) & \sigma_2(\alpha w_2) \cdots & \sigma_n(\alpha w_2) \\ \vdots & & \vdots \\ \sigma_1(\alpha w_n) & \sigma_2(\alpha w_n) \cdots & \sigma_n(\alpha w_n) \end{pmatrix}, \tag{3.2}$$

onde $\{w_1, \cdots, w_n\}$ é uma base de $\mathcal{O}_L$ sobre K, e $\sigma_1, \cdots, \sigma_n$ são mergulhos relativos. Equivalentemente, a matriz (3.2) é a matriz (3.1) multiplicada à esquerda pela matriz diagonal

$$\begin{pmatrix} \sigma_1(\alpha) & & 0 \\ & \ddots & \\ 0 & & \sigma_n(\alpha) \end{pmatrix}.$$

Dada a matriz geradora do reticulado, calculamos o *determinante* do reticulado construído a partir de (3.2), do seguinte modo:

$$\begin{aligned} \det(\Lambda) &= |\det(M)|^2 \\ &= |\det[\sigma_j(\alpha w_i)]|^2 \\ &= |N_{L/K}(\alpha)|^2 |\det[\sigma_j(w_i)]|^2 \\ &= |N_{L/K}(\alpha)|^2 |d_L|. \end{aligned}$$

Para a construção de códigos que faremos no Capítulo 5, restringiremos a extensões de corpos L/K, onde K é um corpo de números, de um tipo especial, a saber, $L/K = L'K/K$, isto é, L é o menor corpo contendo L' e K. Chamamos L de corpo de composição de L' e K (ver Figura abaixo). Além disso, consideramos aqui extensões $L'K/K$ cujos mergulhos relativos $\sigma_1, \cdots, \sigma_n$ de $L'K/K$ são os mesmos que os mergulhos de $L'/\mathbb{Q}$. Com esta suposição temos que o determinante do reticulado é

$$\det(\Lambda) = |N_{K/\mathbb{Q}}(\alpha)|^2 |d_K|,$$

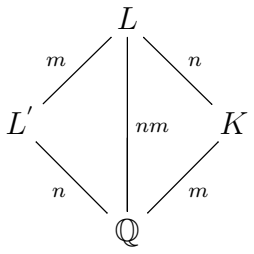
para um reticulado construído sobre $K/\mathbb{Q}$, enquanto

$$\det(\Lambda) = |N_{L'/\mathbb{Q}}(\alpha)|^2 |d_{L'}|. \tag{3.3}$$

Logo

$$\det(\Lambda) = |N_{L/K}(\alpha)|^2 |d_{L'}| \tag{3.4}$$

para um reticulado construído sobre a composição $L'K/K$.



A estrutura da composição de corpos L' e K.

4 Álgebras Cíclicas

Este capítulo é dedicado ao conhecimento matemático necessário para construir códigos a partir de álgebras de divisão cíclicas.

Introduzimos a noção de álgebra de divisão, chave para a codificação espaço-tempo, pois ela dá um modo de construir códigos espaço-tempo totalmente diversos. Visto que corpos de números permitem decodificar constelações QAM e HEX, uma particular família de álgebras, álgebras cíclicas, são construídas sobre corpos de números e estas darão para n antenas transmitidas, $n \times n$ palavras código espaço-tempo que enviam n^2 símbolos de informação, decodificados dentro de n^2 sinais.

Definição 4.1. *Uma* **álgebra** $\mathcal{A}$ *é um conjunto sobre um corpo* K *com operações de adição, multiplicação e multiplicação por elementos de* K *que tem as seguintes propriedades:*

1. $\mathcal{A}$ *é um espaço vetorial com respeito a adição e multiplicação por elementos do corpo.*
2. $\mathcal{A}$ *é um anel com respeito a adição e multiplicação.*
3. $(\lambda a)b = a(\lambda b) = \lambda(ab)$ *para qualquer* $\lambda \in K$, a, $b \in \mathcal{A}$.

Seja R um anel comutativo. O conjunto dos elementos de R que são inversíveis para a multiplicação é chamado de *conjunto das unidades* de R e é denotado por R^*.

Definição 4.2. *Seja* R *um anel tal que* $R^* = R\backslash\{0\}$ *, então dizemos que* R *é uma* **álgebra de divisão**.

Teorema 4.1. *Seja* L *extensão de corpos sobre* K *. O conjunto dos* K*-automorfismos de* L *formam um grupo sob a composição de funções.*

Definição 4.3. *Um* **grupo cíclico** G *é um grupo gerado por um elemento. Escrevendo o grupo com a lei multiplicativa, temos* $G = \{g, g^2, ..., g^{n-1}, 1\}$*, se* G *tem* n *elementos. Denotamos* $G = \langle g \rangle$.

Definição 4.4. *Uma extensão de corpos* L/K *é uma* **extensão de Galois** *se todo polinômio irredutível sobre* K *que tem pelo menos uma raiz em* L *tem, na verdade, todas as raízes em* L*. O* grupo de Galois *da extensão* L/K*, denotado por* $Gal(L/K)$*, é o grupo de todos os* K*-automorfismos de* L *sob a composição de funções.*

Usualmente denotamos um grupo cíclico de Galois por $\langle\sigma\rangle$, onde σ é o gerador do grupo.

Seja L/K uma extensão de Galois de grau n tal que seu grupo de Galois $G = Gal(L/K)$ é cíclico com gerador σ. Denote por K^* (resp. L^*) os elementos não nulos de K (resp. L).

