UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de São José do Rio Preto

Eliton Mendonça Moro

Códigos de Bloco Espaço-Temporais via Corpos Quadráticos

São José do Rio Preto
2017

Eliton Mendonça Moro

Códigos de Bloco Espaço-Temporais via Corpos Quadráticos

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de São José do Rio Preto.

Financiadora: CAPES

Orientadora: Profa. Dra. Carina Alves
Depto. de Matemática, UNESP - Rio Claro

São José do Rio Preto
2017

Moro, Eliton Mendonça.
Códigos de bloco espaço-temporais via corpos quadráticos / Eliton Mendonça Moro. -- São José do Rio Preto, 2017
89 f. : il.

Orientador: Carina Alves
Dissertação (mestrado) – Universidade Estadual Paulista "Júlio de Mesquita Filho", Instituto de Biociências, Letras e Ciências Exatas

1. Matemática. 2. Álgebra. 3. Teoria da codificação. 4. Teoria dos sinais (Telecomunicações) 5. Sistemas MIMO. I. Universidade Estadual Paulista "Júlio de Mesquita Filho". Instituto de Biociências, Letras e Ciências Exatas. II. Título.

CDU – 512

Ficha catalográfica elaborada pela Biblioteca do IBILCE
UNESP - Câmpus de São José do Rio Preto

Eliton Mendonça Moro

Códigos de Bloco Espaço-Temporais via Corpos Quadráticos

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de São José do Rio Preto.

Financiadora: CAPES

Comissão Examinadora

Profa. Dra. Carina Alves
Depto. de Matemática, UNESP - Rio Claro
Orientadora

Prof. Dr. Antonio Aparecido de Andrade
Depto. de Matemática, UNESP - São José do Rio Preto

Prof. Dr. Edson Donizete de Carvalho
Depto. de Matemática, UNESP - Ilha Solteira

São José do Rio Preto
30 de Janeiro de 2017

Aos meus pais, Dorival P. M. Junior e Paula C. M. Moro, ao meu irmão Elton M. Moro e a minha namorada Tatiana K. Yamanouchi, dedico

Agradecimentos

Ao concluir este trabalho, agradeço:

À Profa. Dra. Carina Alves pelos 5 anos de orientação (graduação e mestrado), pela amizade, pelo incentivo, confiança, apoio, paciência e dedicação.

Aos professores do Departamento de Matemática da UNESP - São José do Rio Preto e Rio Claro, pela formação.

Aos meus colegas do curso de Pós-graduação e graduação, pela amizade.

Aos meus pais Dorival P. M. Junior e Paula C. M. Moro , meu irmão Elton M. Moro, a minha namorada Tatiana K. Yamanouchi e a toda minha família por me apoiar ao longo desse trajeto.

Ao pessoal da República Judeu Feliz pela amizade e convívio.

À Capes pelo auxílio financeiro.

À todos que direta ou indiretamente contribuíram para a realização deste trabalho.

"A desvalorização do mundo humano aumenta em proporção direta com a valorização do mundo das coisas."
Karl Marx

RESUMO

Os sistemas de comunicação com Múltiplas Entradas e Múltiplas Saídas (MIMO), são sistemas constituídos por estruturas que utilizam várias antenas, tanto no transmissor como no receptor. Por serem transmitidos via antenas, naturalmente surgem problemas de ruídos e de multipercursos, que impõe um desafio para o desenvolvimento dos sistemas de comunicação MIMO. Por esses motivos, muitos estudos focam em certas propriedades dos sinais enviados a fim de minimizar os efeitos sofridos na informação durante a transmissão. Existem muitos tipos diferentes de Códigos de Bloco Espaço-Temporais (STBC) disponíveis para duas antenas transmissoras, dentre eles, o código de bloco espaço-temporal ciclotômico, Código de Ouro e Código de Prata. Neste trabalho apresentamos uma construção de STBC cujos os sinais utilizados na transmissão são identificados por elementos de anéis de inteiros de corpos de números totalmente imaginários, $\mathbb{Q}(\sqrt{d})$, com $d < 0$, e apresentamos os melhores STBC em termos do critério que denominamos como critério produto, considerando extensões de $\mathbb{Q}(\sqrt{d})$ com $d = -1, -2, -3, -7, -11$.

Palavras-chave: Determinante mínimo, Corpos quadráticos, Códigos de bloco.

ABSTRACT

The communication systems of Multiple Input and Multiple Output (MIMO), are systems consisting of structures that use multiple antennas, both on the transmitter and the receiver. For being transmitted via antennas, noise and path problems naturally arise, which poses a challenge for the development and optimization of MIMO systems. For these reasons, many studies focus on certain properties of the signals sent in order to minimize the effects suffered on the information during transmission. There are many different types of Space-Time Block Codes (STBC) available for two transmitting antennas, such as the cyclotomic space-time block code, Golden Code, and Silver Code. In this work, we present a STBC construct via totally imaginary quadratic fields, $\mathbb{Q}$*, with* $d < 0$ *and present the best STBC in terms of the criterion that we call product criteria, considering extensions of* $\mathbb{Q}(\sqrt{d})$ *with* $d = -1,\ -2,\ -3,\ -7,\ -11$.

Keywords: Minimum determinant, Quadratic fields, Block codes.

Sumário

Capítulo 1

Introdução

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 o sinal se enfraqueça, além da perda natural de energia que ocorre durante a propagação da onda.

Para obter um bom resultado, uma opção é utilizar uma faixa de frequência grande, mas como as faixas de frequências são escassas e caras, essa opção não é viável. Um tipo de sistema que tem sido bastante utilizada e visto como muito promissor é o *Multiple Input Multiple Output* (MIMO), 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 de 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 construtivamente 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, haveriam $n_t \cdot n_r$ 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 a 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 consequentemente 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. Nesse contexto, as álgebras de divisão desempenham um importante papel, pois produzem naturalmente famílias de códigos com diversidade máxima, permitindo assim melhorar a confiabilidade da transmissão de sinais.

Vamos considerar, neste trabalho, códigos STBC com $n_t = 2$ antenas transmissoras e $n_r = 2$ antenas receptoras. Existem muitos tipos diferentes de códigos disponíveis para duas antenas transmissoras, como o código de bloco espaço-temporal ciclotômico [23], o código de ouro (*Golden Code*) [5] e o código de prata (*Silver Code*) [10]. Diversidade máxima (isto é, maior confiabilidade do sinal) e maior determinante mínimo (isto é, menor probabilidade de erro ponto a ponto) são os dois mais importantes critérios para construir bons STBC, [3]. Neste trabalho, apresentamos uma construção de STBC, com diversidade máxima, via corpos quadráticos totalmente imaginários, $\mathbb{Q}(\sqrt{d})$, com $d < 0$. Nestes corpos é possível mostrar que o determinante mínimo possui o valor constante igual a 1, conforme veremos no decorrer do trabalho.

A pergunta que surge então é: como avaliar tais códigos? A fim de responder esta questão, apresentamos um critério dado em [23] e que aqui chamamos de *critério produto*. Seguindo as ideias de [24], em que os autores apresentam os melhores STBC's em termos do critério produto considerando somente as extensões de $\mathbb{Q}(\sqrt{d})$ com $d = -1, -3$ sobre os racionais, apresentamos os melhores STBC's considerando extensões de $\mathbb{Q}(\sqrt{d})$ com $d = -2, -7, -11$. Dentre todas as extensões consideradas, analisamos o STBC ótimo segundo o critério mencionado. Além disso, reformulamos algumas demonstrações apresentadas em [24].

Dessa forma, o restante da dissertação está delineada na sequência que segue.

No Capítulo 2, apresentamos alguns resultados da teoria dos números algébricos,

corpos quadráticos e álgebras de divisão. O conceito de norma apresentado neste capítulo é fundamental para o desenvolvimento do trabalho. Os resultados sobre a teoria de corpos quadráticos são importantes, pois este será o corpo base para a construção dos STBC's. Para tal construção precisamos caracterizar os anéis de inteiros algébricos dos corpos quadráticos e os elementos dos ideais $(1+i)\mathbb{Z}[i]$ e $\sqrt{-3}\mathbb{Z}\left[\frac{1-\sqrt{-3}}{2}\right]$. Através desta caracterização provamos, no Capítulo 5, que certos elementos do anel de inteiros algébricos de $\mathbb{Q}(\sqrt{d})$ não são normas algébricas de uma extensão de $\mathbb{Q}(\sqrt{d})$. Além disso, definimos álgebra dos quatérnios e álgebras de divisão, que produzem naturalmente famílias de STBC's lineares.

No Capítulo 3, abordamos resultados e definições sobre reticulados, empacotamento esférico e apresentamos uma construção algébrica de reticulados via corpos quadráticos. A teoria da Seção 3.3 é necessária para compreender o critério de comparação que é apresentado no Capítulo 5.

No Capítulo 4, apresentamos a teoria de números p-ádicos e o Lema de Hensel, que possui importantes aplicações aos STBC's, por exemplo, nas construções do Golden Code e do Silver Code. Este lema fornece ferramentas para mostrar que certos elementos do anel de inteiros algébricos de $\mathbb{Q}(\sqrt{d})$ não são normas algébricas de uma extensão de $\mathbb{Q}(\sqrt{d})$. Neste trabalho, uma de nossas contribuições inéditas é mostrar que, se $d \equiv 1 \ (mod\ 3)$, então -1 não é norma algébrica de $\mathbb{Q}(\sqrt{d}, \sqrt{-3})$ sobre $\mathbb{Q}(\sqrt{d})$, e se $d \equiv 1 \ (mod\ 8)$, então -1 não é norma algébrica de $\mathbb{Q}(\sqrt{d}, \sqrt{i})$ sobre $\mathbb{Q}(\sqrt{d})$.

No Capítulo 5, introduzimos o modelo do canal MIMO, apresentamos critérios para modelar códigos espaço-temporais, definimos o determinante mínimo de um código, o ganho de codificação e avaliamos a probabilidade de erro. Ainda neste capítulo, apresentamos uma construção de códigos de bloco espaço-temporais via corpos quadráticos, considerando extensões quadráticas de um corpo de números. Além disso, apresentamos os melhores códigos nos corpos bases $\mathbb{Q}(\sqrt{d})$, com $d = -1, -2, -3, -7, -11$, segundo o *critério produto*. Os melhores códigos sobre $\mathbb{Q}(\sqrt{d})$, com $d = -2, -7$ e -11 são contribuições originais de nosso trabalho.

Capítulo 2

Preliminares

Nosso objetivo, neste capítulo, é introduzir resultados e definições de teoria dos números algébricos e álgebras dos quatérnios que utilizamos como ferramentas no decorrer dos próximos capítulos. Deste modo, apresentamos resultados sobre extensões de corpos, elemento algébrico, homomorfismo, norma e traço, corpos quadráticos, base integral, discriminante e álgebra dos quatérnios. Para o desenvolvimento deste capítulo as principais referências utilizadas foram [16], [19], [13], [14], [3], [4], [10] e [22]. Alguns resultados seguem sem demonstrações por se tratarem de resultados elementares ou por utilizar resultados que não estão dentro dos objetivos desse trabalho.

2.1 Módulos

Abordamos aqui as definições de módulos e submódulos que serão necessárias no contexto de reticulados, tema que será apresentado no Capítulo 3. No que segue, consideremos A sendo um anel comutativo com unidade.

Definição 2.1.1. Um A**-módulo** M é um grupo abeliano aditivo M equipado com uma aplicação $A \times M \to M$ definida por $(a, m) \mapsto am$ tal que para todo $a, a' \in A$ e todo $m, m' \in M$ tem-se que

- $(aa')m = a(a'm)$,
- $(a + a')m = am + a'm$,
- $a(m + m') = am + am'$,
- $1m = m$.

Definição 2.1.2. Seja 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.

Definição 2.1.3. Um A-módulo M é dito **finitamente gerado** se existir $x_1, \ldots, x_r \in M$ tal que $M = Ax_1 + \ldots + Ax_r$ e, neste caso, dizemos que $\{x_1, \ldots, x_r\}$ forma um sistema de geradores de M. Se $\{x_1, \ldots, x_r\}$ for linearmente independente sobre A, dizemos que $\{x_1, \ldots, x_r\}$ forma um **base** de M sobre A. E caso exista uma base,

diremos que M é um A-**módulo livre**, e o número de elementos da base é chamado de **posto** de M.

Observação 2.1.4. Nem sempre um A-submódulo N de um A-módulo livre M é livre. Para isso, basta tomarmos $M = A = \mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Temos que $\mathbb{Z}_6$ é um $\mathbb{Z}_6$-módulo livre com base $\{\overline{1}\}$, mas o $\mathbb{Z}_6$-submódulo $N = \{\overline{0}, \overline{2}, \overline{4}\}$ não é livre, visto que qualquer sistemas de geradores que tomarmos para N não é linearmente independente.

Observação 2.1.5. Nem todo módulo finitamente gerado possui uma base. Por exemplo, o anel $\mathbb{Z}_6$ é um $\mathbb{Z}$-módulo finitamente gerado, mas não é livre, pois qualquer sistema de geradores de $\mathbb{Z}_6$ não é linearmente independente.

2.2 Extensões de corpos e elemento algébrico

Nesta seção, apresentamos os conceitos de extensões de corpos e elemento algébrico. Além disso, apresentamos alguns resultados envolvendo estes conceitos.

Definição 2.2.1. Sejam $\mathbb{F}$ e $\mathbb{K}$ corpos. Dizemos que $\mathbb{K}$ é uma **extensão** de $\mathbb{F}$ se $\mathbb{F} \subset \mathbb{K}$. Notação: $\mathbb{K}/\mathbb{F}$.

Observação 2.2.2. Seja $\mathbb{F} \subset \mathbb{K}$ uma extensão de corpos. Pode-se verificar que $\mathbb{K}$ é um $\mathbb{F}$-espaço vetorial, assim, existe uma base de $\mathbb{K}$ sobre $\mathbb{F}$.

Definição 2.2.3. Seja $\mathbb{F} \subset \mathbb{K}$ uma extensão de corpos.

(i) A dimensão do $\mathbb{F}$-espaço vetorial $\mathbb{L}$ é o número de elementos da base de $\mathbb{K}$ sobre $\mathbb{F}$, chamada de **grau da extensão** de $\mathbb{K}$ sobre $\mathbb{F}$ e denotada por $[\mathbb{K} : \mathbb{F}]$.

(ii) Dizemos que $\mathbb{K}$ é uma extensão finita de $\mathbb{F}$ se $[\mathbb{K} : \mathbb{F}]$ é finito, caso contrário, $\mathbb{K}$ é uma extensão infinita.

Definição 2.2.4. Um **corpo de números** $\mathbb{F}$ é uma extensão finita de $\mathbb{Q}$.

Observação 2.2.5. Os corpos de números $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$, onde $i = \sqrt{-1}$ 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 $\mathbb{Z}$, obtemos o conjunto dos inteiros Gaussianos $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ e o conjunto dos inteiros de Eiseinstein $\mathbb{Z}[j] = \{a + bj \mid a, b \in \mathbb{Z}\}$.

Definição 2.2.6. Seja $\mathbb{F}$ um corpo. Chamamos de **polinômio** sobre $\mathbb{F}$ em uma indeterminada x a uma expressão formal $p(x) = a_0 + a_1x + \ldots + a_nx^n$ onde $a_i \in \mathbb{F}$ para todo $i = 1, \ldots, n$. Se $a_n \neq 0$, então o grau de $p(x)$ é definido como n.

Denotamos por $\mathbb{F}[x]$ o **conjunto de todos os polinômios** sobre $\mathbb{F}$, em uma indeterminada x.

Observe que não está definido o grau do polinômio nulo e considere ∂ como uma função definida por

$$\begin{array}{rcl} \partial : \mathbb{F}[x] - \{0\} & \to & \mathbb{N} \\ p(x) & \mapsto & \partial p(x) = grau\ de\ p(x) \end{array}$$

Definição 2.2.7. Seja $f(x) \in \mathbb{F}[x]$ tal que $\partial f(x) \geq 1$. Dizemos que $f(x)$ é um **polinômio irredutível** sobre $\mathbb{F}$ se toda vez que $f(x) = g(x)h(x)$ onde $g(x), h(x) \in \mathbb{F}[x]$. implica que $g(x) = a$ constante em $\mathbb{F}$ ou $h(x) = b$ constante em $\mathbb{F}$. Se $f(x)$ não for irredutível sobre $\mathbb{F}$, dizemos que $f(x)$ é redutível sobre $\mathbb{F}$.

Definição 2.2.8. Sejam $\mathbb{F} \subset \mathbb{K}$ corpos. Um elemento $\alpha \in \mathbb{K}$ é chamado de **algébrico** sobre $\mathbb{F}$ se existe $f(x) \in \mathbb{F}[x]/\{0\}$ tal que $f(\alpha) = 0$.

Proposição 2.2.9. Sejam $\mathbb{F} \subset \mathbb{K}$ corpos. Se $\alpha \in \mathbb{K}$ é algébrico sobre $\mathbb{F}$, então existe um único polinômio irredutível e mônico de menor grau $f(x) \in \mathbb{F}[x]$ tal que $f(\alpha) = 0$.

Demonstração. Se $\alpha \in \mathbb{K}$ é algébrico sobre $\mathbb{F}$, então existe um polinômio $g(x) = a_0 + \cdots + a_n x^n \in \mathbb{F}[x]/\{0\}$ tal que $g(\alpha) = 0$. Tomando $f(x) = a_n^{-1} g(x) \in \mathbb{F}[x]$, temos que $f(x) \in \mathbb{F}[x]$ é um polinômio mônico tal que $f(\alpha) = 0$. Suponhamos que existam $f(x), g(x) \in \mathbb{F}[x]$ irredutíveis e mônicos de menor grau tal que $f(\alpha) = g(\alpha) = 0$, com $f(x) \neq g(x)$. Como $f(x)$ e $g(x)$ são os polinômio de menor grau tal que $f(\alpha) = g(\alpha) = 0$, com $\partial f(x) = \partial g(x) = n$, segue que $0 \leq \partial(f(x) - g(x)) \leq n - 1$, com $f(\alpha) - g(\alpha) = 0$, o que é um absurdo, pois $f(x)$ e $g(x)$ são os polinômios de menor grau tal que $f(\alpha) = g(\alpha) = 0$. Portanto, provamos o resultado. □

Definição 2.2.10. Sejam $\mathbb{F} \subset \mathbb{K}$ corpos e $\alpha \in \mathbb{K}$. O polinômio irredutível e mônico de menor grau $f(x)$ tal que $f(\alpha) = 0$ é chamado de **polinômio minimal** de α sobre $\mathbb{F}$ e é denotado por $min_{\mathbb{F}}\alpha$.

Lema 2.2.11. Sejam $\mathbb{F} \subset \mathbb{K}$ corpos e $\alpha \in \mathbb{K}$ é algébrico sobre $\mathbb{F}$, então o polinômio minimal de α divide todo polinômio $h(x) \in \mathbb{F}[x] - \{0\}$ tal que $h(\alpha) = 0$.

Demonstração. Sejam $f(x)$ o polinômio minimal de α e $h(x) \in \mathbb{F}[x]$ tal que $h(\alpha) = 0$. Usando o algoritmo da divisão de polinômios, podemos escrever que $h(x) = q(x)f(x) + r(x)$, onde $0 \leq \partial r(x) < \partial f(x)$. Assim,

$$r(\alpha) = h(\alpha) - q(\alpha)f(\alpha) = 0,$$

ou seja, α é raiz de $r(x)$. Contudo, como $f(x)$ é o polinômio minimal de menor grau que tem α como raiz, segue que $r(x) = 0$. Logo, $f(x)$ divide $h(x)$. □

Definição 2.2.12. Uma extensão $\mathbb{K}$ sobre $\mathbb{F}$ é **algébrica** se todo $\alpha \in \mathbb{K}$ é algébrico sobre $\mathbb{F}$.

Exemplo 2.2.13. Vamos verificar que a extensão $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$ é algébrica. De fato, se $\alpha \in \mathbb{Q}(\sqrt{2})$, então $\alpha = a + b\sqrt{2}$, com $a, b \in \mathbb{Q}$. Assim, $(\alpha - a)^2 = 2b^2$, ou seja, $\alpha^2 - 2a\alpha + a^2 - 2b^2 = 0$. Logo, α é raiz de $f(x) = x^2 - 2ax + a^2 - 2b^2 \in \mathbb{Q}[x]$ e dessa forma, α é algébrico sobre $\mathbb{Q}$. Portanto, a extensão $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ é algébrica.

Definição 2.2.14. Dizemos que $\alpha \in \mathbb{C}$ é **inteiro algébrico** se existe $f(x) \in \mathbb{Z}[x] \setminus \{0\}$, mônico, tal que $f(\alpha) = 0$. Seja $\mathbb{F}$ um corpo tal que $\mathbb{Q} \subset \mathbb{F}$, o conjunto $\mathcal{O}_{\mathbb{F}} = \{\alpha \in \mathbb{F} \mid \alpha \text{ é inteiro algébrico}\}$ é um anel chamado de **anel dos inteiros algébricos de** $\mathbb{F}$.

Exemplo 2.2.15. O elemento $\alpha = \sqrt{2} + \sqrt{5}$ é inteiro algébrico, pois é raiz do polinômio $x^4 - 14x^2 + 9 \in \mathbb{Z}[x]$.

Observação 2.2.16. Se $\mathbb{F} = \mathbb{Q}$, então $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}$. Contudo, há elementos de $\mathbb{R}$ que não pertencem a $\mathbb{Z}$, mas ainda são inteiros algébricos. Por exemplo,

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

é um inteiro algébrico, pois é raiz do polinômio $x^2 - x - 1$.

Teorema 2.2.17. (Teorema da multiplicatividade dos graus) Se $\mathbb{F}$, $\mathbb{K}$ e $\mathbb{L}$ são corpos tais que $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ e $[\mathbb{L} : \mathbb{F}]$ é finita, então $[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}]\,[\mathbb{K} : \mathbb{F}]$.

Demonstração. Suponha que $[\mathbb{L} : \mathbb{K}] = m$ e $[\mathbb{K} : \mathbb{F}] = n$. Se $B_1 = \{\alpha_1, \ldots, \alpha_m\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ e $B_2 = \{\beta_1, \ldots, \beta_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{F}$, então $B = \{\alpha_i\beta_j, i = 1, \ldots, m \text{ e } j = 1, \ldots, n\}$ é uma base de $\mathbb{L}/\mathbb{F}$, uma vez que

1. O conjunto gerado por B, $[B]$, é $\mathbb{L}$. De fato, se $\alpha \in \mathbb{L}$, então existem $a_1, a_2, \cdots, a_m \in \mathbb{K}$ tais que $\alpha = \sum_{i=1}^{m} a_i\alpha_i$. Por outro lado, se $a_i \in \mathbb{K}$, então existem $b_{i1}, b_{i2}, \cdots, b_{in} \in \mathbb{F}$ tais que $a_i = \sum_{j=1}^{n} b_{ij}\beta_j$. Logo, $\alpha = \sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}\alpha_i\beta_j$, e assim $\mathbb{L} \subset [B]$. Como $[B] \subset \mathbb{L}$, segue que $[B] = \mathbb{L}$.

2. B é linearmente independente sobre $\mathbb{F}$. De fato, suponha que $\sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}\alpha_i\beta_j = 0$, então $\sum_{i=1}^{m}\left(\sum_{j=1}^{n} b_{ij}\beta_j\right)\alpha_i = 0$. Como B_1 é linearmente independente sobre $\mathbb{K}$, segue que $\sum_{j=1}^{n} b_{ij}\beta_j = 0$, e como B_2 é linearmente independente sobre $\mathbb{F}$, segue que $b_{ij} = 0$, para todo i, j.

Portanto, B é uma base de $\mathbb{L}/\mathbb{F}$ com mn elementos. Assim, $[\mathbb{L} : \mathbb{F}] = mn = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}]$. □

Exemplo 2.2.18. Vejamos como 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 $\mathbb{Q}$. Da Teoria de Corpos, segue que $\mathbb{Q}(\sqrt{2}) = \{\alpha + \beta\sqrt{2} : \alpha, \beta \in \mathbb{Q}\}$. Assim, se $x \in \mathbb{Q}(\sqrt{2})$ então $x = \alpha 1 + \beta\sqrt{2}$, com $\alpha, \beta \in \mathbb{Q}$, ou seja, x é combinação linear de $\{1, \sqrt{2}\}$.

2. $\{1, \sqrt{2}\}$ é linearmente independente sobre $\mathbb{Q}$. Suponha que $\alpha 1 + \beta\sqrt{2} = 0$, com $\alpha, \beta, \in \mathbb{Q}$. Se $\beta \neq 0$, então $\sqrt{2} = \frac{-\alpha}{\beta}$, o que é um absurdo pois $\sqrt{2}$ é irracional. Portanto, $\beta = 0$, e assim, $\alpha 1 + 0\sqrt{2} = 0$, ou seja, $\alpha = 0$. 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 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$. De fato,

1. $\{1, \sqrt{3}\}$ gera $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$. Da Teoria de Corpos, segue que $\mathbb{Q}(\sqrt{3}, \sqrt{2}) = \{\alpha + \beta\sqrt{3} : \alpha, \beta \in \mathbb{Q}(\sqrt{2})\}$. Assim, se $x \in \mathbb{Q}(\sqrt{3}, \sqrt{2})$ então $x = \alpha 1 + \beta\sqrt{3}$, com $\alpha, \beta \in \mathbb{Q}(\sqrt{2})$, ou seja, x é combinação linear de $\{1, \sqrt{3}\}$.

2. $\{1, \sqrt{3}\}$ é linearmente independente sobre $\mathbb{Q}(\sqrt{2})$. Suponha que $\alpha 1 + \beta\sqrt{3} = 0$, com $\alpha, \beta, \in \mathbb{Q}(\sqrt{2})$. Assim, podemos reescrever a igualdade como $(p + q\sqrt{2}) + (r + s\sqrt{2})\sqrt{3} = 0$, com $p, q, r\, e\, s \in \mathbb{Q}$. Se $\beta = (r + s\sqrt{2}) \neq 0$, então

$$\begin{aligned}\sqrt{3} &= \frac{-(p+q\sqrt{2})}{r+s\sqrt{2}} = \frac{-(p+q\sqrt{2})}{r+s\sqrt{2}} \cdot \frac{r-s\sqrt{2}}{r-s\sqrt{2}} \\ &= \frac{-(pr - ps\sqrt{2} + qr\sqrt{2} - 2qs)}{r^2 - 2s^2} = \frac{-pr + 2qs + (ps - qr)\sqrt{2}}{r^2 - 2s^2} \\ &= \frac{-pr + 2qs}{r^2 - 2s^2} + \frac{(ps - qr)\sqrt{2}}{r^2 - 2s^2} = a + b\sqrt{2},\ a, b \in \mathbb{Q}.\end{aligned}$$

Assim, $(\sqrt{3})^2 = (a + b\sqrt{2})^2$, ou seja, $3 = a^2 + 2ab\sqrt{2} + 2b^2$. Logo $3 - a^2 - 2b^2 = 2ab\sqrt{2}$, isto é, $\dfrac{3 - a^2 - 2b^2}{2ab} = \sqrt{2}$,

o que é absurdo pois $\sqrt{2}$ é irracional. Portanto, $r + s\sqrt{2} = \beta = 0$, e assim, $p + q\sqrt{2} + 0\sqrt{3} = 0$, ou seja $p + q\sqrt{2} = \alpha = 0$. Dessa forma, $\{1, \sqrt{3}\}$ é uma base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$. Logo $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$.

Pelo Teorema da multiplicatividade dos graus 2.2.17, segue que

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

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

Teorema 2.2.19. [19] Se $\mathbb{Q} \subset \mathbb{F} \subset \mathbb{K}$, com $[\mathbb{K} : \mathbb{F}] < \infty$, então existe $\theta \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{F}(\theta)$. O elemento θ é chamado **elemento primitivo**.

Proposição 2.2.20. [19] Se $\mathbb{F}$ é um corpo de números tal que $\mathbb{F} = \mathbb{Q}(\theta)$, então $[\mathbb{F} : \mathbb{Q}] = \partial(min_{\mathbb{Q}}\theta)$.

Exemplo 2.2.21. Se $\mathbb{F} = \mathbb{Q}(\sqrt{7})$, então $[\mathbb{F} : \mathbb{Q}] = 2$, pois $min_{\mathbb{Q}}(\sqrt{7}) = x^2 - 7$.

Observação 2.2.22. Se $\mathbb{K} = \mathbb{F}(\theta)$ e $\partial(min_{\mathbb{F}}\theta) = n$, então $\mathbb{F}(\theta) = \{a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}; a_i \in \mathbb{F},$ para qualquer $i = 0, 1, \cdots, n-1\}$.

Definição 2.2.23. Seja $\mathbb{F} \subset \mathbb{K}$ uma extensão de corpos. Se σ é um monomorfismo de $\mathbb{K}$ tal que $\sigma(\alpha) = \alpha$ para todo $\alpha \in \mathbb{F}$, então σ é chamado de **$\mathbb{F}$-monomorfismo** de $\mathbb{K}$. Se σ é um $\mathbb{F}$-isomorfismo de $\mathbb{K} = \mathbb{F}(\alpha)$ então $\sigma(\alpha)$ é chamado de **conjugado** de α sobre $\mathbb{F}$.

Teorema 2.2.24. [14] Se $\mathbb{F} = \mathbb{Q}(\theta)$ é uma extensão de $\mathbb{Q}$ de grau n, então existem exatamente n monomorfismos distintos $\{\sigma_1, ..., \sigma_n\}$ de $\mathbb{F}$ em $\mathbb{C}$ que fixam $\mathbb{Q}$. Tais monomorfismos são dados por $\sigma_i(\theta) = \theta_i$, em que $\{\theta_1, ..., \theta_n\}$ são as raízes de $min_{\mathbb{Q}}\theta$ em $\mathbb{C}$.

Exemplo 2.2.25. Considere o corpo $\mathbb{Q}(\sqrt[3]{7})$. O polinômio minimal de $\sqrt[3]{7}$ sobre $\mathbb{Q}$ é $f(x) = x^3 - 7$. As raízes de $f(x)$ são $\{\sqrt[3]{7}, \omega\sqrt[3]{7}, \omega^2\sqrt[3]{7}\}$, em que $\omega = cos\left(\frac{2\pi}{7}\right) + isen\left(\frac{2\pi}{7}\right)$. Assim, existem três monomorfismos:

$$\begin{array}{rccc}\sigma_1: & \mathbb{Q}(\sqrt[3]{7}) & \to & \mathbb{C} \\ & \sqrt[3]{7} & \mapsto & \sqrt[3]{7} \\ \sigma_2: & \mathbb{Q}(\sqrt[3]{7}) & \to & \mathbb{C} \\ & \sqrt[3]{7} & \mapsto & \omega\sqrt[3]{7} \\ \sigma_3: & \mathbb{Q}(\sqrt[3]{7}) & \to & \mathbb{C} \\ & \sqrt[3]{7} & \mapsto & \omega^2\sqrt[3]{7}.\end{array}$$

Definição 2.2.26. Sejam $\mathbb{F}$ um corpo de números de grau n e $\{\sigma_1, ..., \sigma_n\}$ os n $\mathbb{Q}$-monomorfismos distintos de $\mathbb{F}$ em $\mathbb{C}$. Dizemos que o monomorfismo σ_i é **real** se $\sigma_i(\mathbb{F}) \subset \mathbb{R}$, caso contrário, dizemos que σ_i é **imaginário**. Além disso, se todos os $\sigma_i^{'}s$, para $i = 1, ..., n$, são reais, dizemos que o corpo $\mathbb{F}$ é **totalmente real** e, se todos os $\sigma_i^{'}s$, para $i = 1, ..., n$, são imaginários, dizemos que $\mathbb{F}$ é **totalmente imaginário**.

2.3 Norma e traço

Nesta seção, apresentamos os conceitos de norma e traço e algumas de suas propriedades. A teoria apresentada aqui será essencial para o desenvolvimento da teoria de base integral e discriminante, que será abordada na Seção 2.5, e também para a obtenção dos resultados do Capítulo 5.