Escolhendo um elemento $\gamma \in K^*$, construímos uma álgebra não-comutativa denotada por $\mathcal{A} = (L/K, \sigma, \gamma)$, como segue:

$$\mathcal{A} = L \oplus eL \oplus e^2L \oplus ... \oplus e^{n-1}L$$

onde $\oplus$ denota a soma direta e tal que e satisfaz

$$e^n = \gamma \text{ e } \lambda e = e\sigma(\lambda), \text{ para } \lambda \in L.$$

Esta álgebra é chamada de *álgebra cíclica*.

A álgebra $\mathcal{A}$ é definida como uma soma direta de cópias de L, o que significa que um elemento x na álgebra é escrito como

$$x = x_0 + ex_1 + \cdots + e^{n-1}x_{n-1},$$

com $x_i \in L$, $i = 0, \cdots, n-1$.

A razão destas álgebras cíclicas serem interessantes neste trabalho é a existência de um correspondência entre um elemento x da álgebra $\mathcal{A}$ e uma matriz $X \in M_n(L)$.

Para $n = 2$ temos $\mathcal{A} = 1.L + e.L$, com $e^2 = \gamma$ e $\lambda e = e\sigma(\lambda)$, para $\lambda \in L$. Um elemento $x \in \mathcal{A}$ pode ser escrito como

$$x = x_0 + ex_1, \;\; x_0, x_1 \in L.$$

Vamos calcular o produto de x por qualquer elemento $y \in \mathcal{A}$:

$$\begin{aligned} xy &= (x_0 + ex_1)(y_0 + ey_1), \;\; y_0, y_1 \in L \\ &= x_0y_0 + x_0ey_1 + ex_1y_0 + ex_1ey_1 \\ &= x_0y_0 + e\sigma(x_0)y_1 + ex_1y_0 + e^2\sigma(x_1)y_1 \\ &= x_0y_0 + e\sigma(x_0)y_1 + ex_1y_0 + \gamma\sigma(x_1)y_1 \\ &= 1.[x_0y_0 + \gamma\sigma(x_1)y_1] + e[\sigma(x_0)y_1 + x_1y_0]. \end{aligned}$$

Na base $\{1, e\}$, temos a seguinte representação matricial:

$$xy = \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \end{pmatrix}.$$

Existe então uma correspondência

$$x = x_0 + ex_1 \in \mathcal{A} \longleftrightarrow \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix}.$$

Em particular,

$$e \in \mathcal{A} \longleftrightarrow \begin{pmatrix} 0 & \gamma\sigma(1) \\ 1 & \sigma(0) \end{pmatrix} = \begin{pmatrix} 0 & \gamma \\ 1 & 0 \end{pmatrix}$$

e

$$x_0 \in \mathcal{A} \longleftrightarrow \begin{pmatrix} x_0 & 0 \\ 0 & \sigma(x_0) \end{pmatrix}.$$

Para o caso geral de grau n, temos para todo $x_k \in L$,

$$x_k \in \mathcal{A} \longleftrightarrow \begin{pmatrix} x_k & 0 & \cdots & 0 \\ 0 & \sigma(x_k) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma^{(n-1)}(x_k) \end{pmatrix}.$$

$$e \in \mathcal{A} \longleftrightarrow \begin{pmatrix} 0 & 0 & \cdots & \gamma \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Formalmente, podemos associar uma matriz a qualquer elemento $x \in \mathcal{A}$ usando a função α_x, a multiplicação por x de um elemento $y \in \mathcal{A}$:

$$\begin{aligned} \alpha_x : \ & \mathcal{A} \longmapsto \mathcal{A} \\ & y \longmapsto \alpha_x(y) = \ xy \end{aligned}$$

A matriz do produto por α_x, com $x = x_0 + ex_1 + ... + e^{n-1}x_{n-1}$, é dada por

$$\begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \cdots & \gamma\sigma^{n-1}(x_2) \\ \vdots & & \vdots & & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \sigma^2(x_{n-4}) & \cdots & \gamma\sigma^{n-1}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}. \tag{4.1}$$

Então, via α_x, temos uma *matriz representação* de um elemento $x \in \mathcal{A}$.

Se x pertence a uma álgebra cíclica $\mathcal{A}$, então $x = \sum_{k=0}^{n-1} e^k x_k$, $x_i \in L$, $i = 0, \cdots, n-1$. Como L é um espaço vetorial de dimensão n sobre K, então cada x_i é uma combinação linear de n elementos em K. Portanto, dizemos que o STBC $\mathcal{C}_\infty$ é um código sobre K e é dado por

$$\mathcal{C}_\infty = \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \cdots & \gamma\sigma^{n-1}(x_2) \\ \vdots & & \vdots & & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \sigma^2(x_{n-4}) & \cdots & \gamma\sigma^{n-1}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}, x_i \in L, i = 1, ..., n-1. \tag{4.2}$$

Vamos discutir a decodificação e a taxa de tais códigos.

Suponha que os símbolos de informação enviados são vindos de uma constelação QAM ou HEX e considere $L = \mathbb{Q}(i, \sqrt{5})$. Então

$$x_0 = a_0 + \sqrt{5}b_0,\ x_1 = a_1 + \sqrt{5}b_1,\ a_0,\, a_1,\, b_0,\, b_1\ \in \mathbb{Q}(i).$$

Como os símbolos QAM podem ser escritos como elementos de $\mathbb{Z}[i]$, eles pertencem ao corpo base $\mathbb{Q}(i)$. Assim x_0 e x_1 decodificam dois símbolos de informação QAM, a_0, b_0 e a_1, b_1, respectivamente.

Em geral, se L/K tem grau n, cada coeficiente x_k de $x = \sum_{k=0}^{n-1} e^k x_k$ decodificará n símbolos de informação. Como o elemento $x \in \mathcal{A}$ tem n coeficientes, ele decodifica n^2 símbolos de informação. Códigos construídos a partir de álgebras cíclicas são ditos serem de *taxa total*, *taxa total*, neste sentido eles transmitem n^2 sinais que decodificam n^2 símbolos de informação, [3].

Observação 4.1. Como as constelações de sinais usualmente usadas são a QAM e a HEX, isto significa que consideramos extensões de corpos L/K onde K é $\mathbb{Q}(i)$ ou $\mathbb{Q}(j)$, onde j é uma raiz terceira primitiva da unidade.

Para construir STBCs com "boas" propriedades, nos restringiremos a um subconjunto de C_∞, obtido restringindo os coeficientes $x_0, ..., x_{n-1}$ para que estejam em $I \subseteq \mathcal{O}_L$, onde I é um ideal do anel de inteiros de L. Denotamos este código por $\mathcal{C}_I$:

$$\mathcal{C}_I = \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \cdots & \gamma\sigma^{n-1}(x_2) \\ \vdots & & \vdots & & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \sigma^2(x_{n-4}) & \cdots & \gamma\sigma^{n-1}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}, \tag{4.3}$$

$x_i \in I \subseteq \mathcal{O}_L, i = 1, ..., n-1.$

Observação 4.2. : Os códigos C_I são chamados códigos de bloco espaço-tempo de dispersão linear (LD-STBCs). Os LD-STBCs construídos sobre álgebras cíclicas tem as seguintes vantagens:

1) Temos um critério para decidir quando o STBC C_∞ satisfaz o critério do posto. De fato, quando a álgebra cíclica é uma álgebra de divisão, todos os seus elementos são invertíveis. Portanto, as matrizes das palavras código tem determinante não nulo.

2) Devido à linearidade, o determinante mínimo do código C_∞ é

$$\delta_{min}(C_\infty) = \min_{X_1, X_2 \in C_\infty} |det(X_1 - X_2)^2| = \min_{X \in C_\infty, X \neq 0} |det(X)^2|.$$

Definição 4.5. *Seja x um elemento de uma álgebra cíclica A. Então o determinante de sua matriz correspondente, como dada em (4.1), é chamado de* **norma reduzida** *de x.*

Como o critério do posto é totalmente satisfeito considerando uma álgebra de divisão, nosso trabalho será determinar um limitante inferior para o determinante mínimo.

Estamos então interessados em saber quando $det(X) \neq 0$ para todo $X \neq 0$, ou equivalentemente quando $\mathcal{A}$ é uma álgebra de divisão cíclica (isto é, todos os elementos de $\mathcal{A}$ são invertíveis).

Definição 4.6. *Uma álgebra cíclica que também é álgebra de divisão é chamada de* **álgebra de divisão cíclica**.

Vamos determinar quando uma álgebra cíclica é na verdade, uma álgebra de divisão cíclica.

Exemplo 4.1. Se $n = 2$, temos

$$\det \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix} = x_0\sigma(x_0) - \gamma x_1\sigma(x_1) = N_{L/K}(x_0) - \gamma N_{L/K}(x_1). \tag{4.4}$$

Então

$$\det(X) = 0 \Longleftrightarrow \gamma = N_{L/K}\left(\frac{x_0}{x_1}\right),$$

pois a multiplicatividade da norma segue da multiplicatividade do mergulho relativo. Então temos que verificar se γ não é uma norma de algum elemento de L e assim teremos $det(X) \neq 0$, para todo $0 \neq X \in \mathcal{C}$.

A próxima proposição nos diz como determinar se uma álgebra cíclica é uma álgebra de divisão para qualquer dimensão n.

Proposição 4.1 ([7], p. 279)**.** *Seja L/K uma extensão cíclica de grau n com grupo de Galois $Gal(L/K) =< \sigma >$. Se $\gamma, \gamma^2, \cdots, \gamma^{n-1} \in K^*$ não são uma norma de algum elemento de L, então $(L/K, \sigma, \gamma)$ é uma álgebra de divisão cíclica.*

Agora vamos mostrar como obter a *propriedade do determinante não nulo* em dois passos:

1. Como $x_0, x_1 \in L$, pelo Teorema (2.7), $N_{L/K}(x_0)$ e $N_{L/K}(x_1)$ estão em K. Como $\gamma \in K^* \subset L$, então, de acordo com (4.4), $\det(X) \in K$.

2. Agora, se nos restringirmos a $x_0, x_1 \in \mathcal{O}_L$, então novamente pelo Teorema (2.7), obtemos que $N_{L/K}(x_0)$ e $N_{L/K}(x_1)$ estão em $\mathcal{O}_K$. Escolhendo $\gamma \in \mathcal{O}_K$, concluímos, por (4.4), que $\det(X) \in \mathcal{O}_K$.

Quando transmitimos símbolos QAM ou HEX, pela Observação (4.1), K deve ser $\mathbb{Q}(i)$, resp. $\mathbb{Q}(j)$. Então

$$\det(X) \in \mathbb{Z}[i],\, \mathbb{Z}[j] \Longrightarrow |\det(X)|^2 \in \mathbb{Z}.$$

Assim

$$|\det(X)|^2 \geq 1,\ X \neq 0.$$

Este procedimento pode ser generalizado em dimensões altas n. Entretanto, o primeiro passo não pode ser provado do mesmo modo, pois o cálculo explicito do determinante em dimensões altas torna-se mais complicado.