Sejam A um anel e B um A-módulo livre de posto n. Em particular, podemos tomar A e B corpos tal que B é uma extensão de grau n sobre A. Sejam $\psi_\alpha : B \to B$ um endomorfismo de anéis definido por $\psi_\alpha(x) = \alpha x$, onde $\alpha \in B$ e $\{e_1, \ldots, e_n\}$ é uma base de B sobre A. Assim,

$$\begin{cases} \psi_\alpha(e_1) = a_{11}e_1 + \ldots + a_{1n}e_n \\ \quad\vdots \qquad\qquad \vdots \\ \psi_\alpha(e_n) = a_{n1}e_1 + \ldots + a_{nn}e_n \end{cases},$$

com $a_{ij} \in A$, para todo $i, j = 1, \ldots, n$. Assim,

$$\begin{pmatrix} \psi_\alpha(e_1) \\ \vdots \\ \psi_\alpha(e_n) \end{pmatrix} = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix} \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}.$$

Definição 2.3.1. O **traço** de α é definido por $Tr_{B/A}(\alpha) = \sum_{i=1}^{n} a_{ii}$, a **norma** de α é definida por $N_{B/A}(\alpha) = det(a_{ij})$ e o **polinômio característico** de α é definido por $g(x) = det(xI - a_{ij}) = det(x\delta_{ij} - a_{ij})$, onde $\delta_{ij} = 1$ se $i = j$ e 0, caso contrário.

Usamos a notação $Tr_{B/A}(\alpha), N_{B/A}(\alpha)$, ou simplesmente, $Tr(\alpha), N(\alpha)$ quando não houver dúvidas.

Proposição 2.3.2. [16] Sejam $\mathbb{F}$ um corpo de característica zero ou um corpo finito, $\mathbb{K}$ uma extensão algébrica de $\mathbb{F}$ de grau n, e α um elemento de $\mathbb{K}$. Se $\alpha_1, \ldots, \alpha_n$ são as raízes do polinômio minimal de α sobre $\mathbb{F}$, então

$$Tr_{\mathbb{K}/\mathbb{F}}(\alpha) = \alpha_1 + \ldots + \alpha_n,\ N_{\mathbb{K}/\mathbb{F}}(\alpha) = \alpha_1 \ldots \alpha_n \text{ e } g(x) = (x - \alpha_1) \ldots (x - \alpha_n).$$

Demonstração. Consideremos, primeiramente, o caso em que α é um elemento primitivo de $\mathbb{K}$ sobre $\mathbb{F}$. Se $f(x)$ é o polinômio minimal de α sobre $\mathbb{F}$, então $\mathbb{K}$ é $\mathbb{F}$-isomorfo ao anel quociente $\frac{\mathbb{F}[x]}{<f(x)>}$ e $\{1, \ldots, \alpha^{n-1}\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{F}$. Tomando $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$, com $a_i \in \mathbb{F}$, segue que a matriz do endomorfismo ψ_α com respeito a esta base é dada por

$$M = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}, \text{ onde } \begin{cases} \psi(e_1) = a_{11}e_1 + \ldots + a_{1n}e_n \\ \qquad\vdots \qquad\qquad\qquad \vdots \\ \psi(e_n) = a_{n1}e_1 + \ldots + a_{nn}e_n \end{cases}$$

Assim, $det(xI - \psi_\alpha)$ é o determinante da matriz

$$xI_n - M = \begin{pmatrix} x & 0 & \cdots & 0 & a_0 \\ -1 & x & \cdots & 0 & a_1 \\ 0 & -1 & \cdots & 0 & a_2 \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & -1 & x + a_{n-1} \end{pmatrix}.$$

Expandindo esse determinante como um polinômio em x, obtemos o polinômio característico $g(x)$ de α, que é igual a $f(x)$, assim, $Tr(\alpha) = -a_{n-1}$ e $N(\alpha) = (-1)^n a_0$. Como α é primitivo, segue que $f(x) = (x - \alpha_1)\ldots(x - \alpha_n)$ e igualando os coeficientes segue que $Tr(\alpha) = \alpha_1 + \ldots + \alpha_n$ e $N(\alpha) = \alpha_1 \ldots \alpha_n$. Consideramos, agora, o caso geral. Se $r = [\mathbb{K} : \mathbb{F}(\alpha)]$, é suficiente mostrarmos que o polinômio característico $g(x)$ de α, com relação a $\mathbb{K}$ sobre $\mathbb{F}$ é igual a r-ésima potência do polinômio minimal de α sobre $\mathbb{F}$. Se $\{y_i\}_{i=1,\ldots,q}$ é uma base de $\mathbb{F}(\alpha)$ sobre $\mathbb{F}$ e se $\{z_j\}_{j=1,\ldots,r}$ é uma base de $\mathbb{K}$ sobre $\mathbb{F}(\alpha)$, então $\{y_i z_j\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{F}$ com $n = qr$. Se $M = (a_{ih})$ é a matriz de multiplicação por α em $\mathbb{F}(\alpha)$ com relação a base $\{y_i\}$, então $\alpha y_i = \sum_h a_{ih} y_h$. Assim, $\alpha(y_i z_j) = \left(\sum_h a_{ih} y_h\right) z_j = \sum_h a_{ih}(y_h z_j)$. Logo,

$$\begin{cases} \alpha y_1 z_1 &= a_{11}y_1z_1 + a_{12}y_1z_1 + \ldots + a_{1q}y_qz_1 \\ \alpha y_2 z_1 &= a_{21}y_1z_1 + a_{22}y_1z_1 + \ldots + a_{2q}y_qz_1 \\ \quad\vdots & \qquad\qquad\qquad \vdots \\ \alpha y_q z_1 &= a_{q1}y_1z_1 + a_{q2}y_1z_1 + \ldots + a_{qq}y_qz_1 \end{cases}.$$

Assim, a matriz do endomorfismo de α em $\mathbb{L}$ com relação a base $\{y_i z_j\}$, ordenada lexicograficamente, é dada por

$$M_1 = \begin{pmatrix} M & 0 & \ldots & 0 \\ 0 & M & \ldots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & M \end{pmatrix},$$

isto é, M aparece r-vezes na diagonal como blocos na matriz M_1. Daí, a matriz $xI - M_1$ consiste de r blocos diagonais, cada um tem a forma $xI_q - M$, e consequentemente, $det(xI_n - M_1) = det(xI_q - M_1)^r$. Assim $g(x) = det(xI_q - M)$ e $det(xI_q - M)$ é o polinômio característico de α sobre $\mathbb{F}$, de acordo com a primeira parte da demonstração. □

Exemplo 2.3.3. Considere um polinômio irredutível

$$f(x) = ax^2 + bx + c \in \mathbb{Q}[x],$$

onde $a \neq 0$. As raízes de $f(x)$ são dadas por

$$\alpha = \frac{-b+\sqrt{\Delta}}{2a} \quad e \quad \alpha^{'} = \frac{-b-\sqrt{\Delta}}{2a},$$

onde $\Delta = b^2 - 4ac$ é o discriminante do corpo quadrático $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\Delta})$. Portanto,

$$Tr_{\mathbb{F}/\mathbb{Q}}(\alpha) = \alpha + \alpha^{'} = \frac{-b+\sqrt{\Delta}}{2a} + \frac{-b-\sqrt{\Delta}}{2a} = -\frac{b}{a}$$

e

$$N_{\mathbb{F}/\mathbb{Q}}(\alpha) = \alpha\alpha^{'} = \left(\frac{-b+\sqrt{\Delta}}{2a}\right)\left(\frac{-b-\sqrt{\Delta}}{2a}\right) = \frac{b^2-\Delta}{4a^2} = \frac{c}{a}.$$

Assim, o polinômio minimal de α sobre $\mathbb{Q}$ é $min_{\mathbb{Q}}\alpha = x^2 - Tr_{\mathbb{F}/\mathbb{Q}}(\alpha)x + N_{\mathbb{F}/\mathbb{Q}}(\alpha)$.

Se $\mathbb{F} \subset \mathbb{K}$ é uma extensão finita de corpos de números, então valem as seguintes propriedades:

1. $Tr_{\mathbb{K}/\mathbb{F}}(\alpha + \alpha') = Tr_{\mathbb{K}/\mathbb{F}}(\alpha) + Tr_{\mathbb{K}/\mathbb{F}}(\alpha')$,
2. $Tr_{\mathbb{K}/\mathbb{F}}(a\alpha) = aTr_{\mathbb{K}/\mathbb{F}}(\alpha)$,
3. $Tr_{\mathbb{K}/\mathbb{F}}(a) = [\mathbb{K} : \mathbb{F}]a$,
4. $N_{\mathbb{K}/\mathbb{F}}(\alpha\alpha') = N_{\mathbb{K}/\mathbb{F}}(\alpha)N_{\mathbb{K}/\mathbb{F}}(\alpha')$,
5. $N_{\mathbb{K}/\mathbb{F}}(a) = a^{[\mathbb{K}:\mathbb{F}]}$,
6. $N_{\mathbb{K}/\mathbb{F}}(a\alpha) = a^{[\mathbb{K}:\mathbb{F}]}N_{\mathbb{K}/\mathbb{F}}(\alpha)$.

com α, $\alpha^{'} \in \mathbb{K}$ e $a \in \mathbb{F}$.

Definição 2.3.4. Sejam $A \subset B$ anéis. Dizemos que um elemento $\alpha \in B$ é inteiro sobre A, se existem $a_0, \ldots, a_{n-1} \in A$, não todos nulos, tal que

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Proposição 2.3.5. [16] Sejam A um domínio, $\mathbb{F}$ seu corpo de frações com característica zero, e $\mathbb{K}$ uma extensão de $\mathbb{F}$. Se α um elemento de $\mathbb{K}$ inteiro sobre A, então os coeficientes do polinômio característico, $g(x)$, de α são inteiros sobre A. Em particular, $Tr_{\mathbb{K}/\mathbb{F}}(\alpha)$ e $N_{\mathbb{K}/\mathbb{F}}(\alpha)$, são inteiros sobre A.

Demonstração. Como $g(x) = (x - \alpha_1)\ldots(x - \alpha_n)$ e como os coeficientes de $g(x)$ a menos de sinal, são somas de produtos dos $\alpha_i^{'}s$, é suficiente mostrarmos que cada α_i é inteiro sobre A. Mas, cada α_i é um conjugado de α sobre $\mathbb{F}$, ou seja, existe um $\mathbb{F}$-*isomorfismo* $\sigma_i : \mathbb{F}(\alpha) \to \mathbb{F}(\alpha_i)$ tal que $\sigma_i(\alpha) = \alpha_i$. Como α é inteiro sobre A, segue que

$$\alpha_n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0,$$

com $a_i \in A$ não todos nulos, para $i = 1, \ldots, n$. Aplicando σ_i, obtemos

$$\sigma_i(\alpha)^n + a_{n-1}\sigma_i(\alpha)^{n-1} + \ldots + a_1\sigma_i(\alpha) + a_0 = 0,$$

ou seja, $\sigma_i(\alpha) = \alpha_i$ é inteiro sobre A, e portanto, $Tr_{\mathbb{K}/\mathbb{F}}(\alpha)$ e $N_{\mathbb{K}/\mathbb{F}}(\alpha)$, são inteiros sobre A. □

Corolário 2.3.6. [16] Nas condições da Proposição 2.3.5, se $A = \mathcal{O}_{\mathbb{F}}$, então os coeficientes do polinômio característico de α, em particular, $Tr_{\mathbb{K}/\mathbb{F}}(\alpha)$ e $N_{\mathbb{K}/\mathbb{F}}(\alpha)$, são elementos de A.

Demonstração. Por definição, esses coeficientes são elementos de $\mathbb{F}$. Pela Proposição 2.3.5 são inteiros sobre A. Logo, são elementos de A, pois $A = \mathcal{O}_{\mathbb{F}}$. □

Observação 2.3.7. Pela Proposição 2.3.5, segue que $Tr_{\mathbb{K}/\mathbb{F}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$, $N_{\mathbb{K}/\mathbb{F}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$ com σ_i, $i = 1, \ldots, n$ os $\mathbb{F}$-*monomorfismo* de $\mathbb{K}$ em $\mathbb{C}$.

Exemplo 2.3.8. Sejam $\mathbb{F} = \mathbb{Q}(\sqrt{13})$, $\alpha = 1 + \sqrt{13}$ e $\beta = (3 + \sqrt{13})/2$. Os monomorfismos de $\mathbb{F}$ em $\mathbb{C}$ são definidos por

$$\sigma_1 : \sqrt{13} \mapsto \sqrt{13} \quad e \quad \sigma_2 : \sqrt{13} \mapsto -\sqrt{13},$$

onde os elementos de $\mathbb{Q}$ ficam fixos. Assim,

$$N_{\mathbb{F}/\mathbb{Q}}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = (1 + \sqrt{13})(1 - \sqrt{13}) = -12,$$

$$N_{\mathbb{F}/\mathbb{Q}}(\beta) = \sigma_1(\beta)\sigma_2(\beta) = \left(\frac{3 + \sqrt{13}}{2}\right)\left(\frac{3 - \sqrt{13}}{2}\right) = -1,$$

$$Tr_{\mathbb{F}/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) = (1 + \sqrt{13}) + (1 - \sqrt{13}) = 2, \text{ e}$$

$$Tr_{\mathbb{F}/\mathbb{Q}}(\beta) = \sigma_1(\beta) + \sigma_2(\beta) = \frac{3 + \sqrt{13}}{2} + \frac{3 - \sqrt{13}}{2} = 3.$$

Além disso,

$$N_{\mathbb{F}/\mathbb{Q}}(\alpha\beta) = N_{\mathbb{F}/\mathbb{Q}}\left((1 + \sqrt{13})\left(\frac{3 + \sqrt{13}}{2}\right)\right) = N_{\mathbb{F}/\mathbb{Q}}(8+2\sqrt{13}) = \sigma_1(8+2\sqrt{13})\sigma_2(8+2\sqrt{13}) =$$

$$(8 + 2\sqrt{13})(8 - 2\sqrt{13}) = 8^2 - 4.13 = 12 = (-12)(-1) = N_{\mathbb{F}/\mathbb{Q}}(\alpha)N_{\mathbb{F}/\mathbb{Q}}(\beta),$$

e

$$Tr_{\mathbb{F}/\mathbb{Q}}(\alpha + \beta) = Tr_{\mathbb{F}/\mathbb{Q}}\left((1 + \sqrt{13}) + \left(\frac{3 + \sqrt{13}}{2}\right)\right) = Tr_{\mathbb{F}/\mathbb{Q}}\left(\frac{5 + 3\sqrt{13}}{2}\right) =$$

$$= \sigma_1\left(\frac{5 + 3\sqrt{13}}{2}\right) + \sigma_2\left(\frac{5 + 3\sqrt{13}}{2}\right) = 5 = 2 + 3 = Tr_{\mathbb{F}/\mathbb{Q}}(\alpha) + Tr_{\mathbb{F}/\mathbb{Q}}(\beta).$$

Exemplo 2.3.9. Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{-1}, \sqrt{3})$ e $\mathbb{F} = \mathbb{Q}(\sqrt{3})$. Os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ que fixam $\mathbb{F}$ são dados por

$$\sigma_1 : \begin{array}{ccc} \mathbb{K} & \to & \mathbb{C} \\ \sqrt{-1} & \mapsto & \sqrt{-1} \end{array} \quad \text{e} \quad \sigma_2 : \begin{array}{ccc} \mathbb{K} & \to & \mathbb{C} \\ \sqrt{-1} & \mapsto & -\sqrt{-1} \end{array}.$$

Se $\alpha = 5 + \sqrt{-1} \in \mathbb{K}$, então

$$N_{\mathbb{K}/\mathbb{F}}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = (5 + \sqrt{-1})(5 - \sqrt{-1}) = 26, \text{ e}$$

$$Tr_{\mathbb{K}/\mathbb{F}}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) = (5 + \sqrt{-1}) + (5 - \sqrt{-1}) = 10.$$

Definição 2.3.10. Sejam $\mathbb{F} \subset \mathbb{K}$ uma extensão finita de corpos. Dizemos que $a \in \mathbb{F}$ não é norma de $\mathbb{K}$ sobre $\mathbb{F}$ se não existe elemento $\alpha \in \mathbb{K}$ tal que $N_{\mathbb{K}/\mathbb{F}}(\alpha) = a$.

2.4 Corpos quadráticos

Nesta seção, vamos apresentar os corpos quadráticos e algumas de suas propriedades. Esta seção será de extrema importância para o desenvolvimento do trabalho, pois construiremos códigos de bloco espaço-temporais via corpos quadráticos. Para estudar quais os melhores códigos precisaremos dos resultados apresentados neste capítulo. As principais referências utilizadas são [13], [14] e [19].

Definição 2.4.1. Uma extensão de corpos de grau 2 sobre o corpo $\mathbb{Q}$ é chamado de **corpo quadrático**.

Exemplo 2.4.2. O corpo $\mathbb{F} = \mathbb{Q}(\sqrt{17})$ é um corpo quadrático, pois $\theta = \sqrt{17}$ é uma raíz do polinômio irredutível $f(x) = x^2 - 17 \in \mathbb{Q}[x]$.

Proposição 2.4.3. Todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, sendo d um inteiro livre de quadrados.

Demonstração. Sejam $\mathbb{F} = \mathbb{Q}(\theta)$ um corpo quadrático, ou seja, um corpo de números de grau 2, e $f(x) = x^2 + ax + b$, com $a, b \in \mathbb{Q}$, o polinômio minimal de $\theta \in \mathbb{F}$. Resolvendo a equação quadrática $\theta^2 + a\theta + b = 0$, segue que $\theta = \dfrac{-a \pm \sqrt{a^2 - 4b}}{2}$ são as raízes de $f(x)$. Como $2\theta - a = \pm\sqrt{a^2 - 4b}$, segue que $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{a^2 - 4b})$. Por outro lado, $a^2 - 4b$ é um número racional que pode ser escrito como $a^2 - 4b = \dfrac{u}{v} = \dfrac{uv}{v^2}$, com $u, v \in \mathbb{Z}$, $mdc(u, v) = 1$, e de forma que u e v não sejam quadrados perfeitos, pois caso contrário, teremos $\mathbb{Q}(\theta) = \mathbb{Q}$. Assim, $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{a^2 - 4b}) = \mathbb{Q}\left(\sqrt{\dfrac{u}{v}}\right) = \mathbb{Q}\left(\sqrt{\dfrac{uv}{v^2}}\right) = \mathbb{Q}(\sqrt{uv})$. Se que $uv = k^2 d$, com $k, d \in \mathbb{Z}$, e d um inteiro livre de quadrados, então, $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{uv}) = \mathbb{Q}(\sqrt{k^2 d}) = \mathbb{Q}(\sqrt{d})$. □

Observação 2.4.4. Se $d > 0$, então a extensão $\mathbb{Q}(\sqrt{d})$ é **totalmente real** e se $d < 0$, então a extensão $\mathbb{Q}(\sqrt{d})$ é **totalmente imaginária**.

Teorema 2.4.5. Se $\alpha \in \mathbb{Q}$ é tal que existe um polinômio $g(x) \in \mathbb{Z}[x]$ mônico, satisfazendo $g(\alpha) = 0$, então $\alpha \in \mathbb{Z}$.

Demonstração. Sejam $g(x) = x^n + a_1 x^{n-1} + \ldots + a_n$, com $a_1, \ldots, a_n \in \mathbb{Z}$ e $\alpha = \frac{a}{b} \in \mathbb{Q}$ com $b \geq 1$ e a, b primos entre si. Assim,

$$0 = b^n g(\alpha) = a^n + b(a_1 a^{n-1} + b a_2 a^{n-2} + \ldots + b^{n-1} a_n),$$

e portanto b divide a^n. Como a e b são primos entre si, segue que é uma unidade, ou seja, $b = \pm 1$. Logo, $\alpha \in \mathbb{Z}$. □

Teorema 2.4.6. [19] Se $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ é um corpo quadrático com $d \in \mathbb{Z}$ um inteiro livre de quadrados, então o anel dos inteiros algébricos $\mathcal{O}_{\mathbb{F}}$ de $\mathbb{Q}(\sqrt{d})$ é dado por:
a) $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\sqrt{d}]$ se $d \equiv 2$ ou $d \equiv 3 (mod\, 4)$ e uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{F}}$ é dado por $\{1, \sqrt{d}\}$.
b) $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}\left[\dfrac{1 + \sqrt{d}}{2}\right]$ se $d \equiv 1 (mod\, 4)$ e uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{F}}$ é dado por $\left\{1, \dfrac{1 + \sqrt{d}}{2}\right\}$.

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 $m(x) = x - a$. Como α é um inteiro algébrico sobre $\mathbb{Z}$, segue que $a \in \mathbb{Z}$. Se $b \neq 0$, então o polinômio minimal $m(x)$ de α sobre $\mathbb{Q}$ tem grau 2 e é obtido do seguinte modo:

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

Logo $m(x) = x^2 - 2ax + a^2 - db^2$, e desse modo $2a$, $a^2 - db^2 \in \mathbb{Z}$. Assim, $(2a)^2 - d(2b)^2 \in \mathbb{Z}$ e daí $d(2b)^2 \in \mathbb{Z}$, pois $2a \in \mathbb{Z}$. Ainda, $2b \in \mathbb{Z}$, 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 um inteiro livre de quadrados teríamos que $d(2b)^2 \notin \mathbb{Z}$, o que é um absurdo. Logo, $2b \in \mathbb{Z}$. Assim, podemos escrever,

$$a = \frac{u}{2},\ b = \frac{v}{2},\quad com\, u,\ v \in \mathbb{Z}. \tag{2.1}$$

Além disso, temos que

$$(2a)^2 - d(2b)^2 \in 4\mathbb{Z}. \tag{2.2}$$

Substituindo a por $\frac{u}{2}$ e b por $\frac{v}{2}$, segue que $u^2 - dv^2 \in\ 4\mathbb{Z}$.
a) Se $d \equiv 2$ ou $3 (mod\, 4)$, então u e v são pares, pois se v fosse ímpar teríamos $v^2 \equiv 1 (mod\, 4)$. Assim, como $u^2 - dv^2 \in 4\mathbb{Z}$, segue 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 $\alpha = a + b\sqrt{d} \in \mathcal{O}_{\mathbb{F}}$, então $\alpha \in \mathbb{Z}[\sqrt{d}]$ e assim, $\mathcal{O}_{\mathbb{F}} \subset \mathbb{Z}[\sqrt{d}]$. Por outro lado, tomando $\alpha \in \mathbb{Z}[\sqrt{d}]$, segue que α é raiz do polinômio $x^2 - 2ax + a^2 - db^2 \in \mathbb{Z}[x]$, pois $2a$, $a^2 - db^2 \in \mathbb{Z}$. Logo, $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_{\mathbb{F}}$. Portanto, $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\sqrt{d}]$.
b) Se $d \equiv 1 (mod\, 4)$, então $u^2 - dv^2 \in 4\mathbb{Z}$, 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, $\mathcal{O}_{\mathbb{F}} \subset \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. 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, $b \in \mathbb{Z}$, então $2a + b \in \mathbb{Z}$ 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, $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subset \mathcal{O}_{\mathbb{F}}$, pois os coeficientes do polinômio minimal de α, $m(x) = x^2 - (2a + b)x + a^2 + ab + (1 - d)b^2/4$ estão em $\mathbb{Z}$. Portanto, $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathcal{O}_{\mathbb{F}}$. □

Exemplo 2.4.7. Seja $\mathbb{F}$ o corpo quadrático $\mathbb{Q}(\sqrt{-1})$. O anel dos inteiros algébricos de $\mathbb{F}$ é dado por $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, 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 $d = -3 \equiv 1 (mod\, 4)$.

Os resultados que seguem serão de fundamental importância para nos auxiliar nas demonstrações dos resultados do Capítulo 5.

Teorema 2.4.8. Se d é um inteiro negativo e livre de quadrados, então $|\alpha| \geq 1$, para todo $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ não nulo.

Demonstração. Temos dois casos a analisar: $d \equiv 1 \pmod 4$ e $d \equiv 2$ ou $3 \pmod 4$.
Caso 1: Se $d \equiv 2$ ou $3 \pmod 4$, então $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$. Logo, $\alpha \in \mathbb{Z}[\sqrt{d}]$ é da forma $\alpha = a + b\sqrt{d}$, com $a, b \in \mathbb{Z}$. Assim,

$$|\alpha| = \sqrt{a^2 + |d|b^2} \geq \sqrt{a^2 + b^2}.$$

Como $a^2 + b^2 \geq 1 \Leftrightarrow a \neq 0$ e/ou $b \neq 0$, e como $1 \in \mathbb{Z}[\sqrt{d}]$, segue que $|\alpha| \geq 1$ se $\alpha \neq 0$.
Caso 2: Se $d \equiv 1 \pmod 4$, então $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Logo, se $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, então $\alpha = a + b\left(\frac{1+\sqrt{d}}{2}\right)$, com $a, b \in \mathbb{Z}$. Assim,

$$|\alpha| = \sqrt{\left(a + \tfrac{b}{2}\right)^2 + |d|\left(\tfrac{b}{2}\right)^2} \geq \sqrt{\left(a + \tfrac{b}{2}\right)^2 + 3\left(\tfrac{b}{2}\right)^2},$$

pois $|-3| \leq |d|$ para qualquer $d \in \mathbb{Z}$, $d < 0$ e $d \equiv 1 \pmod 4$. Assim, $\left(a + \frac{b}{2}\right)^2 + 3\left(\frac{b}{2}\right)^2 \geq 1 \Leftrightarrow a \neq 0$ e $b = 0$, e como $1 \in \mathbb{Z}[\sqrt{d}]$, segue que $|\alpha| \geq 1$, se $\alpha \neq 0$.
Logo, dos casos 1 e 2, concluímos o resultado. □

Os resultados, a seguir, caracterizam os elementos de certos ideais do anel de inteiros $\mathbb{Z}[i]$ e $\mathbb{Z}[\frac{1-\sqrt{-3}}{2}]$.

Observação 2.4.9. Se $a \in \mathbb{Z}$, então existe um inteiro $l_1 \geq 0$, tal que $a = \sum_{k=0}^{l_1} a_k 2^k$, com $a_k \in \{0, 1, -1\}$.

Este resultado é bem conhecido na teoria dos números e servirá de ferramenta para a proposição que segue.

Proposição 2.4.10. Se $\alpha \in (1+i)\mathbb{Z}[i]$, então existe um inteiro $l_0 \geq 0$ tal que

$$\alpha = \sum_{k=0}^{l_0} y_k (1+i)^k,$$

com $y_k \in \{0, 1, -1, i, -i\}$.

Demonstração. Temos que qualquer número inteiro pode ser escrito como a soma de potência de dois, ou seja, se $a \in \mathbb{Z}$, então existe um inteiro $l_1 \geq 0$ tal que

$$a = \sum_{k=0}^{l_1} a_k 2^k,$$

com $a_k \in \{0, 1, -1\}$. Se $\alpha \in (1+i)\mathbb{Z}[i]$, então $\alpha = (a+bi)(1+i) = (a-b) + i(a+b)$, com $a, b \in \mathbb{Z}$. Assim,

$$a = \sum_{k=0}^{l_1} a_k 2^k \text{ e } b = \sum_{k=0}^{l_2} b_k 2^k,$$

com $a_k, b_k \in \{0, 1, -1\}$. Se $l_3 = max\{l_1, l_2\}$, então

$$a - b = \sum_{k=0}^{l_3} 2^k (a_k - b_k) \text{ e } (a+b)i = \sum_{k=0}^{l_3} 2^k i (a_k + b_k).$$

Como $\alpha = (a-b) + i(a+b)$, segue que

$$\alpha = \sum_{k=0}^{l_3} 2^k (a_k - b_k + i a_k + i b_k),$$

com $a_k - b_k + ia_k + ib_k \in S = \{0, 1+i, -1-i, -1+i, 1-i, 2i, 2, -2, -2i\}$, pois $a_k, b_k \in \{0, 1, -1\}$. Observemos que S pode ser escrito na forma:

$$S = \{(i+1)^{s_k} x_k \mid s_k \in \{1, 2\}, x_k \in \{0, 1, -1, i, -i\}\}.$$

Como o número 2^k pode ser escrito como $(1+i)^{2k}(-i)^k$, segue que

$$\alpha = \sum_{k=0}^{l_3} 2^k(a_k - b_k + ia_k + ib_k) = \sum_{k=0}^{l_3}(1+i)^{2k}(-i)^k(1+i)^{s_k}x_k = \sum_{k=0}^{l_3}(1+i)^{2k+s_k}x_k. \quad (2.3)$$

Mostramos, por indução sobre l, que

$$\sum_{k=0}^{l}(1+i)^{2k+s_k}x_k = \sum_{k=0}^{2l+2}(1+i)^k y_k, \quad (2.4)$$

com $y_k \in \{0, 1, -1, i, -i\}$. Se $l = 0$, então

$$\sum_{k=0}^{0}(1+i)^{2k+s_k}x_k = (1+i)^{s_0}x_0 = \sum_{k=0}^{2}(1+i)^k y_k,$$

com $y_k = x_0$, se $k = s_0$, e 0 caso contrário. Suponhamos que vale para $l = n$, e provemos que vale para $l = n+1$. Assim, por hipótese de indução,

$$\begin{aligned}\sum_{k=0}^{n+1}(1+i)^{2k+s_k}x_k &= (1+i)^{2n+2+s_{n+1}}x_{n+1} + \sum_{k=0}^{n}(1+i)^{2k+s_k}x_k \\ &= (1+i)^{2n+2+s_{n+1}}x_{n+1} + \sum_{k=0}^{2n+2}(1+i)^k y_k\end{aligned}.$$

Para $p \in \{2n+3, 2n+4\}$, definimos

$$y_k = \begin{cases} x_{n+1}, & \text{se } k = 2n+2+s_{n+1} \\ 0, & \text{caso contrário} \end{cases}$$

Assim,

$$\sum_{k=0}^{n+1}(1+i)^{2k+s_k}x_k = \sum_{k=0}^{2n+4}(1+i)^k y_k.$$

Portanto, das Equações (2.3) e (2.4), tomando $l_0 = 2l_3+2$, segue que $\alpha = \sum_{k=0}^{l_0}(1+i)^k y_k$, como queríamos. □

Lema 2.4.11. Se $a \in \mathbb{Z}$, então

$$a = \sum_{k=0}^{m} a_k 3^k,$$

com $a_k \in \{0, 1, -1\}$ e m o menor natural tal que $|a| \leq 3^m$.

Demonstração. Provemos, por indução, que o resultado vale para qualquer inteiro maior que 0. Para números naturais menores que 3^n com $n = 0$ e 1, segue que

$$0 = 0 \cdot 3^0, 1 = 3^0, 2 = -3^0 + 3^1.$$

Suponhamos que o resultado vale para qualquer natural menor ou igual a 3^n, e provemos que vale para qualquer natural a, com $3^n < a \leq 3^{n+1}$. Se $a \leq \sum_{k=0}^{n} 3^k$, então $a - 3^n \leq \sum_{k=0}^{n-1} 3^k < 3^n$. Logo,

$$a - 3^n = \sum_{k=0}^{n} a_k 3^k,$$

com $a_k \in \{0, 1, -1\}$. Como $2 \cdot 3^n = 3^{n+1} - 3^n$, segue que

$$a = 3^n + \sum_{k=0}^{n} a_k 3^k = \sum_{k=0}^{n+1} a_k 3^k.$$

Se $\sum_{k=0}^{n} 3^k < a \leq 2 \cdot 3^n$, então

$$\sum_{k=0}^{n} 3^k - 3^n < a - 3^n \leq 3^n, \text{ ou seja, } \sum_{k=0}^{n-1} 3^k < a - 3^n \leq 3^n.$$

Como $a - 3^n \leq 3^n$, segue que

$$a - 3^n = \sum_{k=0}^{n} a_k 3^k.$$

Logo $\sum_{k=0}^{n-1} 3^k < a - 3^n = \sum_{k=0}^{n} a_k 3^k$, e portanto, $a_n = 1$. Assim,

$$a - 3^n = \sum_{k=0}^{n} a_k 3^k = 3^n + \sum_{k=0}^{n} a_k 3^k \Rightarrow$$

$$a = 2 \cdot 3^n + \sum_{k=0}^{n-1} a_k 3^k = 3^{n+1} - 3^n + \sum_{k=0}^{n-1} a_k 3^k \Rightarrow$$

$$a = \sum_{k=0}^{n+1} a_k 3^k,$$

com $a_n = -1$ e $a_{n+1} = 1$. Se $2 \cdot 3^n \leq a \leq 3^{n+1}$, então $3^{n+1} - a \leq 3^n$. Assim,

$$3^{n+1} - a = \sum_{k=0}^{n} a_k 3^k.$$

Portanto,

$$a = 3^{n+1} - \sum_{k=0}^{n} a_k 3^k \Rightarrow a = \sum_{k=0}^{n+1} b_k 3^k,$$

com $b_k = -a_k$ e $b_n = 1$. Logo concluímos o resultado. □

Proposição 2.4.12. Se $x \in \sqrt{-3}\mathbb{Z}[\frac{1-\sqrt{-3}}{2}]$, então existe um inteiro $l_0 \geq 0$ tal que

$$x = \sum_{k=0}^{l_0} (\sqrt{-3})^k x_k,$$

com $x_k \in \left\{0, 1, -1, \frac{1+\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}\right\}$.