Códigos lineares associados a uma matriz unitária (isto é, $U^{-1} = \overline{U}^t$) tem menor perda de informação. A seguir, mostraremos como obter tal matriz unitária para códigos baseados em álgebras cíclicas.

Lembre que uma palavra-código (4.3) tem a forma

$$\begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \cdots & \gamma\sigma^{n-1}(x_2) \\ \vdots & & \vdots & & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \sigma^2(x_{n-4}) & \cdots & \gamma\sigma^{n-1}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix},$$

onde cada camada é, até a multiplicação por γ, da forma $(x_l, \sigma(x_l), \cdots, \sigma^{n-1}(x_l))$, $l = 0, \cdots, n-1$.

A restrição sobre a forma requer que cada camada da palavra-código seja da forma Mv, onde M é uma matriz unitária e v é um vetor contendo os símbolos de informação. Seja $L = K(\theta)$ e $\{1, \theta, \cdots, \theta^{n-1}\}$ uma base de $\mathcal{O}_L$.

Cada camada de uma palavra-código é da forma

$$\begin{pmatrix} 1 & \theta & \cdots & \theta^{n-1} \\ 1 & \sigma(\theta) & \cdots & \sigma(\theta^{n-1}) \\ \vdots & & \vdots & \\ 1 & \sigma^{n-1}(\theta) & \cdots & \sigma^{n-1}(\theta^{n-1}) \end{pmatrix} \begin{pmatrix} u_{l,0} \\ u_{l,1} \\ \vdots \\ u_{l,n-1} \end{pmatrix} = \begin{pmatrix} x_l \\ \sigma(x_l) \\ \vdots \\ \sigma^{n-1}(x_l) \end{pmatrix} \tag{4.5}$$

para $x_l = \sum_{k=0}^{n-1} u_{l,k}\theta^k \in \mathcal{O}_L$. Como $u_{l,k}$ tomam valores discretos, podemos ver a multiplicação de matrizes acima como gerando pontos em um reticulado. A matriz M é então a *matriz geradora* do reticulado, cuja *matriz de Gram* é dada por $MM^\dagger$ ($M^\dagger = \overline{M}^t$).

Gostaríamos que M fosse unitária, ou seja, o reticulado que gostaríamos de obter para cada camada fosse um $\mathbb{Z}[i]^n$-reticulado, respectivamente um $\mathbb{Z}[j]^n$-reticulado, pois os símbolos QAM e HEX são subconjuntos finitos de $\mathbb{Z}[i]$ e $\mathbb{Z}[j]$, respectivamente.

A matriz M pode ser vista como uma matriz pré-codificação aplicada aos símbolos de informação.

Interpretar a matriz unitária M como a matriz geradora de um reticulado permite-nos usar a teoria dos reticulados algébricos. A idéia chave é que a matriz M dada em (4.5) precisa conter os mergulhos de uma base, mas esta base não precisa ser uma base do corpo L. Esta pode ser uma base de um subconjunto de L e de fato, será uma base de um ideal de L.

Vimos em (3.3) que o determinante de um reticulado algébrico Λ construído sobre um ideal principal $\mathcal{I} = (\alpha)\mathcal{O}_L$, onde $L/K = L^{'}K/K$, é dado por

$$\det(\Lambda) = |N_{L/K}(\alpha)|^2 |d_{L'}|.$$

Assim, para obter $\Lambda = \mathbb{Z}[i]^n$ (resp. $\mathbb{Z}[j]^n$), ou uma versão escalonada $\Lambda^{'} = (c\mathbb{Z}[i])^n$ (resp. $(c\mathbb{Z}[j])^n$), $c \in \mathbb{Z}$,uma condição necessária é encontrar em $\mathcal{O}_L$ um elemento α de norma desejada, pois

$$\det((c\mathbb{Z}[i])^n) = c^n \ \ (resp. \det((c\mathbb{Z}[j])^n = c^n).$$

Dada uma extensão $L^{'}K/K$, o discriminante é dado. Então temos que encontrar um elemento α tal que

$$|N_{L/K}(\alpha)|^2 |d_{L'}| = c^n. \tag{4.6}$$

Esta condição não é entretanto suficiente, e uma vez que este elemento é encontrado, podemos verificar se encontramos o reticulado certo calculando a matriz de Gram $MM^{\dagger}$, e que ela é a matriz identidade.

Estes dois passos:

1. encontrar um elemento α com a norma adequada em $\mathcal{O}_L$,

2. calcular a matriz de Gram,

formam o método que usaremos para obter a propriedade da forma sobre as constelações.

5 O Código de Ouro

Este capítulo é dedicado à construção do código de ouro, que é um código perfeito 2×2. Seu nome, código de ouro, veio de sua construção algébrica [9], que envolve o número de ouro $\frac{1+\sqrt{5}}{2}$.

O nome atribuído a esse número faz referência à razão áurea, obtida através da divisão de um segmento de reta $\overline{AB}$ em duas partes por um ponto C de forma que

$$\frac{\overline{AB}}{\overline{AC}} = \frac{\overline{AC}}{\overline{BC}}.$$

Muitas supostas aplicações desse número nas artes, arquitetura e na natureza são divulgadas em livros e meios de comunicação, mas há estudos como [16] e [17] que desmistificam algumas dessas afirmações.

5.1 Códigos espaço-tempo perfeitos

De acordo com as considerações feitas no Capítulo 2, os dois principais parâmetros para modelar códigos espaço-tempo são:

- **Diversidade total.** O critério do posto diz que para STBCs quadrados que a diversidade total é obtida se o determinante da diferença de duas palavras código distintas é não nulo:

$$\det(X) \neq 0,\ X \neq 0,\ X \in \mathcal{C}.$$

- **Determinante mínimo.** O ganho de codificação é dado pelo determinante mínimo

$$\delta_{\min}(\mathcal{C}_\infty) = \min_{X \in \mathcal{C}_\infty,\, X \neq 0} |\det(X)|^2.$$

Além disso, para melhorar o desempenho de códigos espaço-tempo, exigimos as seguintes propriedades apresentadas no Capítulo 2:

- Determinante não-nulo

- Forma
- Uniformidade média da energia transmitida por antena

Definição 5.1. *Um STBC quadrado $n_t \times n_t$ é chamado de código* **perfeito** *se, e somente se:*

- *É um código com taxa linear total usando n_t^2 símbolos de informação QAM ou HEX.*
- *O determinante mínimo do código infinito é não nulo (deste modo, em particular, o critério do posto é satisfeito).*
- *A energia necessária para enviar a combinação linear dos símbolos de informação em cada camada é similar a energia usada para enviar cada um dos símbolos.*
- *O código induz que a energia média transmitida por antena em todos os T intervalos de tempo seja uniforme, isto é, todos os símbolos codificados na matriz código tem a mesma energia média.*

Vamos resumir agora técnicas exploradas acima e dar os passos para a construção de códigos perfeitos.

1. Consideramos símbolos QAM ou HEX. Como estas constelações podem ser vistas como subconjuntos finitos do anel dos inteiros $\mathcal{O}_K = \mathbb{Z}[i]$ (resp. $\mathcal{O}_K = \mathbb{Z}[j]$), tomamos o corpo base $K = \mathbb{Q}(i)$ (resp.$\mathbb{Q}(j)$).

2. Tomamos a extensão L/K de grau $n = n_t$ (n_t: número de antenas transmissoras) e construímos a correspondente álgebra cíclica:

$$\mathcal{A} = (L/K, \sigma, \gamma).$$

   Escolhemos γ tal que $|\gamma| = 1$ para satisfazer a restrição sobre a energia média transmitida por antena.

3. Para obter determinante não nulo, escolhemos $\gamma \in \mathbb{Z}[i]$, (resp. em $\mathbb{Z}[j]$.) Adicionando a restrição anterior, $|\gamma| = 1$, temos que $\gamma \in \{1, i, -1, -i\} \subset \mathbb{Z}[i]$ (resp. $\gamma \in \{1, j, j^2, -1, -j, -j^2\} \subset \mathbb{Z}[j]$).

4. Entre todos os elementos de $\mathcal{A}$, consideramos o conjunto discreto de palavras código da forma $x = x_0 + x_1 e + \cdots + x_{n-1} e^{n-1}$, onde $x_i \in I$, um ideal de $\mathcal{O}_L$, o anel dos inteiros de L. Obtemos então um STBC da forma

$$\mathcal{C}_I = \left\{ \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \cdots & \gamma\sigma^{n-1}(x_2) \\ \vdots & & \vdots & & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \sigma^2(x_{n-4}) & \cdots & \gamma\sigma^{n-1}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}, x_i \in I \subseteq \mathcal{O}_L, i = 1, ..., n-1. \right\} \tag{5.1}$$

Os n^2 símbolos de informação $u_{\ell,k} \in \mathcal{O}_K$ são codificados em palavras-código por

$$x_\ell = \sum_{k=0}^{n-1} u_{\ell,k} v_k, \quad \ell = 0, \cdots, n-1,$$

onde $\{v_k\}_{k=0}^{n-1}$ é uma base do ideal I.

5. Escolhemos um ideal $\mathcal{I} \subseteq \mathcal{O}_L$ de modo que a constelação de sinais em cada camada seja um subconjunto finito das versões rotacionadas dos reticulados $\mathbb{Z}[i]^n$ ou $\mathbb{Z}[j]^n$.

6. Mostramos que $\mathcal{A} = (L/K, \sigma, \gamma)$ é uma álgebra de divisão escolhendo γ convenientemente, o que significa mostrar que $\gamma, \cdots, \gamma^{n-1}$ não é uma norma em L^*.

5.2 O código de ouro

O código de ouro é um código perfeito 2×2. O código de ouro é construído usando a álgebra cíclica

$$\mathcal{A} = (L = \mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i),\ \sigma,\ i),$$

com $\sigma : \sqrt{5} \longmapsto -\sqrt{5}$. Temos que

$$\mathcal{O}_L = \{a + b\theta |\ a,\ b \in \mathbb{Q}(i)\},$$

onde $\theta = \dfrac{1+\sqrt{5}}{2}$. Antes da propriedade forma, uma palavra-código desta álgebra é

$$\begin{bmatrix} a + b\theta & c + d\theta \\ i(c + d\sigma(\theta)) & a + b\sigma(\theta) \end{bmatrix},$$

com $a, b, c, d \in \mathbb{Z}[i]$.