Demonstração. Pelo Lema 2.4.11, segue que qualquer número inteiro a pode ser escrito como $\sum_{k=0}^{n} a_k 3^k$, com $a_k \in \{0, 1, -1\}$. Se $x \in \sqrt{-3}\mathbb{Z}[\frac{1-\sqrt{-3}}{2}]$, então que $x = \sqrt{-3}(a + b(\frac{1-\sqrt{-3}}{2}))$, com $a, b \in \mathbb{Z}$. Podemos escrever a e b como

$$a = \sum_{k=0}^{l_1} a_k 3^k \text{ e } b = \sum_{k=0}^{l_2} b_k 3^k,$$

com $a_k, b_k \in \{0, 1, -1\}$. Observemos que

$$3^k = (-(-3))^k = (-1)^k(-3)^k = (-1)^k(\sqrt{-3})^{2k}.$$

Seja $l_3 = max\{l_1, l_2\}$. Como $x = \sqrt{-3}(a + b(\frac{1-\sqrt{-3}}{2}))$, segue que

$$\begin{aligned} x &= \sum_{k=0}^{l_3} \sqrt{-3}\left(3^k a_k + 3^k b_k \left(\frac{1-\sqrt{-3}}{2}\right)\right) \\ &= \sum_{k=0}^{l_3} (\sqrt{-3})^{2k+1}(-1)^k \left(a_k + b_k \left(\frac{1-\sqrt{-3}}{2}\right)\right). \end{aligned} \tag{2.5}$$

Agora, $a_k + b_k(\frac{1-\sqrt{-3}}{2}) \in S = \left\{0, 1, -1, \frac{1+\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}, \frac{3+\sqrt{-3}}{2}, \frac{-3-\sqrt{-3}}{2}\right\}$ para $a_k, b_k \in \{0, 1, -1\}$, e assim, $(-1)^k(a_k + b_k(\frac{1-\sqrt{-3}}{2})) \in S$. Seja

$$S_1 = \left\{0, 1, -1, \frac{1+\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}\right\}.$$

Observamos que todo elemento $s \in S$ pode ser escrito como $(\sqrt{-3})^{s_k} x_k$, com $x_k \in S_1$ e $s_k \in \{0, 1\}$. Portanto, pela Equação (2.5), segue que

$$\begin{aligned} x &= \sum_{k=0}^{l_3} (\sqrt{-3})^{2k+1}(-1)^k \left(a_k + b_k \left(\frac{1-\sqrt{-3}}{2}\right)\right) = \sum_{k=0}^{l_3} (\sqrt{-3})^{2k+1}(\sqrt{-3})^{s_k} x_k \\ &= \sum_{k=0}^{l_3} (\sqrt{-3})^{2k+1+s_k} x_k. \end{aligned} \tag{2.6}$$

Mostremos, por indução, que

$$\sum_{k=0}^{l} (\sqrt{-3})^{2k+1+s_k} x_k = \sum_{k=0}^{2l+2} (\sqrt{-3})^k y_k, \tag{2.7}$$

com $x_k, y_k \in S_1$. Se $l = 0$, então

$$\sum_{k=0}^{0}(\sqrt{-3})^{1+s_k}x_k = \sum_{k=0}^{2}(\sqrt{-3})^{k}y_k,$$

com $y_k = x_0$ se $k = 1 + s_0$, e $y_k = 0$, caso contrário. Suponhamos que vale para $l = n$ e provemos que vale para $l = n + 1$. Assim,

$$\begin{aligned}\sum_{k=0}^{n+1}(\sqrt{-3})^{2k+1+s_k}x_k &= (\sqrt{-3})^{2n+3+s_{n+1}}x_{n+1} + \sum_{k=0}^{n}(\sqrt{-3})^{2n+1+s_k}x_k \\ &= (\sqrt{-3})^{2n+3+s_{n+1}}x_{n+1} + \sum_{k=0}^{2l+2}(\sqrt{-3})^{k}y_k.\end{aligned}$$

Lembramos que $s_k \in \{0, 1\}$. Para $k \in \{2n + 3, 2n + 4\}$, definimos $y_k = \begin{cases} x_{n+1}, & \text{se } k = 2n + 3 + s_n \\ 0, & \text{caso contrário} \end{cases}$. Assim,

$$\sum_{k=0}^{n+1}(\sqrt{-3})^{2k+1+s_k}x_k = \sum_{k=0}^{2l+4}(\sqrt{-3})^{k}y_k.$$

Portanto, das Equações (2.6) e (2.7), tomando $l_0 = 2l_3+2$, segue que $\alpha = \sum_{k=0}^{l_0}\sqrt{-3}^{k}x_k$, como queríamos. □

2.5 Base integral e discriminante

Nesta seção, apresentamos os conceitos de base integral, discriminante e alguns resultados, como o determinante de Vandermonde, que serão de muita importância para a construção de reticulados no Capítulo 3. A principal referência utilizada é [14].

Definição 2.5.1. Seja $\mathcal{O}_{\mathbb{F}}$ o anel de inteiros algébricos de um corpo de números $\mathbb{F}$. Uma base de $\mathcal{O}_{\mathbb{F}}$ sobre $\mathbb{Z}$, ou simplesmente, uma $\mathbb{Z}$-base para $\mathcal{O}_{\mathbb{F}}$, é chamada de uma **base integral** para $\mathcal{O}_{\mathbb{F}}$.

Observação 2.5.2. [19] Todo corpo de números $\mathbb{F}$ possui uma base integral.

Observação 2.5.3. Como consequência do Teorema 2.4.6, $\{1, \sqrt{d}\}$ é uma $\mathbb{Z}$-base de $\mathbb{Z}[\sqrt{d}]$ se $d \equiv 2$ ou $d \equiv 3 (mod\, 4)$, e $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ é uma $\mathbb{Z}$-base de $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ se $d \equiv 1 (mod\, 4)$.

Exemplo 2.5.4. Se $\mathbb{F} = \mathbb{Q}(\sqrt{13})$, então

$$\mathcal{O}_{\mathbb{F}} = \mathbb{Z}\left[\frac{1+\sqrt{13}}{2}\right] = \left\{a + b\left(\frac{1+\sqrt{13}}{2}\right); a, b \in \mathbb{Z}\right\} \neq \mathbb{Z}[\sqrt{13}] = \{a+b\sqrt{13}; a, b \in \mathbb{Z}\}.$$

Veja que $\alpha = (1 + \sqrt{13})/2$ é uma raiz de $min_{\mathbb{Q}}\alpha(x) = x^2 - x - 3$, enquanto que $\beta = \sqrt{13}$ é uma raiz de $x^2 - 13$. Apesar de $\{1, \beta\}$ ser uma base para $\mathbb{F}$ contendo inteiros algébricos, ela não é uma base integral para $\mathbb{F}$.

Definição 2.5.5. Sejam $\mathbb{F} = \mathbb{Q}(\alpha)$ um corpo de números com $[\mathbb{F} : \mathbb{Q}] = n$,

$$\mathcal{B} = \{\alpha_1, \alpha_2, ..., \alpha_n\}$$

uma $\mathbb{Q}$-base para $\mathbb{F}$ e σ_i para $i = 1, \ldots, n$ os monomorfismos de $\mathbb{F}$ em $\mathbb{C}$. O **discriminante** da base $\mathcal{B}$ é definido por

$$\mathcal{D}(\mathcal{B}) = (det(\sigma_j(\alpha_i)))^2,$$

onde *det* é o determinante da matriz com entradas $\sigma_j(\alpha_i)$ na i-ésima linha e j-ésima coluna. Em particular, se

$$\mathcal{B} = \{1, \alpha, ..., \alpha^{n-1}\},$$

então o determinante da matriz $(\sigma_j(\alpha^{i-1}))$ é chamado de **determinante de Vandermonde** e seu valor é dada por

$$det(\sigma_j(\alpha^{i-1})) = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i), \tag{2.8}$$

onde $\alpha_k = \sigma_k(\alpha)$ é um k-ésimo conjugado de α, para $k = 1, 2, ..., n$.

Exemplo 2.5.6. Se $\mathbb{F} = \mathbb{Q}(\sqrt{2})$, então $\mathcal{O}_\mathbb{F} = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Z}\}$ e $\mathcal{B} = \{1, \sqrt{2}\}$ é uma base integral de $\mathbb{F}$. Os $\mathbb{Q}$-monomorfismos de $\mathbb{F}$ em $\mathbb{C}$ são dados por:

$$\sigma_1 : \sqrt{2} \mapsto \sqrt{2} \; e \; \sigma_2 : \sqrt{2} \mapsto -\sqrt{2}.$$

Portanto,

$$\mathcal{D}(\mathcal{B}) = (det(\sigma_j(\alpha^{i-1})))^2 = \left(det \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\sqrt{2}) & \sigma_2(\sqrt{2}) \end{pmatrix} \right)^2 =$$

$$= \left(det \begin{pmatrix} 1 & 1 \\ \sqrt{2} & -\sqrt{2} \end{pmatrix} \right)^2 = (-2\sqrt{2})^2 = 8.$$

Proposição 2.5.7. Sejam $\mathbb{F}$ um corpo, $\mathbb{K} = \mathbb{F}(\alpha)$ uma extensão finita de $\mathbb{F}$ de grau n. Se $f(x)$ é o polinômio minimal de α sobre $\mathbb{F}$, então,

$$\mathcal{D}_{\mathbb{K}/\mathbb{F}}(1, \alpha, ..., \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N_{\mathbb{K}/\mathbb{F}}(f'(\alpha)),$$

onde $f'(\alpha)$ é a derivada de $f(x)$ em α.

Demonstração. Sejam $\alpha_1, ..., \alpha_n$ as raízes de $f(x)$ em alguma extensão de $\mathbb{F}$ e σ_i, para $i = 1, ..., n$ os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Da definição, $\mathcal{D}_{\mathbb{K}/\mathbb{F}}(1, \alpha, ..., \alpha^{n-1}) = (det(\sigma_i(\alpha^j)))^2 = det(\alpha_i^j)^2$, com $i = 1, ..., n$ e $j = 0, ..., n-1$. Como $det(\alpha_i^j)$ é um determinante de Vandermonde, segue que

$$\begin{aligned}
(det(\alpha_i^j))^2 &= \left[\prod_{1 \leq k < i \leq n} (\alpha_i - \alpha_k) \right]^2 = \prod_{1 \leq k < i \leq n} [(\alpha_i - \alpha_k)(\alpha_i - \alpha_k)] \\
&= (-1)^{\frac{1}{2}n(n-1)} \prod_{1 \leq k < i \leq n, i \neq k} (\alpha_i - \alpha_k) \\
&= (-1)^{\frac{1}{2}n(n-1)} \prod_{i=1}^{n} \left[\prod_{k=1, k \neq 1}^{n} (\alpha_i - \alpha_k) \right] = (-1)^{\frac{1}{2}n(n-1)} \prod_{i=1}^{n} f'(\alpha_i) \\
&= (-1)^{\frac{1}{2}n(n-1)} N(f'(\alpha)),
\end{aligned}$$

o que prova a proposição. □

Exemplo 2.5.8. Se $\mathbb{F} = \mathbb{Q}$, $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ e $f(x) = x^2 - 3$ é o polinômio minimal de $\sqrt{3}$ sobre $\mathbb{Q}$, então

$$\begin{aligned} \mathcal{D}_{\mathbb{K}/\mathbb{F}}(1, \sqrt{3}) &= (-1)^{\frac{2\cdot 1}{2}} N_{\mathbb{K}/\mathbb{F}}(f'(\sqrt{3})) = -N_{\mathbb{K}/\mathbb{F}}(2\sqrt{3}) \\ &= -2^2 N_{\mathbb{K}/\mathbb{F}}(\sqrt{3}) = -4(\sqrt{3})(-\sqrt{3}) = 12. \end{aligned}$$

Teorema 2.5.9. [14] Se $\mathcal{B}_1 = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ e $\mathcal{B}_2 = \{\beta_1, \beta_2, ..., \beta_n\}$ são duas $\mathbb{Q}$-bases para um corpo de números $\mathbb{F}$, então

$$\mathcal{D}(\mathcal{B}_2) = d^2 \mathcal{D}(\mathcal{B}_1),$$

onde $d = det(q_{k,i}) \in \mathbb{Q}$, com $d \neq 0$, e $q_{k,i} \in \mathbb{Q}$ é determinado por

$$\beta_k = \sum_{i=1}^{n} q_{k,i}\alpha_i, \text{ onde } q_{k,i} \in \mathbb{Q}.$$

Além disso, $d \in \mathbb{Z}$ desde que $\mathcal{B}_1$ seja uma base integral e $\mathcal{B}_2 \subset \mathcal{O}_{\mathbb{F}}$.

Demonstração. Seja σ_j, para $i = 1, \ldots, n$ os n-monomorfismos de $\mathbb{F}$ em $\mathbb{C}$. A representação $\beta_k = \sum_{i=1}^{n} q_{k,i}\alpha_i$, implica que

$$\sigma_j(\beta_k) = \sum_{i=1}^{n} q_{k,i}\sigma_j(\alpha_i),$$

para cada $k = 1, 2, ..., n$. Assim,

$$\begin{pmatrix} \sigma_1(\beta_1) & \sigma_2(\beta_1) & \ldots & \sigma_n(\beta_1) \\ \sigma_1(\beta_2) & \sigma_2(\beta_2) & \ldots & \sigma_n(\beta_2) \\ \vdots & \vdots & & \vdots \\ \sigma_1(\beta_n) & \sigma_2(\beta_n) & \ldots & \sigma_n(\beta_n) \end{pmatrix} =$$

$$\begin{pmatrix} q_{1,1} & q_{1,2} & \ldots & q_{1,n} \\ q_{2,1} & q_{2,2} & \ldots & q_{2,n} \\ \vdots & \vdots & \vdots & \vdots \\ q_{n,1} & q_{n,2} & \ldots & q_{n,n} \end{pmatrix} \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \ldots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \ldots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \ldots & \sigma_n(\alpha_n) \end{pmatrix}.$$

Tomando os determinantes e elevando ao quadrado, segue que:

$$\mathcal{D}(\mathcal{B}_2) = d^2 \mathcal{D}(\mathcal{B}_1),$$

com $d = det(M)$, onde

$$M = \begin{pmatrix} q_{1,1} & q_{1,2} & \ldots & q_{1,n} \\ q_{2,1} & q_{2,2} & \ldots & q_{2,n} \\ \vdots & \vdots & & \vdots \\ q_{n,1} & q_{n,2} & \ldots & q_{n,n} \end{pmatrix}.$$

□

Exemplo 2.5.10. Sejam $\mathbb{F} = \mathbb{Q}(\sqrt{13})$, $\alpha = (1+\sqrt{13})/2$ e $\beta = \sqrt{13}$. Pelo Exemplo 2.5.4, segue que $\mathcal{B}_1 = \{1, \alpha\}$ e $\mathcal{B}_2 = \{1, \beta\}$ são bases para $\mathbb{F}$, sendo a primeira integral, e a última não integral (mas uma base sobre $\mathbb{Q}$). Como

$$\sigma_1 : \sqrt{13} \mapsto \sqrt{13} \ \ e \ \ \sigma_2 : \sqrt{13} \mapsto -\sqrt{13}$$

são os $\mathbb{Q}$-monomorfismos de $\mathbb{F}$ em $\mathbb{C}$, segue que

$$\begin{aligned} \mathcal{D}(\mathcal{B}_2) &= (det(\sigma_j(\beta^i)))^2 = \left(det \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\sqrt{13}) & \sigma_2(\sqrt{13}) \end{pmatrix}\right)^2 \\ &= \left(det \begin{pmatrix} 1 & 1 \\ \sqrt{13} & -\sqrt{13} \end{pmatrix}\right)^2 = (-2\sqrt{13})^2 = 52, \end{aligned}$$

e

$$\begin{aligned} \mathcal{D}(\mathcal{B}_1) &= (det(\sigma_j(\alpha^i)))^2 = \left(det \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1\left(\frac{1+\sqrt{13}}{2}\right) & \sigma_2\left(\frac{1+\sqrt{13}}{2}\right) \end{pmatrix}\right)^2 \\ &= \left(det \begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{13}}{2} & \frac{1-\sqrt{13}}{2} \end{pmatrix}\right)^2 = (-\sqrt{13})^2 = 13. \end{aligned}$$

Assim,

$$\mathcal{D}(\mathcal{B}_2) = d^2\mathcal{D}(\mathcal{B}_1) = 2^2\mathcal{D}(\mathcal{B}_1).$$

Portanto,

$$d = det \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix} = 2,$$

pois

$$\beta_1 = 1 = q_{1,1}\alpha_1 + q_{1,2}\alpha_2 = 1.1 + 0.\frac{1+\sqrt{13}}{2},$$

e

$$\beta_2 = \sqrt{13} = q_{2,1}\alpha_1 + q_{2,2}\alpha_2 = -1.1 + 2.\frac{1+\sqrt{13}}{2}.$$

Teorema 2.5.11. [14] Se $\mathcal{B} = \{\alpha_1, \alpha_2, ..., \alpha_d\}$ é uma $\mathbb{Q}$-base para um corpo de números $\mathbb{F} = \mathbb{Q}(\alpha)$, então

$$\mathcal{D}(\mathcal{B}) = det(Tr_{\mathbb{F}/\mathbb{Q}}(\alpha_i\alpha_j)) \in \mathbb{Q},$$

e $\mathcal{D}(\mathcal{B}) \neq 0$. Além disso, se $\mathbb{F}$ é um corpo totalmente real, então $\mathcal{D}(\mathcal{B}) > 0$.

Demonstração. Como $\mathcal{D}(\mathcal{B}) = det(\sigma_j(\alpha_i))^2$, segue pelas propriedades de determinante que

$$(det(\sigma_j(\alpha_i)))^2 = det\left(\sum_{k=1}^{d} \sigma_k(\alpha_i\alpha_j)\right) = det(Tr_{\mathbb{F}/\mathbb{Q}}(\alpha_i\alpha_j)).$$

Logo $\mathcal{D}(\mathcal{B}) = det(Tr_{\mathbb{F}/\mathbb{Q}}(\alpha_i\alpha_j))$, e portanto, $\mathcal{D}(\mathcal{B}) \in \mathbb{Q}$. Resta mostrar que $\mathcal{D}(\beta)$ é diferente de zero e também positiva quando $\mathbb{F}$ é totalmente real. Para isso, seja $\mathcal{B}_1 = \mathcal{B}$. Pelo Teorema 2.2.19,

$$\mathcal{B}_2 = \{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$$

é uma base para $\mathbb{F}$ sobre $\mathbb{Q}$. Assim, pelo Teorema 2.5.9, segue que $\mathcal{D}(\mathcal{B}_2) = d^2\mathcal{D}(\mathcal{B}_1)$, onde d é dado no Teorema 2.5.9. No entanto, pelo valor do determinante de Vandermonde (2.8), segue que

$$\mathcal{D}(\mathcal{B}_2) = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)^2,$$

e os α_i são distintos de forma que $\mathcal{D}(\mathcal{B}_2) \neq 0$. Assim, $\mathcal{D}(\mathcal{B}_1) \neq 0$. Sendo $\mathcal{B}_2$ é uma base para $\mathbb{F}$ sobre $\mathbb{Q}$, segue pelo Teorema 2.5.9, que

$$\mathcal{D}(\mathcal{B}_1) = d_1^2 \mathcal{D}(\mathcal{B}_2).$$

Portanto, $\mathcal{D}(\mathcal{B}_2)$ é um inteiro ao quadrado. Como $\mathcal{D}(\mathcal{B}_1) \neq 0$ e se $\mathbb{F}$ é totalmente real, todos os α_j são reais e portanto $\mathcal{D}(\mathcal{B}_1) > 0$. □

Corolário 2.5.12. Se $\mathcal{B}$ é uma base de $\mathbb{F}$ sobre $\mathbb{Q}$ com $\mathcal{B} \subseteq \mathcal{O}_\mathbb{F}$, então $\mathcal{D}(\mathcal{B}) \in \mathbb{Z}$.

Demonstração. Como $\mathcal{D}(\mathcal{B}) = det(Tr_{\mathbb{F}/\mathbb{Q}}(\alpha_i\alpha_j))$ onde $\mathcal{B} = \{\alpha_1, ..., \alpha_d\}$ é uma base de $\mathbb{F}$ sobre $\mathbb{Q}$ segue que $\mathcal{D}(\mathcal{B}) \in \mathbb{Z}$. □

Exemplo 2.5.13. Do Exemplo 2.5.10 segue que o corpo totalmente real $\mathbb{F} = \mathbb{Q}(\sqrt{13})$ possui base integral

$$\mathcal{B}_1 = \{1, (1+\sqrt{13})/2\} = \{1, \alpha\} = \{\alpha_1, \alpha_2\}$$

e uma $\mathbb{Q}$ -base não integral

$$\mathcal{B}_2 = \{1, \sqrt{13}\} = \{1, \beta\} = \{\beta_1, \beta_2\}.$$

Além disso,

$$(Tr_{\mathbb{F}/\mathbb{Q}}(\alpha_i\alpha_j)) = \begin{pmatrix} Tr_{\mathbb{F}/\mathbb{Q}}(1) & Tr_{\mathbb{F}/\mathbb{Q}}(\alpha) \\ Tr_{\mathbb{F}/\mathbb{Q}}(\alpha) & Tr_{\mathbb{F}/\mathbb{Q}}(\alpha^2) \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 7 \end{pmatrix},$$

e deste modo,

$$\mathcal{D}(\mathcal{B}_1) = det(Tr_{\mathbb{F}/\mathbb{Q}}(\alpha_i\alpha_j)) = det \begin{pmatrix} 2 & 1 \\ 1 & 7 \end{pmatrix} = 13 \in \mathbb{Z}.$$

Mas, como

$$(Tr_{\mathbb{F}/\mathbb{Q}}(\beta_i\beta_j)) = \begin{pmatrix} Tr_{\mathbb{F}/\mathbb{Q}}(1) & Tr_{\mathbb{F}/\mathbb{Q}}(\beta) \\ Tr_{\mathbb{F}/\mathbb{Q}}(\beta) & Tr_{\mathbb{F}/\mathbb{Q}}(\beta^2) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 26 \end{pmatrix},$$

segue que

$$\mathcal{D}(\mathcal{B}_2) = 52 = det(Tr_{\mathbb{F}/\mathbb{Q}}(\beta_i\beta_j)) \in \mathbb{Z}.$$

O próximo teorema fornece um critério para sabermos quando uma base é integral.

Teorema 2.5.14. [14] Se $\mathcal{B} \subseteq \mathcal{O}_\mathbb{F}$ é uma $\mathbb{Q}$-base para $\mathbb{F}$ e $\mathcal{D}(\mathcal{B})$ é livre de quadrados, isto é, $\mathcal{D}(\mathcal{B})$ não tem divisor que é o quadrado de um número primo, então $\mathcal{B}$ é uma base integral para $\mathbb{F}$.

Exemplo 2.5.15. O Exemplo 2.5.4 fornece um discriminante livre de quadrados de uma base integral. No entanto, $\mathcal{B} = \{1, \sqrt{2}\}$ é uma base integral para $\mathbb{Q}(\sqrt{2})$ mas $\mathcal{D}(\mathcal{B}) = 8$. Portanto, a recíproca do Teorema 2.5.14 não é verdadeira.

Observação 2.5.16. [14] O discriminante associado a uma base integral de um corpo de números é um invariante algébrico, isto é, seu valor independe das bases tomadas para o corpo.

A próxima proposição caracteriza o discriminante de um corpo quadrático.

Proposição 2.5.17. Seja d um inteiro livre de quadrados, o discriminante de $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ sobre $\mathbb{Q}$ é dado por:
(1) $\mathcal{D}_{\mathbb{F}/\mathbb{Q}} = d$, se $d \equiv 1(mod\ 4)$;
(2) $\mathcal{D}_{\mathbb{F}/\mathbb{Q}} = 4d$, se $d \equiv 2(mod\ 4)$ ou $d \equiv 3(mod\ 4)$.

Demonstração. Como os $\mathbb{Q}$-monomorfismos de $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ em $\mathbb{C}$, com $d \in \mathbb{Z}$ um inteiro 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

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

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

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

□

Exemplo 2.5.18. Dado $\mathbb{F} = \mathbb{Q}(\sqrt{5})$, tem-se $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, isto é, $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ é uma base integral de $\mathcal{O}_{\mathbb{F}}$ e o discriminante de $\mathbb{F}$ é

$$\mathcal{D}_{\mathbb{F}/\mathbb{Q}} = \left(\det\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1\left(\frac{1+\sqrt{5}}{2}\right) & \sigma_2\left(\frac{1+\sqrt{5}}{2}\right) \end{pmatrix}\right)^2 = \left(\det\begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{pmatrix}\right)^2 = 5.$$

Os $\mathbb{Q}$-monomorfismos de $\mathbb{F}$ em $\mathbb{C}$ são $\sigma_1(a+b\sqrt{5}) = a+b\sqrt{5}$ e $\sigma_2(a+b\sqrt{5}) = a-b\sqrt{5}$. Logo,

$$Tr_{\mathbb{F}/\mathbb{Q}}(a+b\sqrt{5}) = \sum_{i=1}^{2} \sigma_i(a+b\sqrt{5}) = 2a \text{ e}$$

$$N_{\mathbb{F}/\mathbb{Q}}(a+b\sqrt{5}) = \prod_{i=1}^{2} \sigma_i(a+b\sqrt{5}) = a^2 - 5b^2.$$

2.6 Álgebra dos quatérnios

A álgebra dos quatérnios teve origem com os números complexos, quando William Rowan Hamilton (1805-1865) apresentou o primeiro conceito moderno dos números complexos como pares ordenados de números reais e tentou generalizar esta ideia para

o espaço tridimensional. Após inúmeras tentativas verificou-se que não era possível a existência de um número complexo tridimensional. Com isso, Hamilton descobriu os quatérnios, que é uma álgebra de dimensão quatro sobre um corpo de números e que possui todas as propriedades aritméticas de um corpo, a menos da comutatividade. A álgebra dos quatérnios foi à primeira álgebra não comutativa. Veremos que quando uma álgebra $\mathcal{A}$ é uma álgebra de divisão, a condição $det(X) \neq 0$, com $X \in \mathcal{A}$, é satisfeita. Para o desenvolvimento desta seção as principais referências utilizadas foram [3], [4], [10] e [22].

Combinando os conceitos de espaço-vetorial e anel obtêm-se o conceito de álgebra.

Definição 2.6.1. Uma álgebra $\mathcal{A}$ é um conjunto sobre um corpo $\mathbb{K}$ com operações de adição , multiplicação, e multiplicação por escalares de $\mathbb{K}$ satisfazendo as seguintes propriedades:
1) $\mathcal{A}$ é um espaço vetorial com respeito a adição e a multiplicação de elementos do corpo,
2) $\mathcal{A}$ é um anel com unidade com respeito a adição e a multiplicação,
3) $(\lambda a)b = a(\lambda b) = \lambda(ab)$, para todo $\lambda \in \mathbb{K}$ e para todo $a, b \in \mathcal{A}$.

Exemplo 2.6.2. O conjunto $M_n(\mathbb{R})$ de matrizes $n \times n$ com entradas em $\mathbb{R}$ é um álgebra sobre $\mathbb{R}$.

Definição 2.6.3. Um homomorfismo de álgebras sobre um corpo $\mathbb{F}$ é um homomorfismo de anéis restrito a identidade de $\mathbb{F}$.

Definição 2.6.4. Uma álgebra $\mathcal{A}$ é um álgebra de divisão se todo elemento não nulo de $\mathcal{A}$ tem inverso multiplicativo.

Exemplo 2.6.5. Seja $\{1, i, j, k\}$ uma base para um espaço vetorial de dimensão 4 sobre $\mathbb{R}$, com i, j, k satisfazendo $i^2 = -1, j^2 = -1, k^2 = -1$ e $k = ij = -ji$. A álgebra

$$\mathcal{H} = \{x + yi + zj + wk \mid x, y, z, w \in \mathbb{R}\}$$

tem uma estrutura de anel com a adição e multiplicação bem definidas. Todo elemento não nulo de $\mathcal{H}$ tem inverso, pois se $x + yi + zj + wk = q \in \mathcal{H}$ é não nulo, basta tomar o conjugado de q que é definido como

$$\overline{q} = x - yi - zj - wk,$$

e então

$$q\overline{q} = x^2 + y^2 + z^2 + w^2 > 0,$$

pois q é não nulo. Assim, o elemento inverso de q é dado por

$$q^{-1} = \frac{\overline{q}}{q\overline{q}}.$$

Definição 2.6.6. Seja $\mathbb{F}$ um corpo de números. O conjunto $\mathcal{A} = (\beta, \gamma)_{\mathbb{F}}$ é uma álgebra, chamada de **álgebra dos quatérnios** sobre $\mathbb{F}$ de dimensão 4 e base $\{1, i, j, k\}$ satisfazendo a condição $i^2 = \beta$, $j^2 = \gamma$, $k = ij = -ji$, onde $\beta, \gamma \in \mathbb{F}/\{0\}$.

Representamos uma álgebra dos quatérnios e as extensões de corpos envolvidas, no diagrama abaixo.

$$\begin{array}{c} \mathcal{A} = (\beta,\gamma)_{\mathbb{F}} \\ \Big| 2 \\ \mathbb{F}(\sqrt{\beta}) \\ \Big| 2 \\ \mathbb{F} \\ \Big| n \\ \mathbb{Q} \end{array}$$

Exemplo 2.6.7. A álgebra $\mathcal{H} = (-1,-1)_{\mathbb{R}}$ definida no Exemplo 2.6.5 é chamada de **álgebra dos quatérnios de Hamilton**.

Exemplo 2.6.8. O anel $M(2,\mathbb{F})$ das matrizes 2×2 com coeficientes em $\mathbb{F}$ é uma álgebra dos quatérnios sobre $\mathbb{F}$. De fato, tem-se que o isomorfismo $\varphi : (1,1)_{\mathbb{F}} \to M(2,\mathbb{F})$ é dado por

$$\varphi(i) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ e } \varphi(j) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Em geral, uma álgebra dos quatérnios $\mathcal{A} = (\beta,\gamma)_{\mathbb{F}}$ sobre um corpo de números $\mathbb{F}$ pode ser vista como uma sub-álgebra do conjunto das matrizes 2×2. Para isso, sejam $\mathcal{A} = (\beta,\gamma)_{\mathbb{F}}$ e M_0, M_1, M_2, M_3 matrizes linearmente independentes de $M(2,\mathbb{F}(\sqrt{\beta}))$ dadas por

$$M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ M_1 = \begin{pmatrix} \sqrt{\beta} & 0 \\ 0 & -\sqrt{\beta} \end{pmatrix},$$
$$M_2 = \begin{pmatrix} 0 & 1 \\ \gamma & 0 \end{pmatrix},\ M_3 = \begin{pmatrix} 0 & \sqrt{\beta} \\ -\gamma\sqrt{\beta} & 0 \end{pmatrix}.$$

Consideremos a aplicação $\varphi : \mathcal{A} \to M(2,\mathbb{F}(\sqrt{\beta}))$ definida por

$$\varphi(x_0 + x_1 i + x_2 j + x_3 k) = x_0 M_0 + x_1 M_1 + x_2 M_2 + x_3 M_3.$$

Das seguintes relações

$$\varphi(i^2) = \beta I_2,\ \varphi(j^2) = \gamma I_2 \text{ e } \varphi(ij) = \varphi(i)\varphi(j) = -\varphi(j)\varphi(i),$$

onde I_2 é a matriz identidade de ordem 2, verifica-se que φ é um isomorfismo de $\mathcal{A} = (\beta,\gamma)_{\mathbb{F}}$ em uma sub-álgebra de $M(2,\mathbb{F}(\sqrt{\beta}))$. Dessa forma, cada elemento de $\mathcal{A}$ é identificado com

$$x \mapsto \varphi(x) = \begin{pmatrix} x_0 + x_1\sqrt{\beta} & x_2 + x_3\sqrt{\beta} \\ \gamma(x_2 - x_3\sqrt{\beta}) & x_0 - x_1\sqrt{\beta} \end{pmatrix}. \tag{2.9}$$

Definimos no Exemplo 2.6.5 o conjugado de um elemento na álgebra. A partir deste conceito é possível caracterizar o traço reduzido e a norma reduzida da forma como são apresentados na próxima definição.