5.2.1 O elemento $\gamma = i$ não é uma norma em $\mathbb{Q}(i, \sqrt{5})$

Mostramos aqui que a álgebra cíclica $\mathcal{A}$ que define o código de ouro é uma álgebra de divisão [9]. Para isto, temos que mostrar que $\gamma = i$ não é uma norma em $L/\mathbb{Q}(i)$.

Veremos primeiro a caracterização de um quadrado em um corpo de números.

Seja p um primo e denote por $GF(p)$ o corpo finito com p elementos.

Proposição 5.1. *[1] Seja $x \in GF(p)^*$. Temos*

$$x \text{ é um quadrado} \Leftrightarrow x^{\frac{p-1}{2}} = 1.$$

Corolário 5.1. *Se $p \equiv 1(mod\,4)$, -1 é um quadrado em $GF(p)$.*

Proposição 5.2. *Seja $L = \mathbb{Q}(i, \sqrt{5})$, então o elemento $\gamma = i$ não é uma norma relativa de qualquer $x \in L$, isto é, $N_{L/\mathbb{Q}(i)}(x) \neq i$, $\forall\, x \in L$.*

Demonstração: Seja $\mathbb{Q}_5$ denotando o corpo dos números 5-ádicos, e $\mathbb{Z}_5 = \{x \in \mathbb{Q}_5 | \nu_5(x) \geq 0\}$ seu anel de valorização.

Queremos mostrar que a equação $N_{L/\mathbb{Q}(i)}(x) = i$ não tem solução. Para isso, vamos mostrar que esta equação não tem solução em $\mathbb{Q}_5$, e então, não tem solução para $x \in L$.

Seja $w = a + b\sqrt{5} \in L$ com a, $b \in \mathbb{Q}(i)$ então devemos mostrar que

$$N_{L/\mathbb{Q}(i)}(w) = a^2 - 5b^2 = i \tag{5.2}$$

não tem solução para $a, b \in \mathbb{Q}(i)$. Primeiro vamos verificar que $i \in \mathbb{Z}_5$. De fato, existe um mergulho de $\mathbb{Q}(i)$ em $\mathbb{Q}_5$ se $X^2 + 1$, o polinômio minimal de i, tem raízes em $\mathbb{Z}_5$. Usando o Lema de Hensel ([20],p.75), é suficiente verificar que -1 é um quadrado em $GF(5)$.

Como $5 \equiv 1(mod\,4)$, então, pelo Corolário (5.1), -1 é um quadrado em $GF(5)$.

Usando o mergulho de $\mathbb{Q}(i)$ em $\mathbb{Q}_5$, esta equação pode ser vista em $\mathbb{Q}_p$ como segue:

$$a^2 - 5b^2 = y + 5x \; a,\, b \in \mathbb{Q}_p,\, x \in \mathbb{Z}_5 \tag{5.3}$$

onde $y^2 = -1$. Se existe uma solução para (5.2), então esta solução está em $\mathbb{Q}_p$. Portanto, provando que não existe solução para (5.3), concluímos a prova.

Vamos mostrar agora que em (5.3), a e b estão de fato, em $\mathbb{Z}_5$.

Tomando a valorização de ambos os lados de (5.3), temos

$$\nu_5(a^2 - 5b^2) = \nu_5(y + 5x).$$

Como $x \in \mathbb{Z}_5$ e y é uma unidade, segue que $\nu_5(y + 5x) \geq \min\{\nu_5(y), \nu_5(x) + 1\} = 0$, e temos igualdade pois ambas as valorizações são distintas. Agora, $0 = \nu_5(a^2 - 5b^2) = \min\{2\nu_5(a), 2\nu_5(b) + 1\} = 2\nu_5(a)$. Portanto, $\nu_5(a) = 0$, assim, $a \in \mathbb{Z}_5$ e consequentemente $b \in \mathbb{Z}_5$.

Reduzindo módulo $5\mathbb{Z}_5$ temos

$$\begin{aligned} (a^2 - 5b^2) mod\,(5\mathbb{Z}_5) &\equiv (y + 5x) mod\,(5\mathbb{Z}_5) \\ a^2 &\equiv y (mod\,(5\mathbb{Z}_5), \end{aligned}$$

e vemos que y deve ser um quadrado em $GF(5)$.

Como $y^2 = -1$, temos que $y = (-1)^{1/2}$ e portanto, $y^{(p-1)/2} = (-1)^{(p-1)/4} = -1$, onde a última igualdade segue do fato que, neste caso, $p = 5$. Pela Proposição (5.1), y não é um quadrado, o que é uma contradição.

5.2.2 O reticulado $\mathbb{Z}[i]^2$

Vamos ver agora como adicionar a propriedade da forma na palavra-código construída sobre $\mathcal{A}$. A Equação (4.6) nos diz que

$$\begin{aligned} \det(\Lambda) &= |N_{L/\mathbb{Q}(i)}(\alpha)|^2 |d_{\mathbb{Q}(\sqrt{5})}| \\ c^2 &= 5|N_{L/\mathbb{Q}(i)}(\alpha)|^2. \end{aligned}$$