Definição 2.6.9. Seja $\mathcal{A} = (\beta, \gamma)_{\mathbb{F}}$ uma álgebra dos quatérnios. Definimos o **traço reduzido** e a **norma reduzida** de um elemento $x \in \mathcal{A}$ por

$$Tr_{red}(x) = x + \overline{x} \text{ e } N_{red}(x) = x\overline{x}.$$

Exemplo 2.6.10. Seja $\mathcal{H} = (-1, -1)_{\mathbb{R}}$. Se $x = x_0 + x_1 i + x_2 j + x_3 k \in \mathcal{H}$, então

$$Tr_{red}(x) = x + \overline{x} = 2x_0 \text{ e } N_{red}(x) = x_0^2 + x_1^2 + x_2^2 + x_3^2.$$

As álgebras de divisão produzem códigos com diversidade máxima, permitindo assim projetar STBC confiáveis [3]. Deste modo, apresentamos resultados que fornecem condições quando uma álgebra dos quatérnios é uma álgebra de divisão.

Proposição 2.6.11. Seja $\mathcal{A} = (\beta, \gamma)_{\mathbb{F}}$ uma álgebra dos quatérnios. Assim, $\mathcal{A}$ é uma álgebra de divisão se, e somente se, $N_{red}(x) \neq 0$, para todo $x \in \mathcal{A}$.

Demonstração. Suponhamos que existe $x \in \mathcal{A}$ tal que $N_{red}(x) = 0$, isto é, $x\overline{x} = 0$. Se $\mathcal{A}$ é álgebra de divisão, então x e $\overline{x}$ tem inversos multiplicativos. Seja x' o inverso de x e $\overline{x}'$ o inverso de $\overline{x}$. Daí

$$0 = 0\overline{x}'x' = x\overline{x}\overline{x}'x' = x1x' = 1xx' = 1,$$

o que é um absurdo. Logo $N_{red}(x) \neq 0$, para todo $x \in \mathcal{A}$. Reciprocamente, se $x + yi + zj + wk = \alpha \in (\beta, \gamma)_{\mathbb{F}}$, com $\alpha \neq 0$, então

$$\alpha\overline{\alpha} = (x + yi + zj + wk)(x - yi - zj - wk) = x^2 - \beta^2 y - \gamma^2 c + \beta\gamma d^2 \neq 0.$$

Se α^{-1} é dado por

$$\alpha^{-1} = \frac{\overline{\alpha}}{\alpha\overline{\alpha}},$$

então $\alpha\alpha^{-1} = 1$. Logo, todo elemento não nulo tem inverso multiplicativo, ou seja, $\mathcal{A}$ é uma álgebra de divisão. □

Proposição 2.6.12. Seja $\mathcal{A} = (\beta, \gamma)_{\mathbb{F}}$ uma álgebra dos quatérnios. Assim, $\mathcal{A}$ é uma álgebra de divisão se, e somente se, $\gamma \neq N_{\mathbb{F}(\sqrt{\beta})/\mathbb{F}}(x)$ para todo $x \in \mathbb{F}(\sqrt{\beta})$.

Demonstração. Suponhamos que exista um $x \in \mathbb{F}(\sqrt{\beta})$ tal que $N_{\mathbb{F}(\sqrt{\beta})/\mathbb{F}}(x) = \gamma$. Como $x \in \mathbb{F}(\sqrt{\beta})$, segue que $x = a + b\sqrt{\beta}$. Assim,

$$N_{\mathbb{F}(\sqrt{\beta})/\mathbb{F}}(x) = (a + b\sqrt{\beta})(a - b\sqrt{\beta}) = a^2 - \beta b^2 = \gamma.$$

Se $\alpha = a + bi + 1j + 0k \in \mathcal{A}$, então

$$\alpha\overline{\alpha} = a^2 - \beta b^2 - \gamma(1 - \beta 0) = a^2 - \beta b^2 - \gamma = \gamma - \gamma = 0,$$

o que é um absurdo, pela Proposição 2.6.11. Reciprocamente, suponha que exista $\alpha = a + bi + cj + dk \in \mathcal{A}$ tal que $\alpha\overline{\alpha} = 0$. Assim,

$$0 = a^2 - \beta b^2 - \gamma(c^2 - \beta d^2) \Rightarrow a^2 - \beta b^2 = \gamma(c^2 - \beta d^2) \Rightarrow$$
$$N_{\mathbb{F}(\sqrt{\beta})/\mathbb{F}}(x)(a + b\sqrt{\beta}) = \gamma N_{\mathbb{F}(\sqrt{\beta})/\mathbb{F}}(x)(c + d\sqrt{\beta}) \Rightarrow$$

$$N_{\mathbb{F}(\sqrt{\beta})/\mathbb{F}}(x)\left(\frac{a + b\sqrt{\beta}}{c + d\sqrt{\beta}}\right) = \gamma,$$

o que é um absurdo, pois $\dfrac{a+b\sqrt{\beta}}{c+d\sqrt{\beta}} \in \mathbb{F}(\sqrt{\beta})$, e por hipótese, $\gamma \neq N_{\mathbb{F}(\sqrt{\beta})/\mathbb{F}}(x)$, para todo $x \in \mathbb{F}(\sqrt{\beta})$. □

Neste capítulo vimos resultados que nos fornecem uma base teórica para o desenvolvimento do trabalho.

No capítulo subsequente abordamos a teoria de reticulados, pois os códigos de bloco espaço-temporais apresentados no Capítulo 5 estão relacionados com essa teoria. Recentemente, as álgebras de divisão estão sendo utilizadas para construir reticulados com boa densidade de empacotamento, [1].

Capítulo 3

Reticulados

O conceito de reticulado surgiu a partir do problema de como cobrir o espaço $\mathbb{R}^n$ com esferas de mesmo raio, de forma que quaisquer duas esferas se toquem no máximo em um ponto e ocupem a maior parte do espaço possível.

Apesar de problemas relacionados aos reticulados serem estudados pelo menos desde o século XVII, a formalização da teoria da maneira como a conhecemos é relativamente recente, devido aos trabalhos de matemáticos como Fejes Tóth e Rogers, de meados do século XX, [12]. Antes disso, a maioria das referências no tema trata de construções para problemas específicos e não é raro encontrar resultados relevantes acerca de reticulados enunciados em outros contextos como: equações diofantinas, formas quadráticas e teoria dos números. Para o desenvolvimento, deste capítulo, as principais referências utilizadas foram [23], [14], [16], [17] e [19].

3.1 Definições e propriedades

Intuitivamente, entende-se por um reticulado como sendo um subconjunto discreto do $\mathbb{R}^n$ que tem estrutura de um $\mathbb{Z}$-módulo (que é equivalente a ser um grupo abeliano aditivo) de posto finito m. Nesta seção, apresentamos a definição de reticulados e outras definições importantes como região fundamental, matriz de Gram e volume da região fundamental.

Definição 3.1.1. Sejam $\{v_1, v_2, ..., v_m\}$ vetores linearmente independentes do $\mathbb{R}^n$. O conjunto de pontos

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

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

Observe na Definição 3.1.1, que necessariamente $m \leq n$.

Definição 3.1.2. O paralelepípedo formado pelos pontos

$$\theta_1 v_1 + \cdots + \theta_m v_m, \text{ com } 0 \leq \theta_i < 1,$$

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

Exemplo 3.1.3. $\Lambda = \mathbb{Z}^2$ é um reticulado gerado pelos vetores $e_1 = (1, 0)$ e $e_2 = (0, 1)$, e com região fundamental descrita na figura a seguir.

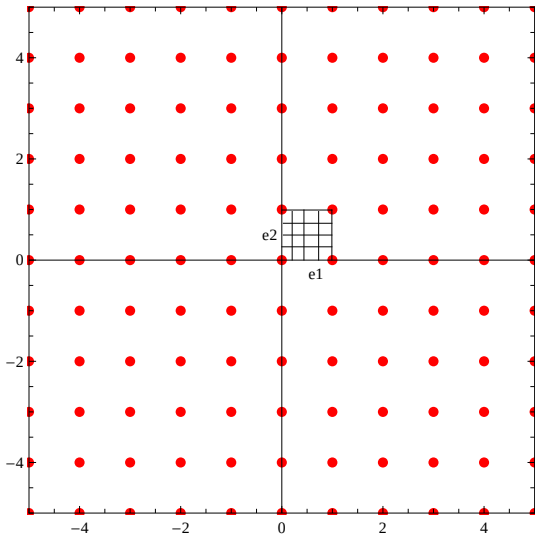


Figura 3.1: Reticulado $\mathbb{Z}^2$

Uma importante característica de um reticulado é que a base não é única. A proposição seguinte dá uma condição necessária e suficiente para que um conjunto de vetores linearmente independentes seja uma base de um dado reticulado.

Proposição 3.1.4. Seja Λ um reticulado com base $\{v_1, \ldots, v_m\}$ e $\{e_1, \ldots, e_m\}$ um conjunto de vetores de Λ linearmente independentes tal que $e_i = \sum_{j=1}^{m} a_{ij} v_j$, com $a_{ij} \in \mathbb{Z}$. Assim, que $\{e_1, \ldots, e_n\}$ é uma base de Λ se, e somente se, $det(A) = \pm 1$, onde $A = (a_{ij})_{i,j=1,\ldots,n}$.

Demonstração. Como

$$\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix},$$

segue que, $\{e_1 \ldots, e_n\}$ é uma base de Λ se, e somente se, $A = (a_{ij})_{i,j=1,\ldots,n}$ é a matriz mudança de base, o que é equivalente a $det(A) = \pm 1$. □

Definição 3.1.5. Seja $\{v_1, \ldots, v_m\}$ uma base do reticulado Λ. Se $v_i = (v_{i1}, \ldots, v_{in})$, para $i = 1, \cdots, m$, a matriz

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

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 e o **volume** de Λ é dado por $vol(\Lambda) = |det(M)|$.

Observação 3.1.6. Existem mais de uma base que determinam o mesmo reticulado Λ, e assim, mais de uma matriz geradora pode determina-lo. No entanto, o módulo do determinante de qualquer matriz geradora de Λ é sempre o mesmo. De fato, sejam $\{f_1, \ldots, f_n\}$ e $\{v_1, \ldots, v_n\}$ duas bases do reticulado Λ tal que $f_i = (f_{i1}, \ldots, f_{in})$ e $v_i = (v_{i1}, \ldots, v_{in})$, para todo i. Se $f_i = \sum_{j=2}^{n} a_{ij} v_j$, com $a_{ij} \in \mathbb{Z}$, então

$$|det(f_{ij})_{i,j=1,\ldots,n}| = |det(a_{ij})_{i,j=1,\ldots,n}||det(v_{ij})_{i,j=1,\ldots,n}| = |det(v_{ij})_{i,j=1,\ldots,n}|,$$

pois $|det(a_{ij})| = 1$.

Desse modo o volume da região fundamental está bem definido.

Observação 3.1.7. Os pontos do reticulado n-dimensional $\Lambda = \Lambda_n(M)$ são formados por

$$\Lambda_n(M) = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}^t = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}^t M \mid z_i \in \mathbb{Z} \text{ para } 1 \leq i \leq n \right\},$$

onde M é uma matriz geradora do reticulado $\Lambda_n(M)$.

Definição 3.1.8. O **determinante do reticulado** Λ é definido como sendo o determinante da matriz G, isto é,

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

Observemos que, se M é uma matriz quadrada, então

$$det(G) = det(MM^t) = det(M)^2.$$

Observação 3.1.9. Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado e M, N duas matrizes geradoras de Λ. Sejam $G_1 = MM^t$ e $G_2 = NN^t$ matrizes de Gram de Λ. Assim, pela Proposição 3.1.4 existe uma matriz inversível A tal que $M = AN$. Logo, $G_1 = ANN^tA^t$. Desta forma, $det(G_1) = det(ANN^tA^t) = (det(A))^2 det(NN^t) = (det(A))^2 det(G_2)$. Como A é inversível, segue que $det(A) = \pm 1$. Assim, $det(G_1) = det(G_2)$. Portanto, o determinante da matriz de Gram independe da matriz geradora utilizada.

Exemplo 3.1.10. Seja Λ um reticulado gerado por $\beta = \{(3, -2, 4), (1, 0, 2), (0, 0, -1)\}$. Uma matriz geradora de Λ é dada por

$$M = \begin{pmatrix} 3 & -2 & 4 \\ 1 & 0 & 2 \\ 0 & 0 & -1 \end{pmatrix},$$

e sua matriz de Gram é dada por

$$G = MM^t = \begin{pmatrix} 3 & -2 & 4 \\ 1 & 0 & 2 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 3 & 1 & 0 \\ -2 & 0 & 0 \\ 4 & 2 & -1 \end{pmatrix} = \begin{pmatrix} 29 & 11 & -4 \\ 11 & 5 & -2 \\ -4 & -2 & 1 \end{pmatrix}.$$

Assim, $det(\Lambda) = det(G) = 4$ e $det(M) = 2$.

Definição 3.1.11. Dado dois vetores $x, y \in \mathbb{R}^n$, definimos a **diversidade**, ou a distância de Hamming, de x e y como

$$div(x,y) = \#\{i, x_i \neq y_i, i = 1, \ldots, n\},$$

onde # representa a cardinalidade do conjunto.

Definição 3.1.12. Dado um subconjunto $S \subset \mathbb{R}^n$, a **diversidade** de S, ou a distância mínima de Hammimg de S, é definida por

$$div(S) = min\{div(x,y)/x \neq y, x, y \in S\}.$$

Como todo reticulado Λ é um subconjunto do $\mathbb{R}^n$, segue que podemos estender as Definições 3.1.11 e 3.1.12 para reticulados. Como reticulados têm estrutura de grupo (com respeito a soma de vetores), podemos reformular a definição de distância de Hamming entre dois vetores da seguinte forma.

Definição 3.1.13. Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado e $x = (x_1, \ldots, x_n) \in \Lambda$.

- A **diversidade** de x é definida como o número de x_i's não nulos.
- A **diversidade** de Λ é definida como $div(\Lambda) = min\{div(x); x \in \Lambda, x \neq 0\}$.

Exemplo 3.1.14. Consideremos o reticulado $\Lambda = \{\lambda M; \lambda \in \mathbb{Z}^4\}$, onde

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix},$$

ou seja, $\Lambda = \{a_1(1,0,0,0) + a_2(0,1,0,0) + a_3(0,0,1,0) + a_4(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}); a_i \in \mathbb{Z}\}$. Assim, $div(\Lambda) = min\{div(x), x \in \Lambda, x \neq 0\} = 1$. Este reticulado é conhecido como D_4.

3.2 Empacotamento esférico

Nesta seção, veremos algumas definições e propriedades como: empacotamento esférico, empacotamento reticulado, norma mínima, densidade de empacotamento e densidade de centro. A densidade de empacotamento é um dos principais tópicos estudados envolvendo reticulados. Dado uma métrica d em $\mathbb{R}^n$, a densidade de empacotamento fornece uma medida de quanto do espaço pode ser coberto por esferas de mesmo raio na métrica d de forma que estas esferas ou não se interceptam, ou se interceptam apenas no bordo. Em cada dimensão busca-se pelo reticulado com a maior densidade de empacotamento possível e são poucas as dimensões em que tais reticulados são conhecidos. A densidade é amplamente estudada para a métrica euclidiana e existem poucas referências de seu estudo na métrica da soma.

Definição 3.2.1.

1. Um **empacotamento esférico**, ou simplesmente um empacotamento no $\mathbb{R}^n$, é uma distribuição de esferas de mesmo raio em $\mathbb{R}^n$ de forma que a interseção de quaisquer duas esferas se interceptem no máximo em um ponto. Um reticulado pode ser descrito indicando apenas o conjunto dos centros das esferas e o raio.

2. Um **empacotamento reticulado** é um empacotamento em que o conjunto dos centros das esferas formam um reticulado Λ no $\mathbb{R}^n$.

Observação 3.2.2. Estudar empacotamentos reticulados equivale ao estudo de reticulados, onde é de interesse empacotamentos associados a um reticulado Λ em que as esferas tenham raio máximo. Para a determinação deste raio, observe que fixado $k > 0$, a interseção do conjunto compacto $\{x \in \mathbb{R}^n; |x| \leq k\}$ com o reticulado Λ é um conjunto finito, visto que Λ é um conjunto discreto. Assim, segue que o número $\Lambda_{min} = min\{|\lambda|; \lambda \in \Lambda, \lambda \neq 0\}$ está bem definido.

Definição 3.2.3. Sejam Λ um reticulado e $\Lambda_{min} = min\{|\lambda| \, , \lambda \in \Lambda, \lambda \neq 0\}$. O número $(\Lambda_{min})^2$ é chamado de **norma mínima** do reticulado.

Observação 3.2.4. O número $\rho = \frac{\Lambda_{min}}{2}$ é o maior raio para o qual é possível distribuir esferas centradas nos pontos de Λ e obter um empacotamento.

Definição 3.2.5. Seja $\mathcal{B}(\rho)$ a esfera com centro na origem e raio ρ. A **densidade de empacotamento** de um reticulado Λ é definida por

$$\Delta(\Lambda) = \frac{\text{volume da região coberta por uma esfera}}{\text{volume da região fundamental}} = \frac{Vol(\mathcal{B}(\rho)}{Vol(\Lambda)} = \frac{Vol(\mathcal{B}(1))\rho^n}{Vol(\Lambda)}.$$

Definição 3.2.6. Definimos a **densidade de centro** de um reticulado Λ por

$$\gamma(\Lambda) = \frac{\rho^n}{Vol(\Lambda)} = \frac{\rho^n}{|det(M)|},$$

onde M é uma matriz geradora do reticulado Λ.

Exemplo 3.2.7. Sejam $\beta = \{(1,0,0),(0,2,0),(1,0,3)\}$ e Λ o reticulado gerado por β. Além disso,

$$\Lambda = \{a(1,0,0) + b(0,2,0) + c(1,0,3); a,b,c \in \mathbb{Z}\} = \{(a+c, 2b, 3c); a,b,c \in \mathbb{Z}\}.$$

Assim, $\Lambda_{min} = min\{|\lambda|, \lambda \in \Lambda, \lambda \neq 0\} = 1$, o que implica que $\rho = \dfrac{\Lambda_{min}}{2} = \dfrac{1}{2}$ é o maior raio para o qual é possível obter um empacotamento. Temos também,

$$Vol(\mathcal{P}_\Lambda) = \left| det \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 1 & 0 & 3 \end{pmatrix} \right| = 6,$$

$$\Delta(\Lambda) = \frac{Vol(\mathcal{B}(1))\rho^3}{Vol(\Lambda)} = \frac{(\frac{4}{3})\pi(\frac{1}{2^3})}{6} = \frac{\pi}{36} \approx 0,0873 \text{ e}$$

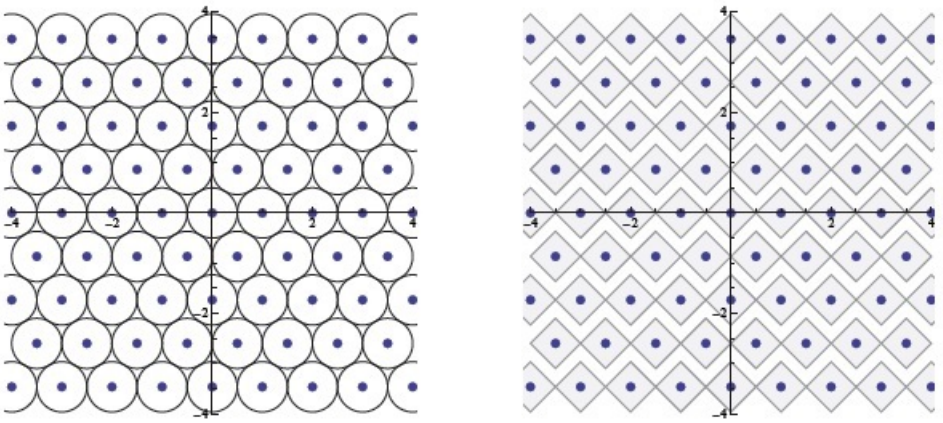
$$\gamma(\Lambda) = \frac{(\frac{1}{2^3})}{6} = \frac{1}{48} \approx 0,020833.$$

Exemplo 3.2.8. Considere o reticulado hexagonal com base $\{(1,0),(1/2,\sqrt{3}/2)\}$ dado pela Figura 3.2. A sua densidade de centro nas métricas euclidiana e da soma são dadas por

$$\Delta_{eucl}(\Lambda) = \frac{1/4\pi}{\sqrt{3}/2} \approx 0,9096 \text{ e } \Delta_{soma}(\Lambda) = \frac{1/4}{\sqrt{3}/2} \approx 0,5773.$$

Este é o empacotamento mais denso em $\mathbb{R}^2$ com a distância euclidiana, até mesmo se comparado com um empacotamento não reticulado.

Observação 3.2.9. Para a métrica euclidiana já foram demonstrados quais são os empacotamentos reticulados mais densos nas dimensões de 1 a 8 [7] e na dimensão 24 [6]. Em algumas outras dimensões são conhecidos empacotamentos reticulados densos, mas nada foi provado.



(a) Métrica euclidiana (b) Métrica da soma

Figura 3.2: Empacotamento de esferas

3.3 Reticulado complexo

A fim de compreender alguns parâmetros dos códigos de bloco que serão apresentados no Capítulo 5, apresentamos a definição de reticulado complexo. A Proposição 3.3.2 é de fundamental importância no cálculo do determinante de reticulados complexos quando transformados em reticulados reais.

Definição 3.3.1. Um reticulado complexo n-dimensional $\Gamma_n(L)$ sobre um reticulado real 2-dimensional $\Lambda_2(M)$ é um subconjunto de $\mathbb{C}^n$ definido por

$$\Gamma_n(L) = \left\{ \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}^t = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}^t L \mid x_i \in \Lambda_2(M) \text{ para } 1 \leq i \leq n \right\},$$

onde L é uma matriz complexa $n \times n$ de posto máximo e M é uma matriz geradora do reticulado $\Lambda_2(M)$.

Seja L uma matriz complexa $n \times n$, dada por

$$L = \begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{n,1} & g_{n,2} & \cdots & g_{n,n} \end{pmatrix},$$

com $|det(L)| > 0$. Definimos $\overline{L}$ por

$$\overline{L} = \begin{pmatrix} Re(g_{1,1}) & -Im(g_{1,1}) & \ldots & Re(g_{1,n}) & -Im(g_{1,n}) \\ Im(g_{1,1}) & Re(g_{1,1}) & \ldots & Im(g_{1,n}) & Re(g_{1,n}) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ Re(g_{n,1}) & -Im(g_{n,1}) & \ldots & Re(g_{n,n}) & -Im(g_{n,n}) \\ Im(g_{n,1}) & Re(g_{n,1}) & \ldots & Im(g_{n,n}) & Re(g_{n,n}) \end{pmatrix}, \tag{3.1}$$

onde $Re(z)$ e $Im(z)$ significam a parte real e a imaginária do elemento z, respectivamente.

Nas mesmas condições das Definição 3.3.1 observamos que, se $(y_1, \ldots, y_n) \in \Gamma_n(L)$, então existem $x_1, \ldots, x_n \in \Lambda_2(M)$ tal que

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}^t = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}^t L.$$

Como $x_k \in \Lambda_2(M)$ para $i = 1, \ldots, n$, segue que $x_k = (x_{k1}, x_{k2})$. Assim, podemos identificá-lo como um número complexo da forma $x_k = x_{k1} + ix_{k2}$. De forma análoga, podemos escrever y_k como $y_k = y_{k1} + iy_{k2}$, com $y_{k1}, y_{k2} \in \mathbb{R}$. Pela Definição 3.1.5, segue que

$$\begin{pmatrix} x_{k1} \\ x_{k2} \end{pmatrix}^t = \begin{pmatrix} z_{k1} \\ z_{k2} \end{pmatrix}^t M, \text{ com } z_{k1}, z_{k2} \in \mathbb{Z}.$$

Portanto, escrevendo $\Gamma_n(L)$ como um reticulado real, se $(Re(y_1), Im(y_1), \ldots, Re(y_n), Im(y_n)) \in \Gamma_n(L)$, então

$$\begin{pmatrix} Re(y_1) \\ Im(y_1) \\ \vdots \\ Re(y_n) \\ Im(y_n) \end{pmatrix}^t = \begin{pmatrix} z_{11} \\ z_{12} \\ \vdots \\ z_{n1} \\ z_{n2} \end{pmatrix}^t \begin{pmatrix} M & & & \\ & M & & \\ & & \ddots & \\ & & & M \end{pmatrix} \overline{L},$$

onde $z_{k1}, z_{k2} \in \mathbb{Z}$. Se $\overline{L}_M = diag\{M, \ldots, M\}\overline{L}$, então para $\overline{L}_M$ ser uma matriz geradora do reticulado real $\Gamma_n(L)$, basta mostrar que seus vetores são linearmente independentes, isto é, mostrar que $\overline{L}_M$ tem posto máximo, o que equivale a mostrar que $|det(\overline{L}_M)| > 0$, o que segue da seguinte proposição.

Proposição 3.3.2. Seja L uma matriz $n \times n$ complexa com $|det(L)| > 0$. Se $\overline{L}$ é a matriz $2n \times 2n$ definida a partir de L como em (3.1), então temos que $|det(L)|^2 = |det(\overline{L})|$.

Demonstração. Sejam L uma matriz complexa $n \times n$ dado por

$$L = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{n1} & g_{n2} & \cdots & g_{nn} \end{pmatrix}$$

com $|det(L)| > 0$, e $\overline{L}$ dado por

$$\overline{L} = \begin{pmatrix} Re(g_{11}) & -Im(g_{11}) & \ldots & Re(g_{1n}) & -Im(g_{1n}) \\ Im(g_{11}) & Re(g_{11}) & \ldots & Im(g_{1n}) & Re(g_{1n}) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ Re(g_{n1}) & -Im(g_{n1}) & \ldots & Re(g_{nn}) & -Im(g_{nn}) \\ Im(g_{n1}) & Re(g_{n1}) & \ldots & Im(g_{nn}) & Re(g_{nn}) \end{pmatrix}, \tag{3.2}$$

onde $Re(z)$ e $Im(z)$ significam a parte real e a imaginária do elemento z, respectivamente. Denotamos por c_i e l_i a i-ésima coluna e a i-ésima linha, respectivamente, e denotamos a permutação da coluna (ou linha) c_i com a coluna (ou linha) c_j por $c_i \leftrightarrow c_j$. Olhando somente a primeira linha de $\overline{L}$, segue que

$$(Re(g_{11}), -Im(g_{11}), \ldots, Re(g_{1n}), -Im(g_{1n})).$$

Definimos a matriz $\overline{L}_{c1}$ como sendo a matriz $\overline{L}$ com a mudança das colunas

$$c_2 \leftrightarrow c_3, c_4 \leftrightarrow c_5, \ldots, c_{2i} \leftrightarrow c_{2i+1}, \ldots, c_{2n-2} \leftrightarrow c_{2n-1}.$$

Assim, a primeira linha de $\overline{L}_{c1}$ é dado por

$$(Re(g_{11}), Re(g_{12}), -Im(g_{11}), Re(g_{13}), \ldots, -Im(g_{1i}), Re(g_{1(i+2)}), -Im(g_{1(i+1)}),\\ Re(g_{1(i+3)}), \ldots, Re(g_{1n}), -Im(g_{1(n-1)}), -Im(g_{1n})).$$

Definimos a matriz $\overline{L}_{c2}$ como sendo a matriz $\overline{L}_{c1}$ com a mudança das colunas

$$c_3 \leftrightarrow c_4, c_5 \leftrightarrow c_6, \ldots, c_{2i+1} \leftrightarrow c_{2i+2}, \ldots, c_{2n-3} \leftrightarrow c_{2n-2}.$$

Assim, a primeira linha de $\overline{L}_{c2}$ é dada por

$$(Re(g_{11}), Re(g_{12}), Re(g_{13}), , \ldots, -Im(g_{1i}), Re(g_{1(i+3)}), -Im(g_{1(i+1)}),\\ Re(g_{1(i+4)}), \ldots, Re(g_{1n}), -Im(g_{1(n-2)}), -Im(g_{1(n-1)}), -Im(g_{1n})).$$

Repetindo esse processo, segue que a matriz $\overline{L}_{c(n-1)}$ tem a primeira linha dada por

$$(Re(g_{11}), Re(g_{12}), \ldots, Re(g_{1n}), -Im(g_{11}), \ldots, -Im(g_{1(n-1)}), -Im(g_{1n})).$$

Como o número de colunas permutadas é $\frac{2n-2}{2}$ no primeiro passo, e $\frac{2n-4}{2}$ no segundo passo, e $\frac{2n-2j}{2}$ no j-ésimo passo, segue que o número de permutações é dado por

$$\sum_{j=1}^{n-1} \frac{2n-2j}{2} = \sum_{j=1}^{n-1} n - j = \frac{(n-1)n}{2}.$$

Repetindo, o mesmo processo, nas linhas da matriz $\overline{L}_{c(n-1)}$, chegamos a uma matriz $\overline{L}_{cl}$ que tem como a primeira coluna dada por

$$(Re(g_{11}), Re(g_{21}), \ldots, Re(g_{n1}), -Im(g_{11}), \ldots, -Im(g_{(n-1)1}), -Im(g_{n1})).$$

Como o número de permutações também é $\frac{(n-1)n}{2}$, segue que o número de permutações de linha e coluna da matriz $\overline{L}$ para $\overline{L}_{cl}$ é $(n-1)n$ que é par. Logo,

$$det(\overline{L}) = (-1)^{(n-1)n} det(\overline{L}_{cl}) = det(\overline{L}_{cl}).$$

Observamos que dado uma elemento $g_{rs} = Re(g_{rs}) + iIm(g_{rs})$ da matriz L, o termo $Re(g_{rs})$ aparece na matriz $\overline{L}$ nas entradas $(2r-1)(2s-1)$ e $(2r)(2s)$, e ao realizar a mudança de $\overline{L}$ para $\overline{L}_{cl}$, segue que o termo da entrada $(2r-1)(2s-1)$ aparece na entrada $(r)(s)$, e o termo da entrada $(2r)(2s)$ aparece na entrada $(r+n)(s+n)$. Já o termo $Im(g_{rs})$ da matriz L aparece na matriz $\overline{L}$ nas entradas $(2r-1)(2s)$ e $(2r)(2s-1)$, sendo que na entrada $(2r-1)(2s)$ seu sinal está trocado. Ao realizar a mudança de $\overline{L}$ para $\overline{L}_{cl}$, segue que o termo da entrada $(2r-1)(2s)$ aparece na entrada $(r)(s+n)$, e o termo da entrada $(2r)(2s-1)$ aparece na entrada $(r+n)(s)$. Assim, dado um elemento g_{rs} em L, segue que

$$L = \begin{pmatrix} g_{11} & \cdots & g_{1s} & \cdots & g_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ g_{r1} & \cdots & g_{rs} & \cdots & g_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ g_{n1} & \cdots & g_{ns} & \cdots & g_{nn} \end{pmatrix},$$

$$\overline{L} = \begin{pmatrix} Re(g_{11}) & -Im(g_{11}) & \ldots & Re(g_{1n}) & -Im(g_{1n}) \\ Im(g_{11}) & Re(g_{11}) & \ldots & Im(g_{1n}) & Re(g_{1n}) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ Re(g_{n1}) & -Im(g_{n1}) & \ldots & Re(g_{nn}) & -Im(g_{nn}) \\ Im(g_{n1}) & Re(g_{n1}) & \ldots & Im(g_{nn}) & Re(g_{nn}) \end{pmatrix},$$

$$\overline{L}_{cl} = \begin{pmatrix} Re(g_{11}) & \ldots & Re(g_{1s}) & \ldots & Re(g_{1n}) & -Im(g_{11}) & \ldots & -Im(g_{1s}) & \ldots & -Im(g_{1n}) \\ \vdots & & & & \vdots & \vdots & & & & \vdots \\ Re(g_{r1}) & \ldots & Re(g_{rs}) & \ldots & & & \ldots & -Im(g_{rs}) & \ldots & \\ \vdots & & & & \vdots & \vdots & & & & \vdots \\ Re(g_{n1}) & \ldots & & \ldots & Re(g_{nn}) & -Im(g_{n1}) & \ldots & & \ldots & -Im(g_{nn}) \\ Im(g_{11}) & \ldots & & \ldots & Im(g_{1n}) & Re(g_{11}) & \ldots & & \ldots & Re(g_{1n}) \\ \vdots & & & & \vdots & \vdots & & & & \vdots \\ Im(g_{r1}) & \ldots & Im(g_{rs}) & \ldots & & & \ldots & Re(g_{rs}) & \ldots & \\ \vdots & & & & \vdots & \vdots & & & & \vdots \\ Im(g_{n1}) & \ldots & & \ldots & Im(g_{nn}) & Re(g_{n1}) & \ldots & & \ldots & Re(g_{nn}) \end{pmatrix}.$$

Portanto, escrevendo $L = A + iB$, com A e B matrizes reais, segue que

$$\overline{L}_{cl} = \begin{pmatrix} A & -B \\ B & A \end{pmatrix}.$$

Portanto,

$$\begin{aligned} det(\overline{L}_{cl}) &= det \begin{pmatrix} A & -B \\ B & A \end{pmatrix} = det \begin{pmatrix} A+iB & -B+iA \\ B & A \end{pmatrix} \\ &= det \begin{pmatrix} A+iB & 0 \\ B & A-iB \end{pmatrix} = det(A+iB)det(A-iB) = |det(L)|^2. \end{aligned}$$

Como $det(\overline{L}) = det(\overline{L}_{cl})$, segue que $|det(L)|^2 = det(\overline{L})$ como queríamos. □

Observação 3.3.3. A Proposição 3.3.2 garante que $\overline{L}_M$ é a matriz geradora do reticulado real $\Gamma_n(L)$ e que o módulo do determinante de $\overline{L}_M$ é dado por

$$|det(\overline{L}_M)| = |det(\overline{L})||det(M)|^n = |det(L)|^2|det(M)|^n.$$

A fim de maximizar a densidade de centro de um reticulado podemos analizar como minimizar $|det(\overline{L}_M)|$.

Exemplo 3.3.4. Seja $\Lambda_2(M)$ um reticulado real 2-dimensional, com

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

Logo, $\Lambda_2(M)$ é da seguinte forma,

$$\begin{aligned}\Lambda_2(M) &= \left\{ \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}^t = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}^t M \mid z_1, z_2 \in \mathbb{Z} \right\} \\ &= \left\{ \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}^t = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}^t \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mid z_1, z_2 \in \mathbb{Z} \right\} \\ &= \left\{ \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}^t \mid z_1, z_2 \in \mathbb{Z} \right\}.\end{aligned}$$

Seja $\Gamma_2(L)$ o reticulado complexo 2-dimensional, com

$$L = \begin{pmatrix} 1 & i \\ -i & -1 \end{pmatrix}.$$

Assim, $\Gamma_2(L)$ é da seguinte forma:

$$\begin{aligned}\Gamma_2(L) &= \left\{ \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}^t = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}^t L \mid x_1, x_2 \in \Lambda_2(M) \right\} \\ &= \left\{ \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}^t = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}^t \begin{pmatrix} 1 & i \\ -i & -1 \end{pmatrix} \mid x_1, x_2 \in \Lambda_2(M) \right\} \\ &= \left\{ \begin{pmatrix} x_1 - ix_2 \\ ix_1 - x_2 \end{pmatrix}^t \mid x_1, x_2 \in \Lambda_2(M) \right\}.\end{aligned}$$

Como $x_1 = (z_{11}, z_{12})$ e $x_2 = (z_{21}, z_{22})$, segue que podemos representa-los da forma $x_1 = z_{11} + iz_{12}$ e $x_2 = z_{21} + iz_{22}$. Assim,

$$\begin{aligned}\Gamma_2(L) &= \left\{ \begin{pmatrix} z_{11} + iz_{12} - i(z_{21} + iz_{22}) \\ i(z_{11} + iz_{12}) - (z_{21} + iz_{22}) \end{pmatrix}^t \mid z_{11}, z_{12}, z_{21}, z_{22} \in \mathbb{Z} \right\} \\ &= \left\{ \begin{pmatrix} z_{11} + z_{22} + i(z_{12} - z_{21}) \\ -z_{12} - z_{21} + i(z_{11} + z_{22}) \end{pmatrix}^t \mid z_{11}, z_{12}, z_{21}, z_{22} \in \mathbb{Z} \right\}.\end{aligned}$$

Para ver $\Gamma_2(L)$ como um reticulado real, tomamos

$$\overline{L} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & -1 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}.$$

Logo,

$\Gamma_2(L) =$

$$\left\{ \begin{pmatrix} Re(y_1) \\ Im(y_1) \\ Re(y_2) \\ Im(y_2) \end{pmatrix}^t = \begin{pmatrix} z_{11} \\ z_{12} \\ z_{21} \\ z_{22} \end{pmatrix}^t \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & -1 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix} \mid z_{11}, z_{12}, z_{21}, z_{22} \in \mathbb{Z} \right\}$$

$$= \left\{ \begin{pmatrix} Re(y_1) \\ Im(y_1) \\ Re(y_2) \\ Im(y_2) \end{pmatrix}^t = \begin{pmatrix} z_{11} + z_{22} \\ z_{12} - z_{21} \\ -z_{12} - z_{21} \\ z_{11} + z_{22} \end{pmatrix}^t \mid z_{11}, z_{12}, z_{21}, z_{22} \in \mathbb{Z} \right\}.$$

Seja $\overline{L}_M = diag\{M, M\}\overline{L}$. Assim, o determinante do reticulado real $\Gamma_2(L)$ é dado por

$$\begin{aligned} |det(\Gamma_2(L))| &= |det(\overline{L}_M)|^2 = |det(M)^2 det(\overline{L})^2|^2 = |det(M)|^4 |det(L)|^4 \\ &= \left|det\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right|^4 \left|det\begin{pmatrix} 1 & i \\ -i & -1 \end{pmatrix}\right|^4 \\ &= 1^4|-2|^4 = 16. \end{aligned}$$

3.4 Reticulados algébricos

Seja $\mathbb{F}$ um corpo de números de grau n. Nesta seção, apresentamos um método para gerar reticulados no $\mathbb{R}^n$ a partir de $\mathbb{F}$. O método consiste em aplicar determinados homomorfismos a certos $\mathbb{Z}$-módulos livres de posto n contidos em $\mathbb{F}$. Os reticulados gerados por este método são conhecidos como reticulados algébricos.

Definição 3.4.1. Sejam $\sigma_1, \cdots, \sigma_n$ os n $\mathbb{Q}$-monomorfismos de um corpo de números $\mathbb{F}$ de grau n, e ordenando os $\sigma_i's$ de modo que, para todo $x \in \mathbb{F}$, $\sigma_i(x) \in \mathbb{R}$, com $1 \leq i \leq r_1$, 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 **monomorfismo canônico** $\sigma : \mathbb{F} \longrightarrow \mathbb{R}^{r_1+2r_2}$ definido por

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

onde $Re(z)$ e $Im(z)$ denotam as partes real e imaginária do número complexo z, respectivamente.

Exemplo 3.4.2. Sejam o corpo quadrático $\mathbb{F} = \mathbb{Q}(i)$, onde $i = \sqrt{-1}$, e $\{\sigma_1, \sigma_2\}$ o grupo dos $\mathbb{Q}$-monomorfismos de $\mathbb{F}$ 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 $x = a + bi \in \mathbb{F}$, com $a, b \in \mathbb{Q}$, segue que $\sigma(x) = (Re(\sigma_1(x)), Im(\sigma_1(x))) = (a, b)$.

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

Teorema 3.4.3. [16] Se $\{w_1, \cdots, w_n\}$ é uma base integral de $\mathbb{F}$ e $\sigma : \mathbb{F} \to \mathbb{C}$ o monomorfismo canônico, então os n vetores $\mathbf{v_i} = \sigma(w_i) \in \mathbb{R}^n$, para $i = 1, \cdots, n$ são linearmente independentes e definem um reticulado em $\mathbb{R}^n$, denominado **reticulado algébrico**.

A proposição que segue é consequência do Teorema 3.4.3.

Proposição 3.4.4. [16] Seja $\mathbb{F}$ um corpo de números de grau n e A um $\mathbb{Z}$-submódulo livre de $\mathbb{F}$ de posto n. Se $(x_i)_{1 \leq i \leq n}$ é uma $\mathbb{Z}$-base de $\mathbb{F}$, então $\sigma(A)$ é um reticulado em $\mathbb{R}^n$.

Como $\mathcal{O}_{\mathbb{F}}$ e seus ideais são $\mathbb{Z}$-módulos livres de posto n, podemos mergulhá-los em $\mathbb{R}^n$ para obter um reticulado algébrico.

Se $\{w_1, \cdots, w_n\}$ é uma $\mathbb{Z}$-base de $A \subset \mathbb{F}$, então a matriz geradora do reticulado $\sigma_{\mathbb{F}}(A) = \left\{ \sum_{i=1}^{n} z_i \sigma_{\mathbb{F}}(w_i),\ z_i \in \mathbb{Z} \right\}$ é dada por

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

Como consequência da Proposição 3.4.4, temos a seguinte Proposição.

Proposição 3.4.5. [16] Se $\mathbb{F}$ é um corpo de números de grau n, $\mathcal{D}_{\mathbb{F}/\mathbb{Q}}$ o discriminante de $\mathbb{F}$, $\mathcal{O}_{\mathbb{F}}$ o anel dos inteiros algébricos de $\mathbb{F}$, I um ideal não nulo de $\mathcal{O}_{\mathbb{F}}$ e r_2 a metade no número de monomorfismos imaginários, então $\sigma_{\mathbb{F}}(\mathcal{O}_{\mathbb{K}})$ e $\sigma_{\mathbb{F}}(I)$ são reticulados, com respectivos volumes,

$$Vol(\sigma_{\mathbb{F}}(\mathcal{O}_{\mathbb{F}})) = 2^{-r_2} |\mathcal{D}_{\mathbb{F}}|^{\frac{1}{2}},$$
$$Vol(\sigma_{\mathbb{F}}(I)) = Vol(\sigma_{\mathbb{F}}(\mathcal{O}_{\mathbb{F}}))N(I).$$

A seguir, apresentamos exemplos de reticulados obtidos através de corpos quadráticos.

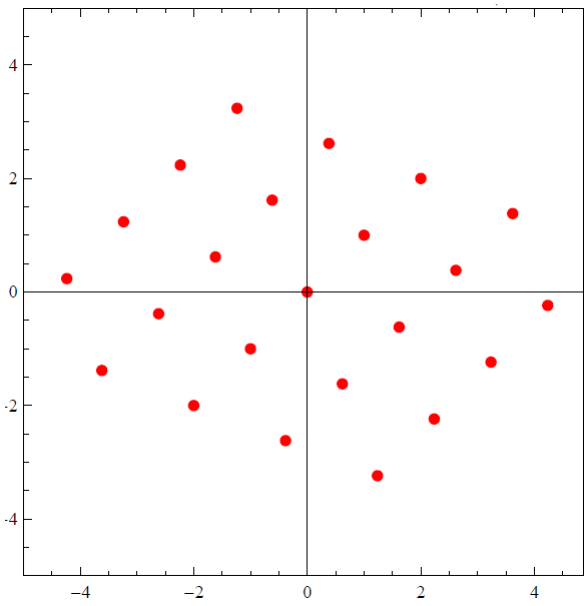


Figura 3.3: Reticulado algébrico construído a partir do corpo $\mathbb{Q}(\sqrt{5})$

Exemplo 3.4.6. Seja $\mathbb{F} = \mathbb{Q}(\sqrt{5})$. A base integral de $\mathbb{F}$ é $\{1, \frac{1+\sqrt{5}}{2}\}$ e $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. Pelo Teorema 3.4.3, segue que $\Lambda = \sigma(\mathcal{O}_{\mathbb{F}})$ é um reticulado em $\mathbb{R}^2$. Os dois monomorfismos são $\sigma_1(\sqrt{5}) = \sqrt{5}$, $\sigma_2(\sqrt{5}) = -\sqrt{5}$. Neste caso, $r_1 = 2$ e $r_2 = 0$, assim a matriz geradora do reticulado é

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

e volume dado por

$$Vol(\sigma_{\mathbb{F}}(\mathcal{O}_{\mathbb{F}})) = 2^{-0}\left|\left[det\begin{pmatrix}\sigma_1(1) & \sigma_1\left(\frac{1+\sqrt{5}}{2}\right)\\ \sigma_2(1) & \sigma_2\left(\frac{1+\sqrt{5}}{2}\right)\end{pmatrix}\right]^2\right|^{\frac{1}{2}} = \left|det\begin{pmatrix}1 & \frac{1+\sqrt{5}}{2}\\ 1 & \frac{1-\sqrt{5}}{2}\end{pmatrix}\right| = \sqrt{5}.$$

Na Figura 3.3, representamos geometricamente o reticulado $\Lambda = \sigma_{\mathbb{F}}(\mathcal{O}_{\mathbb{F}})$.

Exemplo 3.4.7. Seja $\mathbb{F} = \mathbb{Q}(\sqrt{-3})$. A base integral de $\mathbb{F}$ é $\{1, \frac{1+\sqrt{-3}}{2}\}$ e $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. Pelo Teorema 3.4.3, segue que $\Lambda = \sigma(\mathcal{O}_{\mathbb{F}})$ é um reticulado em $\mathbb{R}^2$. Os dois monomorfismos são $\sigma_1(\sqrt{-3}) = \sqrt{-3}$ e $\sigma_2(\sqrt{-3}) = -\sqrt{-3}$. Neste caso, $r_1 = 0$ e $r_2 = 1$. Assim, a matriz geradora do reticulado é dada por

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

e volume dado por

$$\begin{aligned} Vol(\sigma_{\mathbb{F}}(\mathcal{O}_{\mathbb{F}})) &= 2^{-1}\left|\left[det\begin{pmatrix}\sigma_1(1) & \sigma_1\left(\frac{1+\sqrt{-3}}{2}\right)\\ \sigma_2(1) & \sigma_2\left(\frac{1+\sqrt{-3}}{2}\right)\end{pmatrix}\right]^2\right|^{\frac{1}{2}} = \frac{1}{2}\left|det\begin{pmatrix}1 & \frac{1+\sqrt{-3}}{2}\\ 1 & \frac{1-\sqrt{-3}}{2}\end{pmatrix}\right| \\ &= \frac{1}{2}|-i\sqrt{3}| = \frac{1}{2}\sqrt{3}. \end{aligned}$$

Na Figura 3.4, representamos geometricamente o reticulado $\Lambda = \sigma_{\mathbb{F}}(\mathcal{O}_{\mathbb{F}})$.

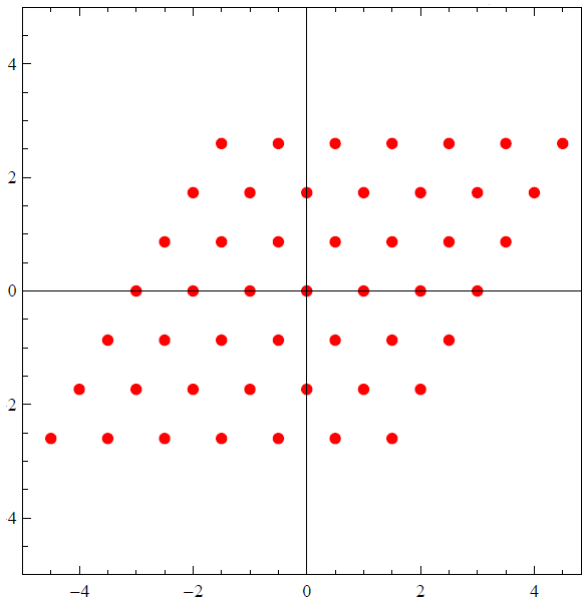


Figura 3.4: Reticulado algébrico construído a partir do corpo $\mathbb{Q}(\sqrt{-3})$

É possível verificar que $\sigma_{\mathbb{F}}(\mathcal{O}_{\mathbb{F}})$ é isomorfo ao reticulado A_2, que é o reticulado de maior densidade de centro na dimensão 2. Para maiores detalhes consultar [17].

Exemplo 3.4.8. Seja $\mathbb{F} = \mathbb{Q}(\sqrt{15})$. A base integral de $\mathbb{F}$ é $\{1, \sqrt{15}\}$ e $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\sqrt{15}]$ o seu anel de inteiros. Pelo Teorema 3.4.3, segue que $\Lambda = \sigma(\mathcal{O}_{\mathbb{F}})$ é um reticulado em $\mathbb{R}^2$. Os dois monomorfismos são $\sigma_1(\sqrt{15}) = \sqrt{15}$ e $\sigma_2(\sqrt{15}) = -\sqrt{15}$. Neste caso, $r_1 = 2$ e $r_2 = 0$. Assim a matriz geradora do reticulado é dada por

$$M = \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(15) & \sigma_2(\sqrt{15}) \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \sqrt{15} & -\sqrt{15} \end{pmatrix},$$

e o volume é dado por

$$Vol(\sigma_{\mathbb{F}}(\mathcal{O}_{\mathbb{F}})) = \left| det \begin{pmatrix} 1 & 1 \\ \sqrt{15} & -\sqrt{15} \end{pmatrix} \right| = 2\sqrt{15}.$$

Neste capítulo apresentamos o conceito de reticulado, empacotamento esférico, reticulado complexo e um método para gerar reticulados no $\mathbb{R}^n$. Reticulados com boa densidade de empacotamento podem ser construídos via álgebra dos quatérnios, por exemplo, em [1] o reticulado de dimensão 8, E_8, é construído através da álgebra dos quatérnios $(5, i)_{\mathbb{Q}(\sqrt{-1})}$, $(-3, -1)_{\mathbb{Q}(\sqrt{-2})}$, $(-7, -1)_{\mathbb{Q}(\sqrt{-3})}$ e $(-1, -1)_{\mathbb{Q}(\sqrt{-7})}$.

No próximo capítulo abordamos a teoria de números p-ádicos e anel de valorização. Apresentamos o Lema de Hensel e mostramos que certos elementos do anel de inteiros algébricos de $\mathbb{Q}(\sqrt{d})$ não são normas algébricas de uma extensão de $\mathbb{Q}(\sqrt{d})$. Estes resultados são de fundamental importância para construir códigos de blocos no Capítulo 5 .

Capítulo 4

Números p-ádicos e Anel de Valorização

Os números p-ádicos e a análise p-ádica são aspectos extremamente importantes da teoria dos números moderna. Quando se escolhe o valor absoluto clássico e se toma o completamento de $\mathbb{Q}$ em relação a métrica induzida, o resultado é o corpo dos números reais. Quando se faz o mesmo com um outros valores absolutos possíveis, pode se obter um dos corpos p-ádicos Q_p.

Neste capítulo, apresentamos os números p-ádicos, o Lema de Hensel e algumas de suas propriedades. O Lema de Hensel é uma importante ferramenta para mostrar que alguns elementos não são normas algébricas de certas extensões. Para o desenvolvimento deste capítulo a principal referência utilizada é [8]. Os Corolário 4.2.4 e 4.2.5 são algumas de nossas contribuições originais deste trabalho.

4.1 Valorização p-ádica

Nesta seção, apresentamos o conceito de valor absoluto não arquimediano e de valorização p-ádica, que servem como base para o Lema de Hensel. No que segue, consideremos p um número primo.

Definição 4.1.1. Seja $\mathbb{F}$ um corpo. O valor absoluto em $\mathbb{F}$ é uma função $|\ |:\mathbb{F}\to\mathbb{R}_+$ satisfazendo as seguinte condições:
i) $|x|=0\Leftrightarrow x=0$,
ii) $|xy|=|x||y|,\forall x,y\in\mathbb{F}$,
iii) $|x+y|\leq|x|+|y|,\forall x,y\in\mathbb{F}$.
Um valor absoluto se diz não arquimediano se satisfaz a condição adicional:
iv) $|x+y|\leq max\{|x|,|y|\},\forall x,y\in\mathbb{F}$,
caso contrário, o valor absoluto se diz arquimediano.

Exemplo 4.1.2. Um exemplo de valor absoluto não arquimediano é dado por $|x|=0$ se $x=0$ e $|x|=1$ se $x\neq 0$.

Teorema 4.1.3. Sejam $\mathbb{K}$ um corpo e $|\ |$ um valor absoluto não arquimediano em $\mathbb{F}$. Se $x,y\in\mathbb{K}$ e $|x|\neq|y|$, então

$$|x+y| = max\{|x|, |y|\}.$$

Demonstração. Sem perda de generalidade, podemos assumir $|x| > |y|$. Por definição, $|x+y| \leq max\{|x|, |y|\} = |x|$. Por outro lado, $x = (x+y) - y$, e assim,

$$|x| \leq max\{|x+y|, |y|\}.$$

Como $|x| > |y|$, segue que $|x| \leq max\{|x+y|, |y|\} = |x+y|$. Assim, $|x| = |x+y|$. □

Observemos que este teorema fornece uma importante relação entre valores absolutos não arquimedianos, que diz que dentre os valores $|x|, |y|$ e $|x+y|$ tem dois deles que são iguais, e denominamos isto por *propriedade não arquimedianidade.*

Definição 4.1.4. Seja $x \in \mathbb{Z}$, com $x \neq 0$, A valorização p-ádica de x é definida como sendo o maior inteiro não-negativo m, tal que $p^m | x$, ou seja

$$x = p^m b \text{ com } (p, b) = 1,$$

onde $(\ ,\ )$ indica o máximo divisor comum entre dois números. Denotamos o valor p-ádico de x por $v_p(x)$. Se $x = \frac{a}{b} \in \mathbb{Q}^*$, definimos a valorização p-ádica de x por

$$v_p(x) = v_p(a) - v_p(b).$$

E por último, definimos $v_p(0) = +\infty$.

Lema 4.1.5. Se $x, y \in \mathbb{Q}$, então
i) $v_p(xy) = v_p(x) + v_p(y)$,
ii) $v_p(x+y) \geq min\{v_p(x), v_p(y)\}$.

Demonstração. Basta usar a Definição 4.1.4. □

Definição 4.1.6. Para qualquer $x \in \mathbb{Q}$, definimos o valor absoluto p-ádico de x por

$$|x|_p = p^{-v_p(x)},$$

convencionando que $|0|_p = 0$.

Definição 4.1.7. Seja $|\ | = |\ |_p$ um valor absoluto não arquimediano em $\mathbb{Q}$. Definimos

$$C = \{(x_n), x_n \in \mathbb{Q}\ \forall n, (x_n) \text{ é uma sequência de Cauchy em relação a } |\ |_p\},$$

e

$$N = \{(x_n), x_n \in \mathbb{Q}\ \forall n,\ x_n \to 0 \text{ com relação a } |\ |_p\}.$$

Definindo as operações de adição e multiplicação em C da seguinte forma

$$(x_n) + (y_n) = (x_n + y_n) \text{ e}$$
$$(x_n)(y_n) = (x_n y_n),$$

é possível mostrar que essas operações C é anel comutativo com unidade e que N é um ideal de C.

Proposição 4.1.8. O ideal N é maximal em C.

Demonstração. Seja $(x_n) \in C - N$, e I o ideal gerado por (x_n) e por N. Queremos provar que $I = C$. Como $(x_n) \in C - N$, é possível exibir um número $c > 0$ e um inteiro n_0 tal que $|x_n|_p \geq c > 0$, sempre que $n \geq n_0$. Considere, então, a sequência (y_n) definida por $y_n = 0$ se $n < n_0$ e $y_n = \frac{1}{x_n}$ se $n \geq n_0$. Em primeiro lugar, para $n \geq n_0$, temos

$$|y_{n+1} - y_n|_p = \left| \frac{1}{x_{n+1}} - \frac{1}{x_n} \right|_p = \frac{|x_{n+1} - x_n|_p}{|x_n x_{n+1}|_p} \leq \frac{|x_{n+1} - x_n|}{c^2} \to 0,$$

de modo que $(y_n) \in C$. Observemos que

$$x_n y_n = \begin{cases} 0, & \text{se } n < n_0 \\ 1, & \text{se } n \geq n_0 \end{cases}.$$

Seja (z_n) um sequência, onde $z_n = 1$, se $n < n_0$ e $z_n = 0$, se $n \geq n_0$. Temos que $z_n \to 0$, e portanto $(z_n) \in N \subset I$. Como I é um ideal, segue que $(x_n)(y_n) \in I$, e assim $(x_n)(y_n) + (z_n) = (1) \in I$. Logo $I = C$, como queríamos. □

O fato de N ser um ideal maximal de C garante que $\dfrac{C}{N}$ possui uma estrutura de corpo.

Definição 4.1.9. O corpo de números p-ádicos é o corpo quociente

$$Q_p = \frac{C}{N}.$$

Podemos definir uma função de $\mathbb{Q}$ em Q_p, onde cada elemento de $\mathbb{Q}$ é levado na sequência constante, e assim, essas sequências são as inclusões de $\mathbb{Q}$ em Q_p.

Lema 4.1.10. Se $(x_i) \in C - N$, então a sequência de números reais $|x_i|_p$ se estabiliza, isto é, existe n_0 tal que

$$\text{se } n, m \geq n_0, \text{ então } |x_n|_p = |x_m|_p.$$

Demonstração. Seja $(x_i) \in C - N$. Como (x_i) não tende a zero, segue que existem $c \in \mathbb{R}$ e $n_1 \in \mathbb{Z}$ tal que

$$\text{se } n \geq n_1, \text{ então } |x_n|_p \geq c > 0.$$

Por outro lado, como a sequência é de Cauchy, segue que existe n_2 tal que

$$\text{se } n, m \geq N_2, \text{ então } |x_n - x_m|_p < c.$$

Logo, se $n_0 = max\{n_1, n_2\}$, então

$$|x_n - x_m|_p < c \leq max\{|x_n|_p, |x_m|_p\}, \text{ para todo } n, m \geq n_0,$$

o que implica $|x_n|_p = |x_m|_p$ pela propriedade da não arquimedianidade. □

Definição 4.1.11. Sejam $\alpha \in Q_p$ e (x_n) um representante da classe α. Definimos $|\alpha| = \lim\limits_{n \to \infty} |x_n|_p$.

Usando o Lema 4.1.10, é fácil de mostrar que Q_p é um corpo completo.

4.2 Lema de Hensel

Nesta seção, apresentamos o Lema de Hensel e algumas de suas consequências. Este lema é uma importante ferramenta para mostrar que alguns elementos não são normas algébricas de certas extensões de corpos de números.

Definição 4.2.1. O anel dos inteiros p-ádicos é $Z_p = \{\alpha \in Q_p, |\alpha|_p \leq 1\}$. Um elemento $\alpha \in Z_p$ é chamado de unidade se $|\alpha|_p = 1$.

Lema 4.2.2. (Lema de Hensel) [18] Seja $f(x) \in Z_p[x]$. Se existe $a_0 \in Z_p$ que satisfaz

$$|f(a_0)|_p < |f'(a_0)|_p^2,$$

onde $f'(x)$ é a derivada formal, então existe $a \in Z_p$ tal que $f(a) = 0$.

Demonstração. Sejam $f_1(x) \in Z_p[x]$ e $f_2(x, y) \in Z_p[x, y], j = 1, 2$, definidas pela identidade

$$f(x + y) = f(x) + f_1(x)y + f_2(x, y)y^2. \tag{4.1}$$

Assim,

$$f'(x) = \lim_{y\to 0} \frac{f(x + y) - f(x)}{y} = \lim_{y\to 0} \frac{f_1(x)y - f_2(x)y^2}{y} = f_1(x).$$

Se $b_0 = \dfrac{-f(a_0)}{f_1(a_0)}$, então $b_0 \in Z_p$, pois como $f_1(x) \in Z_p$ e por hipótese, temos

$$|b_0|_p = \left|\frac{f(a_0)}{f_1(a_0)}\right|_p < \frac{|f'(a_0)|_p^2}{|f_1(a_0)|_p} < |f_1(a_0)|_p \leq 1,$$

onde a primeira desigualdade vem da hipótese e a segunda de $f_1(x) \in Z_p[x]$ e $a_0 \in Z_p$. Assim, $f(a_0) + b_0 f_1(a_0) = f(a_0) + \dfrac{-f(a_0)}{f_1(a_0)} f_1(a_0) = 0$. Como $f_2(x, y) \in Z_p[x, y]$ e $a, b_0 \in Z_p$, pela Equação (4.1), segue que

$$|f(a_0 + b_0)|_p = |f(a_0) + f_1(a_0)b_0 + f_2(a_0, b_0)b_0^2|_p = |f_2(a_0, b_0)b_0^2|_p \leq |b_0^2|_p = \frac{|f(a_0)|_p^2}{|f_1(a_0)|_p^2} <$$
$$\frac{|f(a_0)|_p}{|f_1(a_0)|_p^2} |f(a_0)|_p < |f(a_0)|_p.$$

Novamente, pela Equação (4.1), segue que

$$f(a_0 + b_0) = f(a_0) + f_1(a_0)b_0 + f_2(a_0, b_0)b_0^2$$

e

$$f(a_0) = f(a_0 + b_0 - b_0) = f(a_0 + b_0) + f_1(a_0 + b_0)(-b_0) + f_2(a_0 + b_0, -b_0)b_0^2.$$

Somando as duas equações acima, segue que

$$f_1(a_0 + b_0) - f_1(a_0) = b_0(f_2(a_0, b_0) + f_2(a_0 + b_0, -b_0)).$$

Logo,

$$|f_1(a_0 + b_0) - f_1(a_0)|_p \leq |b_0| < |f_1(a_0)|_p,$$

e assim, $|f_1(a_0+b_0)|_p = |f_1(a_0)|_p$ pela propriedade da não arquimedianidade, pois a propriedade garante que dentre os 3 valores $|-f_1(a_0)|_p, |f_1(a_0+b_0)|_p$ e $|f_1(a_0+b_0)-f_1(a_0)|_p$, tem-se que 2 deles são iguais. Se $a_1 = a_0+b_0$, então $|f(a_1)|_p < |f(a_0)|_p$ e $|f'(a_1)|_p = |f'(a_0)|_p$. Logo, $|f(a_1)|_p < |f'(a_0)|_p^2$, e por hipótese, que $a_1 \in Z_p$. Repetindo o processo, construímos uma sequência $a_{n+1} = a_n + b_n$, com $b_n = \dfrac{-f(a_n)}{f'(a_n)}$ tal que

$$|f(a_{n+1})|_p < |f(a_n)|_p,\ |f'(a_n)|_p = |f'(a_0)|_p \text{ e } |f(a_{n+1})|_p \leq |b_n|_p^2 = \left|\frac{f(a_n)}{f'(a_n)}\right|_p^2.$$

Seja $t = \left|\dfrac{f(a)}{f'(a)^2}\right|_p < 1$. Queremos mostrar que $|f(a_n)|_p \leq |f'(a_n)|_p^2 t^{2^{n-1}}$. Por indução temos que, para $n=1$, segue que

$$|f(a_1)|_p = |f'(a_1)|_p^2 \frac{|f(a_1)|_p}{|f'(a_1)|_p^2} = |f'(a_1)|_p^2 t = |f'(a_1)|_p^2 t^{2^0}.$$

Suponha que a desigualdade seja válida para n. Assim,

$$|f(a_{n+1})|_p \leq \left|\frac{f(a_n)}{f'(a_n)}^2\right|_p = \frac{|f(a_n)|_p^2}{|f'(a_1)|_p^2} \leq \frac{(|f'(a_1)|_p^2 t^{2^{n-1})^2}}{|f'(a_1)|_p^2} = \frac{|f'(a_1)|_p^4 t^{2^n}}{|f'(a_1)|_p^2} = |f(a_1)|_p^2 t^{2^{(n+1)-1}}.$$

Portanto, com $n \to \infty$ tem-se que $|f'(a_n)|_p^{2^{n-1}} \to 0$, o que implica que $|f(a_n)|_p \to 0$. Além disso,

$$|a_{n+1} - a_n|_p = |b_n|_p = \frac{|f(a_n)|_p}{|f_1(a_n)|_p} = |f_1(a_n)|_p t^{2^{n-1}}.$$

Portanto (a_n) é uma sequência de Cauchy e, pela completude segue que, converge para algum a. Se mostrarmos que $f(a_n) \longrightarrow f(a)$, pela unicidade do limite, segue que $f(a) = 0$. Se $f(x) = c_0 + c_1 x + \ldots + c_d c^d$, então

$$\begin{aligned}
|f(a_n) - f(a)|_p &= |c_1(a_n - a) + \ldots + c_r(a_n^d - a^d)|_p \\
&\leq \max_{1\leq k\leq d}\{|c_k|_p |a_n^k - a^k|_p\} \\
&\leq \max_k\{|a_n^k - a^k|_p\} \\
&= |a_n - a|_p \max_k\{1, |a_n^{k-1} + a_n^{k-2}a + \ldots + a_n a^{k-2} + a^{k-1}|_p\} \\
&\leq |a_n - a|_p.
\end{aligned}$$

Como $(a_n) \to a$, segue que $f(a_n) \to f(a)$. Portanto $f(a) = 0$, logo concluímos o resultado. □

Este Lema possui varias aplicações interessantes, como por exemplo:

Exemplo 4.2.3. Seja $b \in \mathbb{Z}$ com $b \equiv 1\ (mod\ 8)$. Tomando $f(x) = x^2 - b$, segue que $|f(1)|_2 \leq 2^{-3}$ e $|f'(1)|_2 = 2^{-1}$. Assim, existe $a \in Z_2$ tal que $a^2 = b$, ou seja, b tem raiz em Z_2.