Então procuramos por um elemento α tal que $|N_{L/\mathbb{Q}(i)}(\alpha)|^2 = 5$. Assim, para encontrar tal elemento, procuramos pela fatoração do elemento 5 em $\mathcal{O}_L$:

$$5 = (1 + i - i\theta)^2(1 - i + i\theta)^2.$$

Então escolhemos $\alpha = 1 + i - i\theta$. Vamos agora verificar que de fato, obtemos o reticulado correto. Sua matriz geradora é obtida aplicando o mergulho canônico complexo

$$\begin{aligned} \sigma : L &\to \mathbb{C}^2 \\ x &\mapsto \sigma(x) = (\sigma_1(x), \sigma_2(x)) \end{aligned}$$

na base relativa $\{\alpha, \alpha\theta\}$ de $\mathcal{I}_L = (\alpha)$:

$$M = \begin{pmatrix} \sigma_1(\alpha) & \sigma_1(\alpha\theta) \\ \sigma_2(\alpha) & \sigma_2(\alpha\theta) \end{pmatrix} = \begin{pmatrix} \alpha & \alpha\theta \\ \overline{\alpha} & \overline{\alpha}\theta \end{pmatrix} = \begin{pmatrix} 1 + i(1-\theta) & \theta - i \\ 1 + i(1-\overline{\theta}) & \overline{\theta} - i \end{pmatrix}$$

Um cálculo direto mostra que $MM^\dagger = 5I_2$. Então $\dfrac{1}{\sqrt{5}}M$ é uma matriz unitária, que nos da a propriedade da forma.

Uma palavra-código X pertencendo ao código de ouro e adicionando a propriedade da forma, é do seguinte modo

$$X = \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha(a + b\theta) & \alpha(c + d\theta) \\ i\sigma(\alpha)(c + d\sigma(\theta)) & \sigma(\alpha)(a + b\sigma(\theta)) \end{bmatrix}$$

onde a, b, c, $d \in \mathbb{Z}[i]$.

Quando a, b, c, d tomam quaisquer valores em $\mathbb{Z}[i]$, dizemos que temos um código infinito, $\mathcal{C}_\infty$.

5.2.3 O determinante mínimo

Vamos agora calcular o determinante mínimo do código infinito. O fator $\frac{1}{\sqrt{5}}$ é necessário para normalizar X de modo a obter uma matriz unitária. Como $\alpha\overline{\alpha} = 2+i$, temos

$$\begin{aligned} \det(X) &= \frac{2+i}{5}[(a+b\theta)(a+b\overline{\theta}) - i(c+d\theta)(c+d\overline{\theta})] \\ &= \frac{1}{2-i}[(a^2+ab-b^2-i(c^2+cd-d^2)]. \end{aligned}$$

Por definição de a, b, c, d, temos que o mínimo não trivial de $|a^2+ab-b^2-i(c^2+cd-d^2)|^2$ é 1 (tome $a=1$ e $b=c=d=0$), então

$$\delta_{min}(\mathcal{C}_\infty) = \frac{1}{25}|N_{L/\mathbb{Q}(i)}(\alpha)|^2 = \frac{1}{25}|2+i|^2 = \frac{1}{5}.$$

Então o determinante mínimo do código infinito é limitado e não nulo, como desejado.

5.3 Alguns comandos em KASH

O Kash é um sistema algébrico computacional usado para fazer sofisticados cálculos em teoria dos números algébricos, seu download é livre e pode ser encontrado em [19].

Nesta seção implementamos alguns cálculos envolvendo a extensão usada para a construção do Código de Ouro $\mathbb{Q}(i,\sqrt{5})/\mathbb{Q}(i)/\mathbb{Q}$.

Para definir $K = \mathbb{Q}(i)$ nós usamos o seu polinômio minimal. O comando Zx significa que o polinômio tem coeficientes em $\mathbb{Z}$.

```
# define o polinômio minimal|


Kash> p1:=Poly(Zx,[1,0,1])));
x^2+1
```

Agora podemos definir $\mathcal{O}_K$. Note que o comando OrderMaximal retorna o anel de inteiros.

```
# define o anel de inteiros de Q(sqrt{-1})

kash> O1:=OrderMaximal(p1);
```

```
Generating polynomial: $x^2 +1 $
Discriminant: -4

# encontra uma base integral

kash> OrderBasis(O1);
[1,[0,1]]
```

Observe que a base é dada com respeito a $\mathbb{Q}$-base, que é $\{1, \sqrt{-1}\}$, pois o polinômio minimal é $x^2 + 1$. Então $[a, b]$ significa $a + b\sqrt{-1}$.

```
# calcula os mergulhos

kash> OrderAutomorphisms(O1);

[[0,1],[0,-1]]
```

O primeiro mergulho é a identidade, o segundo é função $\sqrt{-1} \to -\sqrt{-1}$.

```
# escreve o segundo elemento da base integral

kash> b:=Elt(O1,[0,1]);
[0,1]
```

O comando EltAutomorphism(b,n) calcula um conjugado do elemento b, aplicando sobre ele o n-ésimo mergulho.

```
# calcula a matriz geradora do reticulado

kash> M1:=Mat(O1,[[0,1],[b,EltAutomorphism(b,2)]]);

[0,1]
[[0,1],[0,-1]]

# calcula seu determinante

kash> MatDet(M1);

[0,-1]
```

A matriz geradora pode ser obtida diretamente com o comando Lat.

```
kash> Lat(O1);
[1.414213562373095 0]
[0 1.414213562373095]
```

Construção da extensão $\mathbb{Q}(i,\sqrt{5})/\mathbb{Q}(i)$.

```
kash> zi:=OrderMaximal(Order(Poly(Zx,[1,0,1])));


Generating polynomial: $x^2 +1 $
Discriminant: -4

Zix:=PolyAlg(zi);

Univariate Polynomial Ring in x over Generating polynomial: x^2+1
Discriminant: -4

kash> ok:=OrderMaximal(Order(Poly(Zix,[1,0,-5])));

      F[1]
       |
      F[2]
        /
       /
   E1[1]
    |
   E1[2]
  /
 /
Q
F  [ 1]     Given by transformation matrix
F  [ 2]     x^2 -5
E 1[ 1]     x^2+1
E 1[ 2]
Discriminant: <5>
Coef. Ideals are: <1>, <1>
```