Corolário 4.2.4. Seja $d \in \mathbb{Z}$. Se $d \equiv 1\,(mod\,3)$, então o número inteiro -1 não é norma algébrica da extensão $\mathbb{Q}(\sqrt{d}, \sqrt{-3})$ sobre $\mathbb{Q}(\sqrt{d})$.

Demonstração. Provamos que não existe $x \in \mathbb{Q}(\sqrt{d}, \sqrt{-3})$ tal que $N_{\mathbb{Q}(\sqrt{d},\sqrt{-3})/\mathbb{Q}(\sqrt{d})}(x) = -1$. Para isso vamos trabalhar nas extensões do corpo 3-ádico Q_3. Como $d \in \mathbb{Z}$, segue que $v_3(d) \geq 0$, e assim $d \in Z_3$. Tomando $f(x) = x^2 - d$, segue que $f(x) \in Z_3[x]$. Como $d \equiv 1\,(mod\,3)$, segue que $f(1) = 1 - d \equiv 0\,(mod\,3)$, assim $v_3(1-d) \geq 1$. além disso $f'(x) = 2x$, assim $f'(1) = 2$, e desse modo $v_3(f'(1)) = 0$. Logo, se $v_3(f(1)) \geq 1$, então $|f(1)|_3 \leq 3^{-1}$, e $v_3(f'(1)) = 0$, então $|f'(1)|_3 = 1$. Portanto, $|f(1)|_3 < |f'(1)|_3$. Assim, pelo Lema de Hensel 4.2.2, segue que $\exists \gamma \in Z_3$ tal que $f(\gamma) = 0$, ou seja $\gamma^2 - d = 0$. Logo, $\sqrt{d} \in Z_3 \subset Q_3$, ou seja, $\mathbb{Q}(\sqrt{d})$ pode ser visto como um subcorpo de Q_3. Similarmente, $\mathbb{Q}(\sqrt{d}, \sqrt{-3})$ pode ser visto como um subcorpo de $Q_3(\sqrt{-3})$. Além disso, podemos definir a aplicação $N_{\mathbb{Q}(\sqrt{d},\sqrt{-3})|\mathbb{Q}(\sqrt{d})} : \mathbb{Q}(\sqrt{d}, \sqrt{-3}) \to \mathbb{Q}(\sqrt{d})$ como sendo a restrição da norma $N : Q_3(\sqrt{-3}) \to Q_3$, onde $N(r + s(\frac{1+\sqrt{-3}}{2})) = (r + \frac{s}{2})^2 + 3(\frac{s}{2})^2, \forall r, s \in Q_3$. Fazendo uma mudança de variável da forma $a = r + \frac{s}{2}$ e $b = \frac{s}{2}$, assim $N(r + s(\frac{1+\sqrt{-3}}{2})) = (r + \frac{s}{2})^2 + 3(\frac{r}{2})^2 = a^2 + 3b^2$. Para mostrar o resultado, basta provar que -1 não é imagem de N. Para isso, suponhamos que existam a e b números 3-ádicos tal que $a^2 + 3b^2 = -1$. Mostramos primeiro que a e b estão em Z_3, isto é $|a|_3 \leq 1$ e $|b|_3 \leq 1$. Para isso, suponhamos que pelo menos um deles tem um valorização 3-ádica negativa.

- Se $v_3(a) < 0$, então $v_3(a^2) = 2v_3(a) < 0$ e $|a^2|_3 > 1$. Como $|a^2+3b^2|_3 = |-1|_3 = 1$ e pela propriedade da não arquimedianidade, segue que $v_3(a^2) = v_3(3b^2)$.

- Se $v_3(b) < 0$, então $2v_3(b) < 0$. Como $v_3(3b^2) = v_3(3) + v_3(b^2) = 1 + 2v_3(b)$ e $v_3(n) \in \mathbb{Z}$, $\forall n \in \mathbb{Q}$, segue que

$$v_3(b) < 0 \Rightarrow v_3(b) \leq -1 \Rightarrow 2v_3(b) \leq -2 \Rightarrow 2v_3(b) + 1 \leq -1.$$

  Logo $|3b^2| = 3^{-(2v_3(b)+1)} > 3^{-(-1)} = 3 > 1 = |-1| = |a^2 + 3b^2|$. Portanto, pela propriedade da não arquimedianidade, segue que $v_3(a^2) = v_3(3b^2)$.

Portanto, $2v_3(a) = v_3(a^2) = v_3(3b^2) = 1 + 2v(b)$. Assim, existe $t \in \mathbb{Z}$, com $t < 0$, tal que $a = 3^t a'$ e $b = 3^{t-1/2}b'$, onde a' e b' são unidades ($|a'|_3 = |b'|_3 = 1$), o que implica que $a^2 + 3b^2 = 3^{2t}a'^2 + 3^{2t}b' = 3^{2t}(a'^2 + b'^2)$. Como a' e b' são unidades, segue que $v_3(a') = v_3(b') = 0$, assim,

$$a', b' \equiv 1 \text{ ou } 2\,(mod\,3) \Rightarrow a'^2, b'^2 \equiv 1\,(mod\,3) \Rightarrow a'^2 + b'^2 \equiv 2\,(mod\,3).$$

Logo, $v_3(a^2 + b^2) = 2t$ é um número negativo, pois $t < 0$. Logo, $0 > v_3(a^2 + 3b^2) = v_3(-1) = 0$, o que é um absurdo. Portanto $v_3(a) \geq 0$ e $v_3(b) \geq 0$, e assim, a e b estão em Z_3.

Neste caso o resultado decorre de que o quadrado de um número inteiro é sempre congruente a 0 ou 1 módulo 3. Como $3b^2 \equiv 0\,(mod\,3)$ temos que a^2 não pode ser congruente a 2 módulo 3. Em particular, a soma a^2+3b^2 não pode ser igual a -1, pois $-1 \equiv 2\,(mod\,3)$. Deste modo, -1 não é imagem da aplicação N. Como a norma de $\mathbb{Q}(\sqrt{d}, \sqrt{-3})$ sobre $\mathbb{Q}(\sqrt{d})$ é uma restrição de N, temos que -1 não é norma algébrica desta extensão. □

Corolário 4.2.5. Seja $d \in \mathbb{Z}$ com $d \equiv 1\ (mod\ 8)$, então o número inteiro -1 não é norma algébrica da extensão $\mathbb{Q}(\sqrt{d}, i)$ sobre $\mathbb{Q}(\sqrt{d})$.

Demonstração. Vamos provar que não existe $x \in \mathbb{Q}(\sqrt{d}, i)$ tal que $N_{\mathbb{Q}(\sqrt{d},i)/\mathbb{Q}(\sqrt{d})}(x) = -1$. Para isso, vamos trabalhar nas extensões do corpo 2-ádico Q_2. Como

$$d \equiv 1 \ (mod\ 8) \Rightarrow 8|d-1 \Rightarrow 2|d-1 \Rightarrow 2 \text{ não divide } d \Rightarrow |d| = 1,$$

segue que $d \in Z_2$. Tomando $b = d$ no Exemplo 4.2.3 concluímos pelo Lema de Hensel 4.2.2, que $\sqrt{d} \in Z_2 \subset Q_2$. Assim $\mathbb{Q}(\sqrt{d})$ pode ser visto como um subcorpo de Q_2. Similarmente, $\mathbb{Q}(\sqrt{d}, i)$ pode ser visto como um subcorpo de $Q_2(i)$. Além disso, podemos definir a aplicação $N_{\mathbb{Q}(\sqrt{d},i)|\mathbb{Q}(\sqrt{d})} : \mathbb{Q}(\sqrt{d}, i) \to \mathbb{Q}(\sqrt{d})$ como sendo a restrição da norma $N : Q_2(i) \to Q_2$, onde $N(a + bi) = a^2 + b^2$, para todo $a, b \in Q_2$. Para mostrar o resultado, basta provar que -1 não é imagem de N. Suponhamos que existam a e b números 2-ádico tal que $a^2 + b^2 = -1$. Mostramos, primeiro, que a, $b \in Z_2$, isto é $|a| \leq 1$ e $|b| \leq 1$. Assumimos que pelo menos um deles tem valorização 2-ádica negativa, isto é, $v_2(a) < 0$ ou $v_2(b) < 0$. Como $v_2(a^2 + b^2) = v_2(-1) = 0$, segue que $|-1| = 2^{-v_2(-1)} = 1$, e sem perda de generalidade, segue que

$$v_2(a) < 0 \Rightarrow v_2(a^2) = 2v_2(a) < 0 \Rightarrow |a^2| = 2^{-v_2(a)} > 1.$$

A propriedade da não-arquimediana implica que $2v_2(a) = v_2(a^2) = v_2(b^2) = 2v_2(b)$, e portanto, $v_2(a) = v_2(b)$. Assim, existe um número inteiro $t < 0$ tal que $a = 2^t a'$ e $b = 2^t b'$, com a', b' unidades 2-ádicas, isto é, $|a'| = |b'| = 1$. Logo

$$a^2 + b^2 = a^{2t}a'^2 + b^{2t}b'^2 = 2^{2t}(a'^2 + b^2).$$

Como a' e b' são unidades 2-ádicas, segue que

$$v_2(a') = v_2(b') = 0 \Rightarrow a' \equiv b' \equiv 1 \,(mod\, 2) \Rightarrow a'^2 \equiv b'^2 \equiv 1 \,(mod\, 2) \Rightarrow a'^2 \equiv b'^2 \equiv 1 \ (mod\ 4).$$

Logo, $2|a'^2+b'^2$ e 4 não divide $a'^2+b'^2$. Portanto, $a'^2+b'^2 = 2k$, com k ímpar. Portanto,

$$a^2 + b^2 = 2^{2t}(a'^2 + b'^2) = 2^{2t}2k = 2^{2t+1}k, \text{ com } mdc(2, k) = 1.$$

Assim, $v_2(a^2+b^2) = 2t+1$ é um número inteiro ímpar, e portanto, a^2+b^2 não pode ser uma unidade 2-ádica, o que é uma contradição. Logo, $v_2(a) \geq 0$ e $v_2(b) \geq 0$, assim, a e b são inteiros. Neste caso, o resultado decorre de que o quadrado de um número inteiro é sempre congruente a $0, 1$ ou 4 módulo 8. Assim, a soma de dois quadrados não pode ser congruente a 7 módulo 8. Em particular, a soma $a^2 + b^2$ não pode ser igual a -1, pois $-1 \equiv 7 \,(mod\, 8)$. Deste modo, -1 não é imagem da aplicação N. Como a norma de $\mathbb{Q}(\sqrt{d}, i)$ sobre $\mathbb{Q}(\sqrt{d})$ é uma restrição de N, temos que -1 não é norma algébrica desta extensão. □

Neste capítulo apresentamos a teoria de números p-ádicos e o Lema de Hensel, que possui importantes aplicações aos STBC's, por exemplo, nas construções do Golden Code e do Silver Code, e também é uma ferramenta para a construção dos códigos do capítulo seguinte.

O próximo capítulo é dedicado aos principais resultados deste trabalho, em que abordamos os códigos de bloco espaço-temporais quadráticos baseados em extensões quadráticas imaginária dos racionais. Para isso, apresentamos o modelo do sistema MIMO e os critérios para modelas códigos espaços-temporais.

Capítulo 5

Códigos de Bloco Espaço-Temporais via Corpos Quadráticos Imaginários

Neste capítulo, apresentamos as contribuições inéditas deste trabalho. Veremos, na Seção 5.2, que as duas principais exigências para se construir bons STBC's é construí-los com diversidade máxima e maior determinante mínimo. A partir da estrutura de álgebra apresentamos uma construção de STBC via $\mathbb{Q}(\sqrt{d})$, com $d < 0$ e d inteiro livre de quadrados. Assim, os códigos construídos possuem diversidade máxima.

Veremos, no Lema 5.3.5, que o determinante mínimo desses códigos possuem valor constante igual a 1. Portanto, como avaliar tais códigos? A fim de responder esta questão, apresentamos um critério dado em [23] que aqui chamamos de *critério produto*.

Seguindo as ideias de [24], em que os autores apresentam os melhores STBC's em termos do critério produto considerando somente as extensões de $\mathbb{Q}(\sqrt{d})$ com $d = -1, -3$ sobre os racionais, neste trabalho, além de reformular algumas demonstrações apresentadas em [24], apresentamos os melhores STBC considerando extensões de $\mathbb{Q}(\sqrt{d})$ com $d = -2, -7, -11$. Dentre todas as extensões consideradas, analisamos o STBC ótimo segundo o critério mencionado.

Iniciamos o capítulo apresentando um modelo do sistema MIMO e descrevemos critérios para que a probabilidade de erro seja minimizada. Para o desenvolvimento deste capítulo, as principais referências utilizadas foram [5], [3], [15], [4], [10], [22], [23] e [24].

5.1 O modelo do sistema MIMO

De modo a descrever o modelo do canal no caso geral, consideremos primeiramente, como um exemplo, o caso em que temos duas antenas transmissoras e duas antenas receptoras, que é o caso que abordamos neste trabalho (ver Figura 5.1).

Os símbolos x_1, x_2, x_3 e x_4 são transmitidos. A primeira (respectivamente, a segunda) antena envia os símbolos x_1 e x_2 (respectivamente x_3 e x_4). Primeiro, os dois símbolos x_1 e x_3 são enviados sobre o canal, e são recebidos por duas antenas, que produzem os símbolos recebidos y_1 e y_3, onde cada y_i é uma combinação de x_1 e x_3, enfraquecidos por coeficientes de desvanecimento h_{ij}. Em seguida, os dois outros sím-

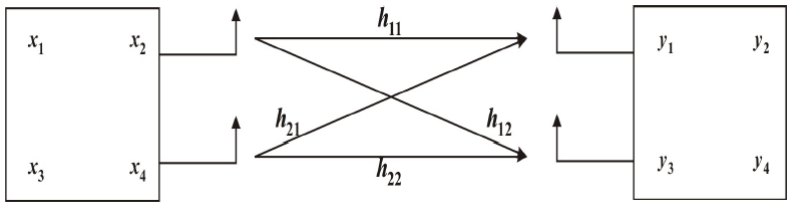


Figura 5.1: Modelo de Sistema MIMO 2×2

bolos x_2 e x_4 são enviados, e analogamente, serão recebidos dois símbolos y_2 e y_4. Em seguida, a palavra código transmitida pode ser escrita como uma matriz X contendo quatro símbolos x_1, x_2, x_3, x_4 e a palavra código recebida é uma matriz Y que é da forma

$$Y = HX + Z, \tag{5.1}$$

onde H é a matriz do canal e Z é uma matriz ruído.

Isto pode ser generalizado para qualquer número de antenas (o número de antenas transmissoras e receptoras não precisa ser o mesmo). Ou seja, sejam n_t o número de antenas transmissoras e n_r o número de antenas receptoras. Se $y(t) \in \mathbb{C}^{n_r}$ é o vetor (coluna) recebido no tempo t, escrevemos

$$y(t) = H(t)x(t) + Z(t),$$

onde a matriz $H(t) \in \mathbb{C}^{n_r \times n_t}$ representa o canal, o vetor coluna $x(t) \in \mathbb{C}^{n_t}$ é o vetor de entrada no canal e $Z(t) \in \mathbb{C}^{n_r}$ é o vetor ruído Gaussiano com média zero, independente e identicamente distribuído. Aqui, assumimos um modelo de canal com desvanecimento do tipo Rayleigh plano, isto é, os elementos de $H(t)$ são independentes e identicamente distribuído com média zero e distribuição Gaussiana complexa de variância unitária. O canal é assumido ser um bloco de tempo invariante, isto é, $H(t)$ é independente de t através de uma transmissão de um bloco de m símbolos, digamos $H(t) = H$ (embora $H(t)$ possa variar de bloco em bloco).

Olhando para um único bloco de comprimento m e assumindo que o canal tenha tempo invariante, podemos escrever

$$\begin{aligned} Y &= [y(1), \ldots, y(m)] \\ &= H[x(1), \ldots, x(m)] + [z(1), \ldots, z(m)] \\ &= HX + Z, \end{aligned} \tag{5.2}$$

que é uma generalização da Equação (5.1).

A palavra código transmitida X pertence a um código, chamado de *Código Espaço-Temporal* (STC) $\mathcal{C}$. Os símbolos de informações são tomados de uma constelação de sinais (ou um alfabeto) S, que são codificados em uma palavra código X. A terminologia código espaço-temporal para múltiplas antenas vem do fato de que estamos codificando sobre o espaço (pois temos várias antenas) e "tempo". Um conjunto infinito de matrizes complexas é um *Código de Bloco Espaço-Temporal* (STBC).

5.2 Critérios para modelar códigos espaço-temporais

O critério para modelar códigos espaço-temporais 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, que é o caso considerado neste trabalho, o receptor recupera a informação exata sobre o estado do canal (isto também é 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. O caso não-coerente, foi tratado nas referências [2] e [9].

Para o caso coerente, 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, ou seja,

$$P(e) \leq \frac{1}{|\mathcal{C}|} \sum_{x \in \mathcal{C}} \sum_{\hat{X} \neq X} P(X \longrightarrow \hat{X}), \tag{5.3}$$

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 ($h_{ij} \sim N_c(0,1)$), segue que

$$P(X \longrightarrow \hat{X}) \leq \det \left[I_{n_t} + \frac{(X - \hat{X})(X - \hat{X})^\dagger}{4N_0} \right]^{-n_r}, \tag{5.4}$$

onde $\dagger$ denota a matriz transposta conjugada, e N_0 a densidade espectral da potência de ruído.

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

$$A = (X - \hat{X})(X - \hat{X})^\dagger \tag{5.5}$$

podemos reescrever a Equação (5.5) como

$$P(X \longrightarrow \hat{X}) \leq \prod_{j=1}^{r} \left(1 + \frac{\lambda_j}{4N_0} \right)^{-n_r}. \tag{5.6}$$

Para alta relação sinal-ruído, ou seja, N_0 pequeno, segue que

$$P(X \longrightarrow \hat{X}) \leq \delta^{-n_r} \left(\frac{1}{4N_0} \right)^{-rn_r}, \tag{5.7}$$

onde $\delta = \prod_{j=1}^{r} \lambda_j$. Assim,

$$P(X \longrightarrow \hat{X}) \leq \left(\frac{\delta^{1/r}}{4N_0} \right)^{-rn_r}. \tag{5.8}$$

No caso de códigos de posto máximo ($r = n_t$), segue que $\delta = \det(A) = \prod_{j=1}^{n_t} \lambda_j \neq 0$ para todo A, e nesse caso, dizemos que o código tem *diversidade máxima*. Desse modo a Equação (5.8) pode ser reescrita como

$$P(X \longrightarrow \hat{X}) \leq \left(\frac{(4N_0)^{n_t}}{det((X-\hat{X})(X-\hat{X})^{\dagger})} \right)^{n_r}. \tag{5.9}$$

No caso de códigos com diversidade máxima, o termo dominante da união limitada (Equação (5.3)) é dado por

$$det_{min}(\mathcal{C}) = \min_{X \neq \hat{X}} det((X-\hat{X})(X-\hat{X})^{\dagger}), \tag{5.10}$$

chamado *determinante mínimo* do código $\mathcal{C}$. O termo $(det_{min}(\mathcal{C}))^{1/n_t}$ é conhecido como *ganho de codificação* [20].

Consequentemente, para minimizar a probabilidade de erro descrita acima é necessário considerar:

1. **Diversidade máxima:** para atingir diversidade máxima $n_t n_r$, a matriz $(X-\hat{X})$ deve ter posto total para qualquer par de palavras código X e $\hat{X}$, isto é,

$$det(X-\hat{X}) \neq 0. \tag{5.11}$$

   Códigos que atingem a diversidade máxima são chamados de *totalmente diversos*.

2. **Determinante mínimo**: se a diversidade $n_t n_r$ é atingida, então o determinante mínimo da Equação (5.10) deve ser maximizado.

No caso de códigos proveniente de uma álgebra, a soma ou a diferença de quaisquer duas palavras código é uma palavra código, isto é, $X - \hat{X} = \mathcal{X}$. Portanto, a união limitada reduz a

$$P(e) \leq \frac{1}{|\mathcal{C}|} \sum_{X \neq 0} P(0 \longrightarrow X), \tag{5.12}$$

e da Equação (5.9), segue que

$$P(X \longrightarrow \hat{X}) \leq \left(\frac{(4N_0)^{r_t}}{|det(\mathcal{X})|^2} \right)^{n_r}. \tag{5.13}$$

Se o código $\mathcal{C}$ é procedente de um reticulado Λ então vale a desigualdade da Equação (5.13) e o determinante mínimo $det_{min}(\Lambda)$ do reticulado Λ é dado por

$$d_{min}(\Lambda) = \min_{0 \neq X \in \Lambda} |det(X)|. \tag{5.14}$$

No caso de duas antenas transmissoras ($n_t = 2$), segue que o ganho de codificação coincide com $det_{min}(\Lambda)$. Como o determinante mínimo determina a probabilidade de erro assintótica ponto a ponto, segue que o mesmo da origem a medidas numéricas para avaliar a qualidade de um reticulado.

De [11] o *determinante mínimo normalizado* de Λ é definido como

$$\delta(\Lambda) = \frac{d_{min}(\Lambda)}{vol(\Lambda)^{-2n_t}} = \frac{d_{min}(\Lambda)}{|\det(M)|^{-2n_t}}, \tag{5.15}$$

onde M é uma matriz geradora do reticulado Λ, e o ganho de codificação de Λ é definido como $\delta(\Lambda)^2$. Quando $d_{min}(\Lambda) = 1$, podemos avaliar a qualidade do código em termos do ganho de codificação do reticulado Λ. Com isso,

$$\text{menor } det(M) \implies \text{maior } \delta(\Lambda)^2.$$

Além disso, de acordo com a Definição 3.2.6, segue que

$$\text{menor } det(M) \implies \text{maior } \gamma(\Lambda) \text{ (densidade de centro).}$$

Isto significa que podemos empacotar mais palavras códigos dentro de um mesmo espaço e com isso as chances de decodificarmos corretamente serão maiores.

Vamos tratar deste assunto nas próximas seções em que um dos objetivos será obter menor $det(M)$.

Devido a linearidade de álgebras, códigos definidos a partir de álgebras satisfazem

$$det(X_i - X_j) = det(X), \text{ com } X_i \neq X_j,\ X \in \mathcal{C}.$$

A fim de obter diversidade máxima em códigos definidos a partir de álgebras, na próxima seção veremos quando $det(X) \neq 0$, para todo $X \neq 0$.

5.3 Códigos de bloco espaço-temporais

Nesta seção apresentaremos e estudaremos um critério de comparação baseado na Seção 3.3. Apresentamos, também, os melhores códigos de bloco espaço-temporais quadráticos considerando extensões de $\mathbb{Q}(\sqrt{d})$, com $d = -1$ e -3.

Primeiramente, vamos definir um STBC considerando duas antenas transmissoras e duas antenas receptoras.

Definição 5.3.1. Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d}, \sqrt{\beta})$ uma extensão quadrática de $\mathbb{F} = \mathbb{Q}(\sqrt{d})$, com $d < 0$ e d um inteiro livre de quadrados. O STBC $\mathcal{C}$ é definido como sendo o conjunto de matrizes da forma

$$\mathcal{C} = \left\{ X = \begin{pmatrix} x_0 + x_1\sqrt{\beta} & x_2 + x_3\sqrt{\beta} \\ \gamma(x_2 - x_3\sqrt{\beta}) & x_0 - x_1\sqrt{\beta} \end{pmatrix} \mid x_0, x_1, x_2, x_3 \in \mathcal{O}_{\mathbb{F}} \right\}.$$

onde $\gamma \in \mathcal{O}_{\mathbb{F}}$ é um número escolhido de forma que $\gamma \neq N_{\mathbb{K}/\mathbb{F}}(x)$, para todo $x \in \mathbb{K}$.

Vimos, na Seção 2.6, que cada elemento de uma álgebra dos quatérnios $\mathcal{A} = (\beta, \gamma)_{\mathbb{F}}$ pode ser identificada com uma matriz 2×2. Comparando a matriz (2.9) com o código $\mathcal{C}$, vemos que as matrizes são as mesmas, a menos do elemento γ que aqui é escolhido de modo conveniente.

De acordo com a Proposição 2.6.11, se $\mathcal{A} = (\beta, \gamma)_{\mathbb{F}}$ é uma álgebra de divisão e $\gamma \in \mathcal{O}_{\mathbb{F}}$, então a exigência sobre γ na Definição 5.3.1 é satisfeita, e portanto podemos definir o código de bloco $\mathcal{C}$ considerando a álgebra de divisão $\mathcal{A} = (\beta, \gamma)_{\mathbb{F}}$, $\mathbb{F} = \mathbb{Q}(\sqrt{d})$,

com $d < 0$ e d um inteiro livre de quadrados. Dentre os códigos construídos a partir de álgebra dos quatérnios podemos citar como exemplo, o código de ouro (Golden Code) e o código de prata (Silver Code) que são construídos usando as álgebras $\mathcal{A} = (5, i)_{\mathbb{Q}(i)}$ e $\mathcal{A} = (-1, -1)_{\mathbb{Q}(\sqrt{-7})}$, respectivamente. Estas construções podem ser encontradas nas referências [5] e [10].

No artigo [24], os autores propõem uma outra estrutura de STBC, chamada de Código de Bloco Espaço-Temporal Quadrático e que apresentamos a seguir.

Sejam $\mathbb{F}$ um corpo de números, $x^2 + px + q$ um polinômio irredutível sobre $\mathbb{F}$, com $p, q \in \mathcal{O}_{\mathbb{F}}$, o anel de inteiro de $\mathbb{F}$. O polinômio $x^2 + px + q$ tem duas raízes, a saber;

$$\alpha_1 = \frac{-p + \sqrt{p^2 - 4q}}{2} \notin \mathbb{F} \text{ e } \alpha_2 = \frac{-p - \sqrt{p^2 - 4q}}{2} \notin \mathbb{F}.$$

Se $\mathbb{K} = \mathbb{F}(\alpha_1)$, então $[\mathbb{K} : \mathbb{F}] = 2$ e $\{1, \alpha_1\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{F}$. Sejam σ_1 e σ_2, os dois mergulhos de $\mathbb{K}$ em $\mathbb{C}$ que fixam $\mathbb{F}$ e $\sigma_1(\alpha_1) = \alpha_1, \sigma_2(\alpha_1) = \alpha_2$.

Definição 5.3.2. Um **código de bloco espaço-temporal quadrático** (QSTBC) $\mathcal{C}(\mathbb{F}, \alpha_1, \alpha_2, \gamma)$ baseado em um polinômio quadrático irredutível $x^2 + px + q \in \mathcal{O}_{\mathbb{F}}[x]$ sobre $\mathbb{F}$, onde $\mathbb{F}$ é um corpo de números, é definido por

$$\mathcal{C}(\mathbb{F}, \alpha_1, \alpha_2, \gamma) = \left\{ X = \begin{pmatrix} x_1(1) + x_1(2)\alpha_1 & x_2(1) + x_2(2)\alpha_1 \\ \gamma(x_2(1) + x_2(2)\alpha_2) & x_1(1) + x_1(2)\alpha_2 \end{pmatrix} \mid x_k(1), x_k(2) \in \mathcal{O}_{\mathbb{F}}, k = 1, 2 \right\},$$

onde $\gamma \in \mathcal{O}_{\mathbb{F}}$ é um número escolhido de forma que $\gamma \neq N_{\mathbb{F}(\alpha_1)/\mathbb{F}}(x)$, para todo $x \in \mathbb{F}(\alpha_1)$.

Observação 5.3.3. Para fins de notação, podemos considerar

$$X = \begin{pmatrix} y_1(1) & y_2(1) \\ \gamma y_2(2) & y_1(2) \end{pmatrix}, \text{ onde } \begin{pmatrix} y_k(1) \\ y_k(2) \end{pmatrix} = \begin{pmatrix} 1 & \alpha_1 \\ 1 & \alpha_2 \end{pmatrix} \begin{pmatrix} x_k(1) \\ x_k(2) \end{pmatrix},$$

com $\gamma, x_k(1), x_k(2) \in \mathcal{O}_{\mathbb{F}}$ para $k = 1, 2$, α_1, α_2 duas raízes do polinômio irredutível, e γ não é norma algébrica de $\mathbb{F}(\alpha_1)$ sobre $\mathbb{F}$.

Podemos associar o código da Definição 5.3.2 com a álgebra de divisão $\mathcal{A} = (p^2 - 4q, \gamma)_{\mathbb{F}}$, onde essa associação é dada no diagrama abaixo.

$$\begin{array}{ccc} \mathbb{K} = \mathbb{F}\left(\underbrace{\dfrac{-p + \sqrt{p^2 - 4q}}{2}}_{\alpha_1}\right) & & (p^2 - 4q, \gamma)_{\mathbb{F}} \\ \Big| 2 & & \Big| 2 \\ \mathbb{F} & \simeq & \mathbb{F}(\sqrt{p^2 - 4q}) \\ \Big| n & & \Big| 2 \\ \mathbb{Q} & & \mathbb{F} \\ & & \Big| n \\ & & \mathbb{Q} \end{array}$$

Um STBC é um reticulado sobre $\mathcal{O}_{\mathbb{F}} \times \mathcal{O}_{\mathbb{F}}$, com uma matriz geradora do reticulado complexo dada por

$$L = \begin{pmatrix} 1 & 1 & 0 & 0 \\ \alpha_1 & \alpha_2 & 0 & 0 \\ 0 & 0 & 1 & \gamma \\ 0 & 0 & \alpha_1 & \gamma\alpha_2 \end{pmatrix}.$$

Portanto, o valor absoluto do determinante da matriz geradora L é dado por

$$|det(L)| = |\gamma||\alpha_1 - \alpha_2|^2 = |\gamma||\sqrt{p^2 - 4q}|^2 = |\gamma||p^2 - 4q|. \tag{5.16}$$

Observação 5.3.4. A partir da Definição 5.3.2, se $X \in \mathcal{C}(\mathbb{F}, \alpha_1, \alpha_2, \gamma)$, então

$$\begin{aligned} det(X) &= y_1(1)y_1(2) - \gamma y_2(1)y_2(2) \\ &= (x_1(1) + \alpha_1 x_1(2))(x_1(1) + \alpha_2 x_1(2)) - \gamma(x_2(1) + \alpha_1 x_2(2))(x_2(1) + \alpha_2 x_2(2)), \end{aligned}$$

e assim, tomando $x_1 = x_1(1) + \alpha_1 x_1(2)$ e $x_2 = x_2(1) + \alpha_1 x_2(2)$, temos que

$$det(X) = N_{\mathbb{F}(\alpha_1)/\mathbb{F}}(x_1) - \gamma N_{\mathbb{F}(\alpha_1)/\mathbb{F}}(x_2).$$

Portanto, como γ não é norma algébrica de $\mathbb{F}(\alpha_1)$ sobre $\mathbb{F}$, segue que se $X \neq 0$, então $det(X) \neq 0$. Além disso, como $\gamma \in \mathcal{O}_\mathbb{F}$ e pela Proposição 2.3.5, $N_{\mathbb{F}(\alpha_1)/\mathbb{F}}(x_1), N_{\mathbb{F}(\alpha_1)/\mathbb{F}}(x_2) \in \mathcal{O}_\mathbb{F}$, segue que $det(X) \in \mathcal{O}_\mathbb{F}$.

O próximo Lema nos diz que quando consideramos corpos quadráticos totalmente imaginários, o determinante mínimo do QSTBC é igual a 1.

Lema 5.3.5. Se $\mathbb{F} = \mathbb{Q}(\sqrt{d})$, com $d < 0$ e d um inteiro livre de quadrados, então qualquer $\mathcal{C}(\mathbb{F}, \alpha_1, \alpha_2, \gamma)$ possui $d_{min}(\mathcal{C}(\mathbb{F}, \alpha_1, \alpha_2, \gamma)) = 1$.

Demonstração. Se $\mathcal{C} \in X(\mathbb{F}, \alpha_1, \alpha_2, \gamma)$, pela Observação 5.3.4, segue que

$$det(X) = N_{\mathbb{F}(\alpha_1)/\mathbb{F}}(x_1) - \gamma N_{\mathbb{F}(\alpha_1)/\mathbb{F}}(x_2),$$

onde $x_1 = x_1(1) + \alpha_1 x_1(2)$ e $x_2 = x_2(1) + \alpha_1 x_2(2)$. Além disso, se $X \neq 0$, então $det(X) \neq 0$ e $det(X) \in \mathcal{O}_\mathbb{F}$. Logo, $d_{min}(\mathcal{C}(\mathbb{F}, \alpha_1, \alpha_2, \gamma)) \geq 1$. Agora, tomando X da forma $x_1(1) = 1, x_1(2) = x_2(1) = x_2(2) = 0$, segue que $y_1(1) = y_1(2) = 1, y_2(1) = y_2(2) = 0$, e assim, $det(X) = 1$. Portanto, $d_{min}(\mathcal{C}(\mathbb{F}, \alpha_1, \alpha_2, \gamma)) = 1$, o que completa a prova. □

Com base no Lema 5.3.5, os códigos que construiremos possuem diversidade máxima (Observação 5.3.4). Assim, para avaliar a eficiência de um QSTBC adotamos um critério que denominamos por *critério produto*.

Sejam $\mathcal{C}(\mathbb{F}, \alpha_1, \alpha_2, \gamma)$ um reticulado complexo sobre $\mathcal{O}_\mathbb{F} \times \mathcal{O}_\mathbb{F}$ com matriz geradora L, M uma matriz geradora do reticulado obtido via $\mathcal{O}_\mathbb{F}$ e $\overline{L}_M$ a matriz geradora do reticulado real. Vimos, na Seção 3.3, que

$$|det(\overline{L}_M)| = |det(L)|^2 |det(M)|^4.$$

Denotamos $\sqrt{|det(\overline{L}_M)|}$ por $g_{prod}(\mathcal{C}(\mathbb{F}, \alpha_1, \alpha_2, \gamma))$, isto é,

$$g_{prod}(\mathcal{C}(\mathbb{F}, \alpha_1, \alpha_2, \gamma)) = |det(L)||det(M)|^2.$$

Definição 5.3.6. (Critério Produto) Sejam $\mathcal{C}(\mathbb{F},\alpha_1,\alpha_2,\gamma_1)$ e $\mathcal{C}(\mathbb{K},\beta_1,\beta_2,\gamma_2)$, com $d_{min}(\mathcal{C}(\mathbb{F},\alpha_1,\alpha_2,\gamma_1)) = d_{min}(\mathcal{C}(\mathbb{K},\beta_1,\beta_2,\gamma_2))$. Dizemos que $\mathcal{C}(\mathbb{F},\alpha_1,\alpha_2,\gamma_1)$ é melhor, ou seja, possui maior ganho de codificação que $\mathcal{C}(\mathbb{K},\beta_1,\beta_2,\gamma_2)$ se

$$g_{prod}(\mathcal{C}(\mathbb{F},\alpha_1,\alpha_2,\gamma_1)) \leq g_{prod}(\mathcal{C}(\mathbb{K},\beta_1,\beta_2,\gamma_2)).$$

Nas condições da Definição 5.3.6 e da Equação (5.16) segue que se $\mathcal{C}(\mathbb{F},\alpha_1,\alpha_2,\gamma_1)$ e $\mathcal{C}(\mathbb{K},\beta_1,\beta_2,\gamma_2)$ são reticulados sobre $\mathcal{O}_\mathbb{F}\times\mathcal{O}_\mathbb{F}$ e $\mathcal{O}_\mathbb{K}\times\mathcal{O}_\mathbb{K}$, respectivamente, com M_1 uma matriz geradora do reticulado $\Lambda_{\mathcal{O}_\mathbb{F}}$ e M_2 uma matriz geradora do reticulado $\Lambda_{\mathcal{O}_\mathbb{K}}$, e $d_{min}(\mathcal{C}(\mathbb{F},\alpha_1,\alpha_2,\gamma_1)) = d_{min}(\mathcal{C}(\mathbb{K},\beta_1,\beta_2,\gamma_2))$, então $\mathcal{C}(\mathbb{F},\alpha_1,\alpha_2,\gamma_1)$ é melhor que $\mathcal{C}(\mathbb{K},\beta_1,\beta_2,\gamma_2)$ se

$$|\gamma_1||\alpha_1-\alpha_2|^2|det(M_1)|^2 \leq |\gamma_2||\beta_1-\beta_2|^2|det(M_2)|^2. \tag{5.17}$$

O cálculo do valor do $g_{prod}(\mathcal{C})$ de um código $\mathcal{C}$ representa o valor do módulo do determinante da matriz geradora de um código $\mathcal{C}$ proveniente de um reticulado, e pela Seção 5.2, possuir o menor valor do módulo do determinante da matriz geradora representa ter maior ganho de codificação e maior densidade de centro, isto significa que podemos empacotar mais palavra códigos dentro de um mesmo espaço, e assim, as chances de decodificarmos corretamente serão maiores.

Definição 5.3.7. Seja S um conjunto de QSTBC, onde $d_{min}\mathcal{C} = d_{min}\overline{\mathcal{C}}$ para todo $\mathcal{C},\overline{\mathcal{C}} \in S$. Dizemos que $\mathcal{C}$ é um QSTBC **ótimo** em S, se

$$g_{prod}(\mathcal{C}) \leq g_{prod}(\overline{\mathcal{C}}),$$

para todo $\overline{\mathcal{C}} \in S$.

Observamos que códigos associados a uma mesma álgebra, podem terem $g_{prod}(\cdot)$ diferentes, conforme o seguinte exemplo.

Exemplo 5.3.8. Sejam os códigos $\mathcal{C}_1 = \mathcal{C}(\mathbb{Q}(\sqrt{-2}),\sqrt{-3},-\sqrt{-3},\gamma)$, $\mathcal{C}_2 = \mathcal{C}(\mathbb{Q}(\sqrt{-2}),\frac{1+\sqrt{-3}}{2},\frac{1-\sqrt{-3}}{2},\gamma)$ e M uma matriz geradora do reticulado $\Lambda_{\mathbb{Z}(\sqrt{-2})}$. Observamos que $\mathcal{C}_1$ e $\mathcal{C}_2$ estão associados a álgebra $(-3,\gamma)_{\mathbb{Q}(\sqrt{-2})}$. Usando a Equação (5.17), segue que

$$g_{prod}(\mathcal{C}_1) = |\gamma||\sqrt{-3}-(-\sqrt{-3})|^2|detM|^2 = |\gamma||2\sqrt{-3}|^2|detM^2| = 12|\gamma||detM|^2$$

e

$$g_{prod}(\mathcal{C}_2) = |\gamma|\left|\frac{1+\sqrt{-3}}{2}-\frac{1-\sqrt{-3}}{2}\right|^2|detM|^2 = |\gamma||\sqrt{-3}|^2|detM|^2 = 3|\gamma||detM|^2.$$

Logo, $g_{prod}(\mathcal{C}_1) > g_{prod}(\mathcal{C}_2)$.

Teorema 5.3.9. Se $\mathcal{C}(\mathbb{F},\alpha_1,\alpha_2,\gamma)$, onde $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ e com $d<0$ um inteiro livre de quadrados, então

$$g_{prod}(\mathcal{C}(\mathbb{F},\alpha_1+p_0,\alpha_2+p_0,\gamma)) = g_{prod}(\mathcal{C}(\mathbb{F},\alpha_1,\alpha_2,\gamma)),$$

para qualquer $p_0 \in \mathcal{O}_\mathbb{F}$.

Demonstração. Pelo Lema 5.3.5 segue que $d_{min}(\mathcal{C}(\mathbb{F},\alpha_1,\alpha_2,\gamma)) = 1 = d_{min}(\mathcal{C}(\mathbb{F},\alpha_1 + p_0,\alpha_2+p_0,\gamma))$. Se α_1 e α_2 são as duas raízes do polinômio irredutível x^2+px+q sobre $\mathbb{F}$, então α_1+p_0 e α_2+p_0 são raízes do polinômio

$$(x-\alpha_1-p_0)(x-\alpha_2-p_0) = x^2+(p-2p_0)x+(q-p_0p+p_0^2),$$

com $p-2p_0, q-p_0p+p_0^2 \in \mathcal{O}_{\mathbb{F}}$ e $\alpha_1+p_0, \alpha_2+p_0 \notin \mathbb{F}$. Assim, o polinômio $(x-\alpha_1-p_0)(x-\alpha_2-p_0)$ é irredutível sobre $\mathbb{F}$. Como $\alpha_1 \in \mathbb{F}(\alpha_1+p_0)$ e $\alpha_1+p_0 \in \mathbb{F}(\alpha_1)$, segue que $\mathbb{F}(\alpha_1+p_0) = \mathbb{F}(\alpha_1)$. Além disso, as matrizes geradoras de $\mathcal{C}(\mathbb{F},\alpha_1,\alpha_2,\gamma)$ e $\mathcal{C}(\mathbb{F},\alpha_1+p_0,\alpha_2+p_0,\gamma)$ são $diag(L_1,L_2)$ e $diag(L_3,L_4)$, respectivamente, com

$$L_1 = \begin{pmatrix} 1 & 1 \\ \alpha_1 & \alpha_2 \end{pmatrix}, L_2 = \begin{pmatrix} 1 & \gamma \\ \alpha_1 & \gamma\alpha_2 \end{pmatrix}, L_3 = \begin{pmatrix} 1 & 1 \\ \alpha_1+p_0 & \alpha_2+p_0 \end{pmatrix} \text{ e}$$
$$L_4 = \begin{pmatrix} 1 & \gamma \\ \alpha_1+p_0 & \gamma(\alpha_2+p_0) \end{pmatrix}.$$

Portanto, $det(L_1) = det(L_3)$ e $det(L_2) = det(L_4)$. Pelo critério produto, segue que $g_{prod}(\mathcal{C}(\mathbb{F},\alpha_1+p_0,\alpha_2+p_0,\gamma)) = g_{prod}(\mathcal{C}(\mathbb{F},\alpha_1,\alpha_2,\gamma))$. □

A próxima observação é uma ferramenta muito importante quando formos calcular os melhores QSTBC's.

Observação 5.3.10. Nas condições do Teorema 5.3.9, segue que se

$$g_{prod}(\mathcal{C}(\mathbb{F},\alpha_1,\alpha_2,\gamma)) = g_{prod}(\mathcal{C}(\mathbb{F},\alpha_1+p_0,\alpha_2+p_0,\gamma)) \text{ então}$$
$$|det(M)|^2|\alpha_1-\alpha_2|^2|\gamma| = |det(M)|^2|(\alpha_1-p_0)-(\alpha_2-p_0)|^2|\gamma|.$$

Além disso, o polinômio irredutível de α_1 sobre $\mathbb{F}$ é $(x-\alpha_1)(x-\alpha_2) = x^2+px+q$ e o polinômio irredutível de α_1-p_0 sobre $\mathbb{F}$ é

$$(x-\alpha_1-p_0)(x-\alpha_2-p_0) = x^2+(p-2p_0)x+(q-p_0p+p_0^2) = x^2+p'x+q'.$$

Assim, dado $\mathcal{C}(\mathbb{F},\alpha_1,\alpha_2,\gamma)$, podemos tomar p_0 de modo a minimizar p'. Como $p, p_0 \in \mathcal{O}_{\mathbb{F}}$, segue que

- se $d \equiv 2$ ou 3 $(mod\ 4)$, então $p = a+b\sqrt{d}$, com $a,b \in \mathbb{Z}$. Se $p_0 = r+s\sqrt{d}$, com

$$r = \begin{cases} \frac{a}{2}, & \text{se } a \text{ é par} \\ \frac{a-1}{2}, & \text{se } a \text{ é ímpar} \end{cases} \quad \text{e} \quad s = \begin{cases} \frac{b}{2}, & \text{se } b \text{ é par} \\ \frac{b-1}{2}, & \text{se } b \text{ é ímpar} \end{cases},$$

  então

  - a par, b par $\Rightarrow |p-2p_0| = |a+b\sqrt{d}-2(\frac{a}{2}+\frac{b}{2}\sqrt{d})| = 0$,
  - a par, b ímpar $\Rightarrow |p-2p_0| = |a+b\sqrt{d}-2(\frac{a}{2}+\frac{b-1}{2}\sqrt{d})| = |\sqrt{d}|$,
  - a ímpar, b par $\Rightarrow |p-2p_0| = |a+b\sqrt{d}-2(\frac{a-1}{2}+\frac{b}{2}\sqrt{d})| = 1$,
  - a ímpar, b ímpar $\Rightarrow |p-2p_0| = |a+b\sqrt{d}-2(\frac{a-1}{2}+\frac{b-1}{2}\sqrt{d})| = |1+\sqrt{d}|$.

  Logo, dado $p \in \mathcal{O}_{\mathbb{F}}$, existe $p_0 \in \mathcal{O}_{\mathbb{F}}$ tal que $|p-2p_0| \leq |1+\sqrt{d}| = \sqrt{1-d}$.

- se $d \equiv 1$ $(mod\ 4)$, então $p = a+b(\frac{1+\sqrt{d}}{2})$ com $a,b \in \mathbb{Z}$, tomemos $p_0 = r+s(\frac{1+\sqrt{d}}{2})$ da seguinte forma:

$$r = \begin{cases} \frac{a}{2}, & \text{se } a \text{ é par} \\ \frac{a+1}{2}, & \text{se } a \text{ é ímpar} \end{cases} \quad s = \begin{cases} \frac{b}{2}, & \text{se } b \text{ é par} \\ \frac{b-1}{2}, & \text{se } b \text{ é ímpar} \end{cases}.$$

Então

- a par, b par $\Rightarrow |p - 2p_0| = |a + b(\frac{1+\sqrt{d}}{2}) - 2(\frac{a}{2} + \frac{b}{2}(\frac{1+\sqrt{d}}{2}))| = 0$,
- a par, b ímpar $\Rightarrow |p - 2p_0| = |a + b(\frac{1+\sqrt{d}}{2}) - 2(\frac{a}{2} + \frac{b-1}{2}(\frac{1+\sqrt{d}}{2}))| = |(\frac{1+\sqrt{d}}{2})|$,
- a ímpar, b par $\Rightarrow |p - 2p_0| = |a + b(\frac{1+\sqrt{d}}{2}) - 2(\frac{a+1}{2} + \frac{b}{2}\sqrt{d})| = 1$,
- a ímpar, b ímpar $\Rightarrow |p - 2p_0| = |a + b(\frac{1+\sqrt{d}}{2}) - 2(\frac{a+1}{2} + \frac{b-1}{2}(\frac{1+\sqrt{d}}{2}))| = |-1 + (\frac{1+\sqrt{d}}{2})| = |\frac{-1+\sqrt{d}}{2}|$.

Logo, dado $p \in \mathcal{O}_{\mathbb{F}}$, existe $p_0 \in \mathcal{O}_{\mathbb{F}}$ tal que $|p - 2p_0| \leq |\frac{1+\sqrt{d}}{2}| = \sqrt{\frac{1-d}{4}}$.

Assim, para encontrar os melhores QSTBC's considerando o corpo base $\mathbb{Q}(\sqrt{d})$, com $d = -1, -2, -3, -7$ e -11, precisamos exibir convenientes α_1, α_2 e γ, em que γ não é norma algébrica de $\mathbb{Q}(\sqrt{d}, \alpha_1)$ sobre $\mathbb{Q}(\sqrt{d})$. Em cada corpo base, antes de encontrar quais são os códigos ótimos, mostramos que γ não é norma algébrica de $\mathbb{Q}(\sqrt{d}, \alpha_1)$ sobre $\mathbb{Q}(\sqrt{d})$, para que a Definição de QSTBC (5.3.2) seja satisfeita.

Recordemos do cálculo de uma variável complexa que o número complexo ζ_n é definido por $\zeta_n = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i\,\text{sen}\left(\frac{2\pi}{n}\right)$. Observe que $\sqrt{-1} = \zeta_4$ e $\frac{-1+\sqrt{-3}}{2} = \zeta_3$. Além disso, dizemos que ζ_n é uma raiz *n-ésima* primitiva da unidade se $\zeta_n^n = 1$ e $\zeta_n^m \neq 1$ para $1 < m < n$. Um *corpo ciclotômico* $\mathbb{F}$ é a menor extensão de $\mathbb{Q}$ contendo ζ_n, ou seja, $\mathbb{F} = \mathbb{Q}(\zeta_n)$, e seu anel de inteiro é $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\zeta_n]$.

Proposição 5.3.11. [24] O número complexo $1 + i$ não é uma norma algébrica de $\mathbb{Q}(\zeta_4, \frac{i+\sqrt{3}}{2})$ sobre $\mathbb{Q}(\zeta_4)$.

Demonstração. Seja $\alpha_1 = \frac{i+\sqrt{3}}{2}$ e suponhamos que existam $x = x_1 + x_2\alpha_1, y = y_1 + y_2\alpha_1 \in \mathbb{Z}[\zeta_4, \alpha_1]$ tal que

$$N_{\mathbb{Q}(\zeta_4,\alpha_1)/\mathbb{Q}(\zeta_4)}(x) = (1+i)N_{\mathbb{Q}(\zeta_4,\alpha_1)/\mathbb{Q}(\zeta_4)}(y). \tag{5.18}$$

Observemos que $\zeta_{12} = e^{2\pi i/12} = cos(\frac{\pi}{6}) + isen(\frac{\pi}{6}) = \frac{\sqrt{3}}{2} + i\frac{1}{2}$, ou seja, $\alpha_1 = \zeta_{12}$ e assim, $\mathbb{Q}(\zeta_4, \alpha_1) = \mathbb{Q}(\zeta_{12})$. Logo , x pode ser escrito como $x = x_1 + x_2\zeta_{12}$ e $N_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4)}(x) = \sigma_1(x)\sigma_2(x)$, onde $\sigma_1(\zeta_{12}) = \zeta_{12}$, $\sigma_2(\zeta_{12}) = \zeta_{12}^5$ e ambos fixam $\mathbb{Q}(\zeta_4)$. Portanto,

$$\begin{aligned} N_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4)}(x) &= \sigma_1(x)\sigma_2(x) = (x_1 + x_2\zeta_{12})(x_1 + x_2\zeta_{12}^5) \\ &= x_1^2 + x_1x_2(\zeta_{12} + \zeta_{12}^5) + x_2^2\zeta_{12}^6 = x_1^2 + x_1x_2i - x_2^2. \end{aligned} \tag{5.19}$$

Analogamente se $y \in \mathbb{Z}[\zeta_{12}]$, com $y = y_1 + y_2\zeta_{12}$ e $y_1, y_2 \in \mathbb{Z}[i]$ então

$$N_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}(\zeta_4)}(y) = y_1^2 - y_2^2 + iy_1y_2. \tag{5.20}$$

Pela Proposição 2.4.10, segue que existe um inteiro l_0 tal que

$$x_k = \sum_{l=1}^{l_0} p^{l-1}x_{k,l} \text{ e } y_k = \sum_{l=1}^{l_0} p^{l-1}y_{k,l}, \tag{5.21}$$

para $k = 1, 2$, onde $p = 1 + i$ e $x_{k,l}, y_{k,l} \in \{0, e^{\frac{2\pi ij}{4}}\}_{j=1,\ldots,4}$. Combinando as Equações (5.18), (5.19) e (5.20) com (5.21), segue que

$$\begin{aligned} x_{1,1}^2 - x_{2,1}^2 + ix_{1,1}x_{2,1} &= p(y_1^2 - y_2^2 + iy_1y_2) - p(p\overline{x}_{1,1}^2 - p\overline{x}_{2,1}^2 + ip\overline{x}_{1,1}\overline{x}_{2,1}) \\ &\quad -2p(x_{1,1}\overline{x}_{1,1} - x_{2,1}\overline{x}_{2,1}) - ip(x_{1,1}\overline{x}_{2,1} + x_{2,1}\overline{x}_{1,1}), \quad (5.22) \end{aligned}$$

onde $\overline{x}_{k,1} = \sum_{l=2}^{l_0} p^{l-2}x_{k,l} \in \mathbb{Z}[\zeta_4]$ para $k = 1, 2$. Como o termo da direita na igualdade (5.22) pertence a $p\mathbb{Z}[\zeta_4]$, temos que o termo da esquerda também pertence, isto é,

$$x_{1,1}^2 - x_{2,1}^2 + ix_{1,1}x_{2,1} \in \rho\mathbb{Z}[\zeta_4]. \quad (5.23)$$

A Equação (5.23), com $x_{1,1}, x_{2,1} \in \{0, e^{\frac{2\pi ij}{4}}\}_{j=1,\ldots,4}$ é válida somente quando $x_{1,1} = x_{2,1} = 0$. Neste caso, pela Equação (5.22), segue que

$$y_1^2 - y_2^2 + iy_1y_2 - p(\overline{x}_{1,1}^2 - \overline{x}_{2,1}^2 + i\overline{x}_{1,1}\overline{x}_{2,1}) = 0, \quad (5.24)$$

isto é,

$$\begin{aligned} y_{1,1}^2 - y_{2,1}^2 + iy_{1,1}y_{2,1} &= p(\overline{x}_{1,1}^2 - \overline{x}_{2,1}^2 + ix_{1,1}\overline{x}_{2,1}) - p(p(\overline{y}_{1,1}^2 - \overline{y}_{2,1}^2) + ip\overline{x}_{1,1}\overline{x}_{2,1}) \\ &\quad -2p(y_{1,1}\overline{y}_{1,1} - y_{2,1}\overline{y}_{2,1} + iy_{2,1}\overline{y}_{1,1}) \end{aligned}$$

onde $\overline{y}_{k,1} = \sum_{l=2}^{l_0} p^{l-2}y_{k,l} \in \mathbb{Z}[\zeta_4]$ com $k = 1, 2$. De modo análogo a prova de $x_{1,1}$ e $x_{2,1}$, da Equação (5.23) segue que $y_{1,1} = y_{2,1} = 0$. Continuando esse processo até $x_{1,l_0} = x_{2,l_0} = 0$ e $y_{1,l_0} = y_{2,l_0} = 0$, segue que $x = y = 0$, e isto completa a prova. □

Teorema 5.3.12. [24] O código $\mathcal{C}(\mathbb{Q}(\zeta_4), \frac{-i-\sqrt{3}}{2}, \frac{-i+\sqrt{3}}{2}, 1+i)$ é um QSTBC ótimo dentre todos os QSTBC sobre $\mathbb{Q}(\zeta_4)$ com determinante mínimo 1.

Demonstração. Pela Proposição 5.3.11 e pelo Lema 5.3.5, segue que $\mathcal{C}(\mathbb{Q}(\zeta_4), \frac{-i-\sqrt{3}}{2}, \frac{-i+\sqrt{3}}{2}, 1+i)$ é um QSTBC com determinante mínimo 1. Se M é uma matriz geradora de $\Lambda_{\mathcal{O}_{\mathbb{Q}(\zeta_4)}}$ então $g_{prod}(\mathcal{C}(\mathbb{Q}(\zeta_4), \frac{-i-\sqrt{3}}{2}, \frac{-i+\sqrt{3}}{2}, 1+i))$ é dado por

$$|i+1| \left| \frac{-i-\sqrt{3}}{2} - \frac{-i+\sqrt{3}}{2} \right|^2 |det(M)|^2 = 3\sqrt{2}.$$

Para mostrarmos que $\mathcal{C}(\mathbb{Q}(\zeta_4), \frac{-i-\sqrt{3}}{2}, \frac{-i+\sqrt{3}}{2}, 1+i)$ é um QSTBC ótimo temos que mostrar que qualquer $\mathcal{C} = \mathcal{C}(\mathbb{Q}(\zeta_4), \beta_1, \beta_2, \gamma)$ tem $g_{prod}(\mathcal{C}) \geq 3\sqrt{2}$. Pela Observação 3.1.9, o módulo do determinante da matriz geradora de $\Lambda_{\mathcal{O}_{\mathbb{Q}(\zeta_4)}}$ é sempre o mesmo e assim, este parâmetro será invariante no cálculo do $g_{prod}(C)$, e portanto podemos desconsiderá-lo em nossa análise. Portanto, devemos mostrar que $|\gamma||\beta_1 - \beta_2|^2 \geq \sqrt{3}^2\sqrt{|1+i|}^2$, ou seja, $|det(\overline{L})\gamma| \geq \sqrt{3}\sqrt{|1+i|}$, onde

$$\overline{L} = \begin{pmatrix} 1 & 1 \\ \beta_1 & \beta_2 \end{pmatrix}.$$

Consideremos o polinômio irredutível $x^2 + px + q$ sobre $\mathbb{F}$ com $p, q \in \mathbb{Z}[\zeta_4]$. Pelo Teorema 5.3.9 podemos assumir, sem perda de generalidade, que $|p| \leq \sqrt{2}$, isto é, $p \in \{0, \pm 1, \pm i, \pm 1 \pm i\}$. Suponhamos que existe um QSTBC baseado em $x^2 + px + q$ tal que

$$|det(\overline{L})\gamma| < \sqrt{3}\sqrt{|1+i|}. \tag{5.25}$$

Como $det(\overline{G}) = \beta_2 - \beta_1$, segue que

$$|\beta_1 - \beta_2|^2|\gamma| = |p^2 - 4q||\gamma| < 3|1+i| = 3\sqrt{2}.$$

Analisamos os seguintes casos:

1º caso: $|p^2-4q| < 3$. Como $p \in \{0, \pm 1, \pm i, \pm 1 \pm i\}$, segue que $p^2 \in \{0, 1, -1, \pm 2i\}$. Se $q = a + bi$, com $a, b \in \mathbb{Z}$, então temos os seguinte casos:

- $p^2 = 0 \Rightarrow 3 > |p^2 - 4q| = |0 - 4a - 4bi| = \sqrt{(4a)^2 + (4b)^2} \Rightarrow a = 0, b = 0 \Rightarrow x^2 + px + q = x^2$ que é redutível sobre $\mathbb{Q}(i)$.
- $p^2 = 1 \Rightarrow 3 > |p^2 - 4q| = |1 - 4a - 4bi| = \sqrt{(1-4a)^2 + (4b)^2} \Rightarrow a = 0, b = 0 \Rightarrow x^2 + px + q = x^2 \pm x$ que é redutível sobre $\mathbb{Q}(i)$.
- $p^2 = -1 \Rightarrow 3 > |p^2 - 4q| = |-1 - 4a - abi| = \sqrt{(-1-4a)^2 + (4b)^2} \Rightarrow a = 0, b = 0 \Rightarrow x^2 + px + q = x^2 \pm xi$ que é redutível sobre $\mathbb{Q}(i)$.
- $p^2 = 2i \Rightarrow 3 > |p^2 - 4q| = |2i - 4a - abi| = \sqrt{(4a)^2 + (2-4b)^2} \Rightarrow$
$$\Rightarrow \begin{cases} a = 0, b = 0 \Rightarrow x^2 + px + q = x^2 \pm (1+i)x \text{ que é redutível sobre } \mathbb{Q}(i). \\ a = 0, b = 1 \Rightarrow x^2 + px + q = x^2 \pm (1+i)x + i \text{ que tem como raiz } \mp 1 \\ \text{ e portanto é redutível sobre } \mathbb{Q}(i). \end{cases}$$
- $p^2 = -2i \Rightarrow 3 > |p^2 - 4q| = |-2i - 4a - abi| = \sqrt{(4a)^2 + (-2-4b)^2} \Rightarrow$
$$\Rightarrow \begin{cases} a = 0, b = 0 \Rightarrow x^2 + px + q = x^2 \pm (1-i)x \text{ que é redutível sobre } \mathbb{Q}(i). \\ a = 0, b = -1 \Rightarrow x^2 + px + q = x^2 \pm (1-i)x + i \text{ que tem como raiz } \mp 1 \\ \text{ e portanto é redutível sobre } \mathbb{Q}(i). \end{cases}$$

Logo, se $|p^2 - 4q| < 3$, então $x^2 + px + q$ é redutível sobre $\mathbb{Q}(i)$.

2º caso: $|p^2 - 4a| \geq 3$. Como $p^2 - 4q, \gamma \in \mathbb{Z}[\zeta_4]$ segue que para $|p^2 - 4q||\gamma| < 3\sqrt{2}$ só restam as seguintes possibilidades:

$$(|p^2 - 4q|, |\gamma|) \in \{(3,1), (4,1)\}.$$

Analisamos ambos os casos:

- $|p^2 - 4q| = 3$ e $|\gamma| = 1$. Como $|\gamma| = 1$ e $\gamma \in \mathbb{Z}[\zeta_4]$, segue que $\gamma \in \{\pm 1, \pm i\}$. Além disso, de acordo com as possibilidades para p, se $p = \pm 1 \pm i$ então $p^2 = \pm 2i$. Logo, $3\sqrt{2} > |p^2 - 4q| = |\pm 2i - 4a - 4b| \Rightarrow a = 0$ e $b = 1$. Portanto, $x^2 + px + q = x^2 \pm (1 \pm i)x + i$ que é redutível sobre $\mathbb{Q}(i)$. Se $p = 0$, então $3\sqrt{2} > |4q| \Rightarrow q = 0$. Assim, $x^2 + px + q = x^2$ que é redutível sobre $\mathbb{Q}(i)$. Logo, sobraram os casos

  $$(p, q) \in \{(\pm 1, 1), (\pm i, -1)\},$$

  e portanto,

  $$(p, \sqrt{p^2 - 4q}) \in \{(\pm 1, \sqrt{3}i), (\pm i, \sqrt{3})\}.$$

Assim, $\mathbb{Q}(\zeta_4,\beta_1) = \mathbb{Q}\left(\zeta_4, \frac{-p\pm\sqrt{p^2-4q}}{2}\right) = \mathbb{Q}\left(\zeta_4, \frac{1\pm\sqrt{3}i}{2}\right)$, ou $\mathbb{Q}(\zeta_4,\beta_1) = \mathbb{Q}\left(\zeta_4, \frac{i\pm\sqrt{3}}{2}\right)$. Porém, em ambos os casos, observe que γ é norma algébrica:

	$N_{\mathbb{Q}(\zeta_4,\frac{1\pm\sqrt{3}i}{2})/\mathbb{Q}(\zeta_4)}(x)=\gamma$	$N_{\mathbb{Q}(\zeta_4,\frac{i\pm\sqrt{3}}{2})/\mathbb{Q}(\zeta_4)}(x)=\gamma$
$\gamma^2=1$	$x=1$	$x=1$
$\gamma^2=-1$	$x=i$	$x=i$
$\gamma^2=i$	$x=i+\frac{1+\sqrt{3}i}{2}$	$x=i+\frac{i+\sqrt{3}}{2}$
$\gamma^2=-i$	$x=i(i+\frac{1+\sqrt{3}i}{2})$	$x=i(i+\frac{i+\sqrt{3}}{2})$

O que é um absurdo, pois pela Definição (5.3.2), γ não pode ser norma algébrica.