Procura um ideal de norma 5 na extensão absoluta $\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}$.

```
i5:=IdealFactor(5*ok)[1][1];
<5,[[9,1],[-5,3]]>

gen5:=IdealIsPrincipal(i5);
[1,[1,-1]]
```

Isso significa que o elemento de norma 5 é $\alpha = 1 + i - i\theta$, onde $\theta = \frac{1+\sqrt{5}}{2}$

6 Conclusão

Neste trabalho nos focamos na aplicação da teoria dos números algébricos para a construção do Código de Ouro, que é um STBC 2×2. Entretanto, existem outros contextos onde estes métodos algébricos são úteis. Por exemplo,

- reticulados densos para o canal gaussiano
- reticulados complexos para o canal com desvanecimento do tipo Rayleigh
- sistemas MIMO para mais antenas

Modelar códigos espaço-tempo eficientes para o sistema MIMO envolve mais do que saber o posto e o critério do determinante. Neste trabalho, detalhamos vários outros parâmetros que levam em conta a otimização da eficiência de códigos espaço-tempo, tal como forma da constelação, ganho de diversidade e multiplexagem e a propriedade de menor perda de informação. Na verdade, para construir códigos satisfazendo estas exigências, nós dependemos fortemente das estruturas algébricas das álgebras de divisão cíclicas baseadas em corpos de números e acreditamos que estas aproximações algébricas são muito promissoras para enfrentar novos problemas vindos de redes sem fio.

Uma aplicação do Código de Ouro proposta recentemente é usá-lo em redes sem fio para tráfego multimídia, que demanda esquemas de codificação com eficiência espectral muito alta, [21].

Referências

[1] Oggier,F. E., Rekaya, G., Belfiore, J.-C. & Viterbo, E. " Perfect space time block codes". *IEEE Transactions on Information Theory*, September 2006.

[2] I. N. Stewart and D. O. Tall "Algebraic Number Theory ". *Chapman and Hall*, 1979.

[3] Oggier,F. E., Belfiore, J.-C. & Viterbo, E. "Cyclic Division Algebras: A Tool for Space-Time Coding". *Communications and Information Theory*, Vol. 4, n.1, 2007.

[4] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras",*IEEE Trans. Inform. Theory*, vol. 49, pp. 2596 - 2616, October 2003.

[5] Conway, J.H. & Sloane, N.J.A. "Sphere Packings, Lattices and Groups. Springer-Verlag", New York, 1988.

[6] Oggier, F. & Viterbo, E. "Algebraic number theory and code design for Rayleigh fading channels". *Foundations and Trends in Communications and Information Theory*, vol. 1, 2004.

[7] Pierce, R.S. "Associative Algebras". *Springer-Verlag*, New York, 1982.

[8] Scharlau, W. "Quadratic and Hermitian Forms". *Springer Verlag*, 1985.

[9] Belfiore, J.-C., Rekaya, G. & Viterbo, E. "The golden code: A 2x2 full-rate space-time code with non-vanishing determinants."*IEEE Transactions on Information Theory*, vol. 51, no. 4, April 2005.

[10] Damen, M. O., Tewfik, A. & Belfiore, J.-C. "A construction of a space-time code based on number theory". *IEEE Trans.Inform. Theory*, 48:753-760, March 2002.

[11] Belfiore, J-C. & Cipriano, A.M. " Space-time coding for non-coherent channels". *Chapter 10 in Space-Time Wireless*, Cambridge University Press, June 2006.

[12] Hochwald, B. M. & Marzetta, T. L. "Unitary space-time modulation for multiple-antenna communications in Rayleigh flat fading", *IEEE Trans. Inform. Theory*, 46:543-564, March 2000.

[13] Tarokh, V., Seshadri, N. & Calderbank A.R. "Space-time block codes from orthogonal design". *IEEE Transactions on Information Theory*, 51(8), August 2005.

[14] Hernstein, V., Seshadri, N. & Calderbank A.R. "Space-time block codes from orthogonal design". *IEEE Transactions on Information Theory*, 51(8), August 2005.

[15] Howie, J. M. "Fields and Galois Theory". *Springer-Verlag*, London, 2006.

[16] Markowsky, G. "Misconceptions About The Golden Ratio". *College Mathematics Journal*, vol. 23, n. 1, pp. 2-19, 1992.

[17] Gardner, M. "Notes on a Fringe-Watcher: The Cult of the Golden Ratio.". *Skeptical Inquirer*, n. 18, pp. 243-247, 1994.

[18] Samuel, P. "Algebraic Theory of Numbers". *Hermana*, Paris, 1986.

[19] Darbekow, M., Fieker, C., Klüners, J., Pohst, M., Roegner, K. & Wildanger, K. "KASH 2.5" Disponível em: `http://page.math.tu-berlin.de/~kant/download.html`. Último acesso em: 18/08/2012.

[20] Gouvea, F.Q "p-adic Numbers: An Introduction." *Springer Verlag*, 1993.

[21] Viterbo, E., Yi Hong "Applications of the Golden Code". *Information Theory and Applications Workshop*, 2007.