- $|p^2-4q|=4$ e $|\gamma|=1$. Neste caso, como $|p|<2$, segue que $p=0$ e $q\in\{\pm1,\pm i\}$. Se $q=\pm1$, então $x^2+px+q=x^2\pm1$ que é redutível sobre $\mathbb{Q}(i)$. Se $q=\pm i$, então $x^2+px+q=x^2\pm i$ que tem como raiz $\beta_1=\sqrt{\pm i}$. Logo, $\mathbb{Q}(\zeta_4,\beta_1)=\mathbb{Q}(\zeta_4,\sqrt{\pm i})$. Assim, $N_{\mathbb{Q}(\zeta_4,\beta_1)/\mathbb{Q}(\zeta_4)}(\sqrt{-i})=i$ e $N_{\mathbb{Q}(\zeta_4,\beta_1)/\mathbb{Q}(\zeta_4)}(\sqrt{i})=-i$. Portanto, para todo $\forall\gamma\in\{\pm1,\pm i\}$, γ é norma algébrica. O que é um absurdo, pois como mencionado, γ não pode ser norma algébrica.

Desse modo, concluímos que não existem valores para $p,q,\gamma\in\mathbb{Z}[\zeta_4]$ que satisfaçam a Equação (5.25) e isto completa a prova. □

Exemplo 5.3.13. O código de ouro definido como $\mathcal{C}=\mathcal{C}(\mathbb{Q}(\zeta_4),\frac{1+\sqrt{5}}{2},\frac{1-\sqrt{5}}{2},i)$ possui $g_{prod}(\mathcal{C})=5$, que é maior que $g_{prod}(\mathcal{C}(\mathbb{Q}(\zeta_4),\frac{-i-\sqrt{3}}{2},\frac{-i+\sqrt{3}}{2},1+i))=3\sqrt{2}\approx 4,24$. Portanto, sob este critério, este QSTBC possui melhor desempenho em relação ao código de ouro.

Proposição 5.3.14. [24] O número complexo ζ_6 não é norma algébrica de $\mathbb{Q}(\zeta_3,\alpha_1)$ sobre $\mathbb{Q}(\zeta_3)$, onde $\alpha_1=\frac{-p\pm\sqrt{p^2-4q}}{2}$, com $p=-1-\zeta_6$ e $q=\sqrt{3}i$.

Demonstração. Suponhamos que exista $x=x_1+x_2\alpha_1$ e $y=y_1+y_2\alpha_1$, com $x_1,x_2,y_1,y_2\in\mathbb{Z}[\zeta_3]$, tal que

$$N_{\mathbb{Q}(\zeta_3,\alpha_1)/\mathbb{Q}(\zeta_3)}(x)=\zeta_6 N_{\mathbb{Q}(\zeta_3,\alpha_1)/\mathbb{Q}(\zeta_3)}(y). \tag{5.26}$$

Assim,

$$N_{\mathbb{Q}(\zeta_3,\alpha_1)/\mathbb{Q}(\zeta_3)}(x)=(x_1+x_2\alpha_1)(x_1+x_2\alpha_2)=x_1^2-px_1x_2+qx_2^2=x_1^2+(1+\zeta_6)x_1x_2+\sqrt{3}ix_2^2 \tag{5.27}$$

e

$$N_{\mathbb{Q}(\zeta_3,\alpha_1)/\mathbb{Q}(\zeta_3)}(y)=(y_1+y_2\alpha_1)(y_1+y_2\alpha_2)=x_1^2-py_1x_2+qy_2^2=y_1^2+(1+\zeta_6)y_1y_2+\sqrt{3}iy_2^2. \tag{5.28}$$

Substituindo as Equações (5.27) e (5.28) em (5.26), segue que

$$x_1^2+(1+\zeta_6)x_1x_2-\zeta_6(y_1^2+(1+\zeta_6)y_1y_2)=\sqrt{3}i(\zeta_6y_2^2-x_2^2). \tag{5.29}$$

Pela Proposição 2.4.12, segue que existe $l_0\in\mathbb{N}$ tal que os elementos $x_k,y_k\in\mathbb{Z}[\zeta_6]$ podem ser escritos como

$$x_k=\sum_{l=1}^{l_0}(\sqrt{3}i)^{l-1}x_{k,l} \text{ e } y_k=\sum_{l=1}^{l_0}(\sqrt{3}i)^{l-1}y_{k,l}, \tag{5.30}$$

com $x_{k,l}, y_{k,l} \in S = \{0, e^{\frac{2\pi im}{6}}\}_{m=1,\ldots,6}$. Combinando as Equações (5.29) e (5.30), segue que

$$\begin{aligned} x_{1,1}^2 + (1+\zeta_6)x_{1,1}x_{2,1} - \zeta_6(y_{1,1}^2 + (1+\zeta_6)y_{1,1}y_{2,1}) &= \sqrt{3}i(\zeta_6 y_2^2 - x_2^2) \\ -\sqrt{3}i(2x_{1,1}\overline{x}_{1,1} + (1+\zeta_6)(\overline{x}_{1,1}\overline{x}_{2,1} + x_{1,1}\overline{x}_{2,1}) + \sqrt{3}i\overline{x}_{1,1}^2) \\ +\sqrt{3}i\zeta_6(2y_{1,1}\overline{y}_{1,1} + (1+\zeta_6)(\overline{y}_{1,1}y_2 + y_{1,1}\overline{y}_{2,1}) + \sqrt{3}i\overline{y}_{1,1}^2), \end{aligned} \tag{5.31}$$

onde $\overline{x}_{k,1} = \sum_{l=2}^{l_0}(\sqrt{3}i)^{l-2}x_{k,l}$ e $\overline{y}_{k,1} = \sum_{l=2}^{l_0}(\sqrt{3}i)^{l-2}y_{k,l}$. Como o termo da direita na Equação (5.31) pertence a $\sqrt{3}i\mathbb{Z}[\zeta_6]$, segue que o termo da esquerda também pertence, isto é,

$$x_{1,1}^2 + (1+\zeta_6)x_{1,1}x_{2,1} - \zeta_6(y_{1,1}^2 + (1+\zeta_6)y_{1,1}y_{2,1}) \in \sqrt{3}i\mathbb{Z}[\zeta_6]. \tag{5.32}$$

A Equação (5.32) somente é valida quando $x_{1,1} = y_{1,1} = 0$. Assim, a Equação (5.31) fica

$$\begin{aligned} x_{2,1}^2 + (1+\zeta_6)x_{2,1}x_{1,2} - \zeta_6(y_{2,1}^2 + (1+\zeta_6)y_{1,2}y_{2,1}) &= \sqrt{3}i(\zeta_6\overline{y}_{1,1}^2 - \overline{x}_{1,1}^2) \\ -\sqrt{3}i(2x_{2,1}\overline{x}_{2,1} + (1+\zeta_6)(\overline{x}_{2,1}\overline{x}_{1,1} + x_{2,1}\overline{x}_{1,2}) + \sqrt{3}i\overline{x}_{2,1}^2) \\ +\sqrt{3}i(2y_{2,1}\overline{y}_{2,1} + (1+\zeta_6)(\overline{y}_{2,1}\overline{y}_{1,1} + y_{2,1}\overline{y}_{1,2}) + \sqrt{3}i\overline{y}_{2,1}^2), \end{aligned} \tag{5.33}$$

isto é,

$$x_{2,1}^2 + (1+\zeta_6)x_{2,1}x_{1,2} - \zeta_6(y_{2,1}^2 + (1+\zeta_6)y_{2,1}y_{1,2}) \in \mathbb{Z}[\zeta_6],$$

onde $\overline{x}_{k,2} = \sum_{l=2}^{l_0}(\sqrt{3}i)^{l-3}x_{k,l}$ e $\overline{y}_{k,2} = \sum_{l=2}^{l_0}(\sqrt{3}i)^{l-3}y_{k,l}$. Analogamente, concluímos que $x_{2,1} = y_{2,1} = 0$. Continuando o processo, segue que $x = y = 0$. □

Teorema 5.3.15. [24] O código $\mathcal{C}(\mathbb{Q}(\zeta_3), \frac{-p+\sqrt{p^2-4q}}{2}, \frac{-p-\sqrt{p^2-4q}}{2}, \zeta_6)$ é um QSTBC ótimo dentre todos os QSTBC sobre $\mathbb{Q}(\zeta_3)$ com determinante mínimo 1, onde $p = -1-\zeta_6$ e $q = \sqrt{3}i$.

Demonstração. Pela Proposição 5.3.14 e pelo Lema 5.3.5, segue que $\mathcal{C}(\mathbb{Q}(\zeta_3), \frac{-p+\sqrt{p^2-4q}}{2}, \frac{-p-\sqrt{p^2-4q}}{2}, \zeta_6)$, onde $p = -1-\zeta_6$ e $q = \sqrt{3}i$, é um QSTBC com determinante mínimo 1. Se M é uma matriz geradora de $\Lambda_{\mathcal{O}_{\mathbb{Q}(\zeta_3)}}$ então $g_{prod}(\mathcal{C}(\mathbb{Q}(\zeta_3), \frac{-p+\sqrt{p^2-4q}}{2}, \frac{-p-\sqrt{p^2-4q}}{2}, \zeta_6)) =$

$$|\zeta_6| \left| \frac{-p+\sqrt{p^2-4q}}{2} - \frac{-p-\sqrt{p^2-4q}}{2} \right|^2 |det(M)|^2 = \frac{3}{4}\sqrt{21}.$$

Assim, como no Teorema 5.3.12, para mostrarmos que $\mathcal{C}(\mathbb{Q}(\zeta_3), \frac{-p+\sqrt{p^2-4q}}{2}, \frac{-p-\sqrt{p^2-4q}}{2}, \zeta_6)$ é um QSTBC ótimo, devemos mostrar que qualquer $\mathcal{C} = \mathcal{C}(\mathbb{Q}(\zeta_4), \beta_1, \beta_2, \gamma)$ possui $g_{prod}(\mathcal{C}) \geq \frac{3}{4}\sqrt{21}$. Pela Observação 3.1.9, o módulo do determinante da matriz geradora de $\Lambda_{\mathcal{O}_{\mathbb{Q}(\zeta_3)}}$ é sempre o mesmo e assim, este parâmetro será invariante no cálculo do $g_{prod}(C)$, e portanto podemos desconsiderá-lo em nossa análise. Portanto, devemos mostrar que $|\gamma||\beta_1 - \beta_2|^2 \geq \sqrt{21}$. Para isso, vamos provar que para todo $x^2 + px + q \in \mathbb{Z}[\zeta_3][x]$, com $|p| \leq 1$ tal que

$$|p^2 - 4q| < |(1+\zeta_6)^2 - 4\sqrt{3}i| = \sqrt{21},$$

é redutível sobre $\mathbb{Q}(\zeta_3)$. Como $|p| = |a + b\frac{1+\sqrt{-3}}{2}| \leq 1$, segue que

$$(a,b) \in \{(1,-1),(-1,1),(\pm 1,0),(0,\pm 1),(0,0)\}.$$

Suponhamos que exista $q = \alpha + \beta\frac{1+\sqrt{-3}}{2}$ tal que $|p^2 - 4q| < \sqrt{21}$. De modo análogo a demonstração do Teorema 5.3.12, concluímos que em todos os casos o polinômio $x^2 + px + q$ é redutível sobre $\mathbb{Q}(\zeta_3)$, e isto completa a prova. □

5.4 Novas contribuições de códigos espaço-temporais

Após termos apresentado e reformulado resultados contidos em [24], a partir de agora, apresentamos as contribuições originais de nosso trabalho, além dos Corolários 4.2.4 e 4.2.5 e das demonstrações das Proposições já existentes 2.4.10, 2.4.12 e 3.3.2.

Proposição 5.4.1. O número inteiro -1 não é norma algébrica da extensão $\mathbb{Q}(\sqrt{-2},\sqrt{-3})$ sobre $\mathbb{Q}(\sqrt{-2})$.

Demonstração. Como $-2 \in \mathbb{Z}$ e $-2 \equiv 1\,(mod\,3)$, o resultado segue do Corolário 4.2.4. □

Teorema 5.4.2. O código $\mathcal{C}(\mathbb{Q}(\sqrt{-2}),\frac{1+\sqrt{-3}}{2},\frac{1-\sqrt{-3}}{2},-1)$ é um QSTBC ótimo dentre todos os QSTBC sobre $\mathbb{Q}(\sqrt{-2})$ com determinante mínimo 1.

Demonstração. Pela Proposição 5.4.1 e do Lema 5.3.5, segue que $\mathcal{C}(\mathbb{Q}(\sqrt{-2}),\frac{1+\sqrt{-3}}{2},\frac{1-\sqrt{-3}}{2},-1)$ é um QSTBC com determinante mínimo 1. Se M uma matriz geradora de $\Lambda_{\mathcal{O}_{\mathbb{Q}(\sqrt{-2})}}$, então $g_{prod}(\mathcal{C}(\mathbb{Q}(\sqrt{-2}),\frac{1+\sqrt{-3}}{2},\frac{1-\sqrt{-3}}{2},-1))$ é dado por

$$|-1|\left|\frac{1+\sqrt{-3}}{2} - \frac{1-\sqrt{-3}}{2}\right|^2 |det(M)|^2 = 6.$$

Assim, como no Teorema 5.3.12, para mostrarmos que $\mathcal{C}(\mathbb{Q}(\sqrt{-2}),\frac{1+\sqrt{-3}}{2},\frac{1-\sqrt{-3}}{2},-1)$ é um QSTBC ótimo devemos mostrar que todo $\mathcal{C} = \mathcal{C}(\mathbb{Q}(\sqrt{-2}),\beta_1,\beta_2,\gamma)$ possui $g_{prod}(\mathcal{C}) \geq 6$. Pela Observação 3.1.9, o módulo do determinante da matriz geradora de $\Lambda_{\mathcal{O}_{\mathbb{Q}(\sqrt{-2})}}$ é sempre o mesmo e assim, este parâmetro será invariante no cálculo do $g_{prod}(C)$, e portanto podemos desconsiderá-lo em nossa análise. Portanto, devemos mostrar que $|\gamma||\beta_1 - \beta_2|^2 \geq 3$. Para isso, vamos provar que qualquer $x^2 + px + q \in \mathbb{Z}[\sqrt{-2}][x]$, com $|p| \leq \sqrt{3}$ tal que

$$|p^2 - 4q| < |\sqrt{-3}| = 3,$$

é redutível sobre $\mathbb{Q}(\sqrt{-2})$. Como $|p| = |a + b\sqrt{-2}| \leq \sqrt{3}$, segue que

$$(a,b) \in \{(0,0),(0,\pm 1),(\pm 1,0)\}.$$

Suponhamos que exista $q = \alpha + \beta\sqrt{-2}$ tal que $|p^2 - 4q| < 3$. De modo análogo a demonstração feita no Teorema 5.3.12, concluímos que em alguns os casos o polinômio $x^2 + px + q$ é redutível sobre $\mathbb{Q}(\sqrt{-2})$, exceto quando $(a,b) \in \{(0,\pm 1)\}$ e $q = -1$. No caso $(a,b) = (0,1)$ o polinômio x^2+px+q não é redutível sobre $\mathbb{Q}(\sqrt{-2})$ quando $q = -1$, e portanto, $x^2+px+q = x^2+\sqrt{-2}x-1$. Para $g_{prod}(\mathcal{C}(\mathbb{Q}(\sqrt{-2}),\frac{-\sqrt{-2}+\sqrt{2}}{2},\frac{-\sqrt{-2}-\sqrt{2}}{2},\gamma))$ ser menor que 6, devemos ter que $|\gamma| < 3/2$, ou seja, $\gamma \in \{0,\pm 1,\pm\sqrt{-2}\}$. Porém, sejam $\mathbb{K} = \mathbb{Q}(\sqrt{-2},\sqrt{-3})$ e $\mathbb{F} = \mathbb{Q}(\sqrt{-2})$, então

$$N_{\mathbb{K}/\mathbb{F}}(0)=0, \quad N_{\mathbb{K}/\mathbb{F}}(1)=1, \quad N_{\mathbb{K}/\mathbb{F}}\left(-\left(\tfrac{-\sqrt{-2}+\sqrt{2}}{2}\right)-\sqrt{-2}-1\right)=\sqrt{-2},$$
$$N_{\mathbb{K}/\mathbb{F}}\left(\tfrac{-\sqrt{-2}+\sqrt{2}}{2}\right)=-1 \qquad N_{\mathbb{K}/\mathbb{F}}\left(\left(\tfrac{-\sqrt{-2}+\sqrt{2}}{2}\right)\left(\sqrt{-2}+1\right)-1\right)=-\sqrt{-2}.$$

Portanto, não existe um QSTBC $\mathcal{C}$ sobre $\mathbb{F}=\mathbb{Q}(\sqrt{-2})$ tal que $g_{prod}(\mathcal{C})<6$. De modo análogo, segue para $(a,b)=(0,-1)$ e $q=-1$, o que conclui a demonstração. □

Proposição 5.4.3. O número inteiro -1 não é norma algébrica da extensão $\mathbb{Q}(\sqrt{-7},i)$ sobre $\mathbb{Q}(\sqrt{-7})$.

Demonstração. Como $-7\in\mathbb{Z}$ e $-7\equiv 1\,(mod\ 8)$, o resultado segue do Corolário 4.2.5. □

Teorema 5.4.4. O código $\mathcal{C}(\mathbb{Q}(\sqrt{-7}),i,-i,-1)$ é um QSTBC ótimo dentre todos os QSTBC sobre $\mathbb{Q}(\sqrt{-7})$ com determinante mínimo 1.

Demonstração. Pela Proposição 5.4.3, segue que -1 não é norma algébrica da extensão $\mathbb{Q}(\sqrt{-7},i)$ sobre $\mathbb{Q}(\sqrt{-7})$ e do Lema 5.3.5 segue que $\mathcal{C}(\mathbb{Q}(\sqrt{-7}),i,-i,-1)$ é um QSTBC com determinante mínimo 1. Se M uma matriz geradora de $\Lambda_{\mathcal{O}_{\mathbb{Q}(\sqrt{-7})}}$ então $g_{prod}(\mathcal{C}(\mathbb{Q}(\sqrt{-7}),i,-i,-1))$ é dado por

$$|-1||i-(-i)|^2|det(M)|^2=7.$$

Assim, como no Teorema 5.3.12, para mostrarmos que $\mathcal{C}(\mathbb{Q}(\sqrt{-7}),i,-i,-1)$ é um QSTBC ótimo, devemos mostrar que qualquer $\mathcal{C}=\mathcal{C}(\mathbb{Q}(\sqrt{-7}),\beta_1,\beta_2,\gamma)$ possui $g_{prod}(\mathcal{C})\geq 7$. Pela Observação 3.1.9, o módulo do determinante da matriz geradora de $\Lambda_{\mathcal{O}_{\mathbb{Q}(\sqrt{-7})}}$ é sempre o mesmo e assim, este parâmetro será invariante no cálculo do $g_{prod}(C)$, e portanto podemos desconsiderá-lo em nossa análise. Portanto, devemos mostrar que $|\gamma||\beta_1-\beta_2|^2\geq 4$. Para isso, vamos provar que para todo $x^2+px+q\in\mathbb{Z}[\frac{1-\sqrt{-7}}{2}][x]$, com $|p|\leq\sqrt{2}$ tal que

$$|p^2-4q|<|2i|^2=4,$$

é redutível sobre $\mathbb{Q}(\sqrt{-7})$. Como $|p|=|a+b(\frac{1+\sqrt{-7}}{2})|\leq\sqrt{2}$, segue que

$$(a,b)\in\{(0,0),(\pm1,0)\}.$$

Suponhamos que exista $q=\alpha+\beta(\frac{1+\sqrt{-7}}{2})$ tal que $|p^2-4q|<4$. Se $p=0$ então $q=0$. Logo, $x^2+px+q=x^2$ que é redutível sobre $\mathbb{Q}(\sqrt{-7})$. Se $p=\pm1$, então $p^2=1$, o que implica que $q=0$ ou 1. Se $q=0$, então $x^2+px+q=x^2+px$ que é redutível sobre $\mathbb{Q}(\sqrt{-7})$, e se $q=1$, então

$$p=1,q=1\Rightarrow x^2+px+q \text{ tem como raiz } r_0=\frac{-1\pm\sqrt{-3}}{2},$$
$$p=-1,q=1\Rightarrow x^2+px+q \text{ tem como raiz } r_1=\frac{1\pm\sqrt{-3}}{2}.$$

Assim, $\mathbb{Q}(\sqrt{-7},r_0)=\mathbb{Q}(\sqrt{-7},r_1)$. Assim, em ambos os casos, para que $g_{prod}(\mathcal{C}(\mathbb{Q}(\sqrt{-7}),r_j,\overline{r_j},\gamma))$ com $j=0,1$, seja menor que $7=g_{prod}(X(\mathbb{Q}(\sqrt{-7}),i,-i,i))$, o valor absoluto de γ tem que ser menor que $\frac{4}{3}$, isto é, $|\gamma|<\frac{4}{3}$. Se $|\gamma|<\frac{4}{3}$ então $\gamma=\pm1$. Como $N_{\mathbb{Q}(\sqrt{-7},i)/\mathbb{Q}(\sqrt{-7})}(1)=1$ e $N_{\mathbb{Q}(\sqrt{-7},i)/\mathbb{Q}(\sqrt{-7})}((\frac{1+\sqrt{-7}}{2}-1)(\frac{1+\sqrt{-3}}{2})-\frac{1+\sqrt{-7}}{2})=-1$, segue que não existe um QSTBC $\mathcal{C}$ sobre $\mathbb{Q}(\sqrt{-7})$ com $g_{prod}(\mathcal{C})<7$. □

Proposição 5.4.5. O número inteiro -1 não é norma algébrica da extensão $\mathbb{Q}(\sqrt{-11},\sqrt{-3})$ sobre $\mathbb{Q}(\sqrt{-11})$.

Demonstração. Como $-11 \in \mathbb{Z}$ e $-11 \equiv 1\,(mod\ 3)$, o resultado segue do Corolário 4.2.4. □

Teorema 5.4.6. O código $\mathcal{C}(\mathbb{Q}(\sqrt{-11}), \frac{1+\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}, -1)$ é um QSTBC ótimo dentre os QSTBC sobre $\mathbb{Q}(\sqrt{-11})$ com determinante mínimo 1.

Demonstração. Pela Proposição 5.4.5, segue que -1 não é norma algébrica da extensão $\mathbb{Q}(\sqrt{-11}, \frac{1+\sqrt{-3}}{2})$ sobre $\mathbb{Q}(\sqrt{-11})$ e do Lema 5.3.5, segue que $\mathcal{C}(\mathbb{Q}(\sqrt{-11}), \frac{1+\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}, -1)$ é um QSTBC com determinante mínimo 1. Se M é uma matriz geradora de $\Lambda_{\mathcal{O}_{\mathbb{Q}(\sqrt{-11})}}$, então $g_{prod}\mathcal{C}(\mathbb{Q}(\sqrt{-11}), \frac{1+\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}, -1))$ é dado por

$$|-1|\left|\frac{1+\sqrt{-3}}{2} - \frac{1-\sqrt{-3}}{2}\right|^2 |det(M)|^2 = \frac{33}{4}.$$

Assim, como no Teorema 5.3.12, para mostrarmos que $\mathcal{C}(\mathbb{Q}(\sqrt{-11}), \frac{1+\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}, -1)$ é um QSTBC ótimo, devemos mostrar que todo $\mathcal{C} = \mathcal{C}(\mathbb{Q}(\sqrt{-11}), \beta_1, \beta_2, \gamma)$ possui $g_{prod}(\mathcal{C}) \geq \frac{33}{4}$. Pela Observação 3.1.9, o módulo do determinante da matriz geradora de $\Lambda_{\mathcal{O}_{\mathbb{Q}(\sqrt{-11})}}$ é sempre o mesmo e assim, este parâmetro será invariante no cálculo do $g_{prod}(C)$, e portanto podemos desconsiderá-lo em nossa análise. Portanto, devemos mostrar que $|\gamma||\beta_1 - \beta_2|^2 \geq 3$. Para isso, vamos provar que todo $x^2 + px + q \in \mathbb{Z}[\frac{1-\sqrt{-11}}{2}][x]$, com $|p| \leq \sqrt{3}$ tal que

$$|p^2 - 4q| < |\sqrt{-3}|^2 = 3,$$

é redutível sobre $\mathbb{Q}(\sqrt{-11})$. Como $|p| = |a + b(\frac{1-\sqrt{-11}}{2})| \leq \sqrt{3}$, segue que

$$(a, b) \in \{(0, 0), (\pm 1, 0)\}.$$

Suponhamos que exista $q = \alpha + \beta\frac{1-\sqrt{-11}}{2}$ tal que $|p^2 - 4q| < 3$. De modo análogo ao Teorema 5.3.12, concluímos que em todos os casos o polinômio $x^2 + px + q$ é redutível sobre $\mathbb{Q}(\sqrt{-11})$, e isto completa a prova. □

Observação 5.4.7. Seja $\mathbb{F}$ é uma extensão quadrática imaginária de $\mathbb{Q}$, isto é, $\mathbb{F} = \mathbb{Q}(\sqrt{d})$, com $d < 0$ inteiro livre de quadrados. O polinômio minimal de $\mathbb{Q}(\sqrt{d})$ é da forma

$$\begin{array}{ll} x^2 - d, & \text{se } d \equiv 2\ (mod\ 4)\ \text{ ou }\ d \equiv 3\ (mod\ 4) \\ x^2 - x + \frac{1-d}{4}, & \text{se } d \equiv 1\ (mod\ 4) \end{array}$$

Seja M_d a matriz geradora de $\Lambda_{\mathbb{F}}$. Analisando $|det(M_d)|$, temos os seguintes casos, onde assumimos que $d < 0$ e σ_1, σ_2 os são os dois mergulhos de $\mathbb{Q}(\sqrt{d})$ em $\mathbb{C}$ que fixam $\mathbb{Q}$, onde $\sigma_1 = id$:

- se $d \equiv 1\ (mod\ 4)$, então $|det(M_d)|^2 = \left|\begin{array}{cc} Re(\sigma_1(1)) & Im(\sigma_1(1)) \\ Re\left(\sigma_1\left(\frac{1+\sqrt{d}}{2}\right)\right) & Im\left(\sigma_1\left(\frac{1+\sqrt{d}}{2}\right)\right) \end{array}\right|^2 =$

$$\left|\begin{array}{cc} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{d}}{2} \end{array}\right|^2 = \left|\frac{\sqrt{d}}{2}\right|^2 = \left|\frac{d}{4}\right|.$$

- se $d \equiv 2 \ (mod\ 4)$ ou $d \equiv 3 \ (mod\ 4)$, então $|det(M_d)|^2 = \begin{vmatrix} Re(\sigma_1(1)) & Im(\sigma_1(1)) \\ Re(\sigma_1(\sqrt{d})) & Im(\sigma_1(\sqrt{d})) \end{vmatrix}^2 = \begin{vmatrix} 1 & 0 \\ 0 & \sqrt{d} \end{vmatrix}^2 = \left|\sqrt{d}\right|^2 = |d|$.

Pelo Lema 5.3.5, segue que se $\mathbb{F}/\mathbb{Q}$ é uma extensão quadrática imaginária, então $d_{min}(X(\mathbb{F}, \alpha_1, \alpha_2, \gamma)) = 1$. Assim, queremos encontrar o melhor QSTBC dentre todos os corpos quadráticos imaginários.

Teorema 5.4.8. O código $\mathcal{C}(\mathbb{Q}(\zeta_3), \frac{-p+\sqrt{p^2-4q}}{2}, \frac{-p-\sqrt{p^2-4q}}{2}, \zeta_6)$ é um QSTBC ótimo dentre os QSTBC sobre $\mathbb{Q}(\sqrt{d})$, com $d < 0$ um inteiro livre de quadrados, onde $p = -1-\zeta_6$ e $q = \sqrt{3}i$.

Demonstração. Suponhamos que exista um QSTBC $\mathcal{C}(\mathbb{Q}(\sqrt{d}), \alpha_1, \alpha_2, \gamma)$, com $d < 0$ inteiro livre de quadrados, tal que

$$|det(M)|^2|\alpha_1 - \alpha_2|^2|\gamma| = g_{prod}(\mathcal{C}(\mathbb{Q}(\sqrt{d}), \alpha_1, \alpha_2, \gamma)) < g_{prod}(\mathcal{C}(\mathbb{Q}(\zeta_3), \frac{-p+\sqrt{p^2-4q}}{2}, \frac{-p-\sqrt{p^2-4q}}{2}, \zeta_{12})) \approx 3,44,$$

onde M é uma matriz geradora de $\Lambda_{\mathcal{O}_{\mathbb{F}}}$. Assim,

$$|det(M)|^2|\alpha_1 - \alpha_2|^2|\gamma| < 3,44.$$

Analisamos $|det(M)|^2$:

- se $d < 0, d \equiv 1 \ (mod\ 4)$, então $|det(M)|^2 = \frac{|d|}{4}$ e $d \in \{-3, -7, -11, -15, \ldots\}$. Logo $d \in \{-3, -7, -11\}$ são os únicos d que satisfazem $|det(M)|^2 < 3,44$.
- se $d < 0, d \equiv 2 \ (mod\ 4)$ ou $d \equiv 3 \ (mod\ 4)$ então $|det(M)|^2 = |d|$ e $d \in \{-1, -2, -5, -6, \cdots\}$. Logo, $d \in \{-1, -2\}$ são os únicos d que satisfazem $|det(M)|^2 < 3,44$.

Assim, precisamos analisar os casos onde $d \in \{-1, -2, -3, -7, -11\}$. Mas, para estes casos já conhecemos os melhores códigos. Denotando por $g_{\text{ótimo } \mathbb{Q}(\sqrt{d})}$ o g_{prod} do melhor QSTBC sobre o corpo base $\mathbb{Q}(\sqrt{d})$, segue que

$$g_{\text{ótimo } \mathbb{Q}(\sqrt{-11})} = \frac{33}{4} > g_{\text{ótimo } \mathbb{Q}(\sqrt{-7})} = 7 > g_{\text{ótimo } \mathbb{Q}(\sqrt{-2})} = 6 > g_{\text{ótimo } \mathbb{Q}(\sqrt{-1})} = 3\sqrt{2} > g_{\text{ótimo } \mathbb{Q}(\sqrt{-3})} = \frac{3}{4}\sqrt{21} \approx 3,44,$$

o que conclui o resultado. □

Neste capítulo apresentamos o calculo da probabilidade de erro em um sistema MIMO, e a partir dessa probabilidade de erro, definimos alguns parâmetros para construir STBC. Apresentamos os melhores QSTBC sobre $\mathbb{Q}(\sqrt{d})$, com $d = -1, -2, -3, -7$ e -11, segundo o critério produto, e provamos que o melhor QSTBC sobre $\mathbb{Q}(\sqrt{-3})$ é também, o melhor QSTBC dentre todos os QSTBC baseados em extensões quadráticas imaginárias dos racionais. Para o desenvolvimento deste capítulo utilizamos todas as ferramentas abordadas neste trabalho.

Conclusão Final

Este trabalho foi dedicado a construção de códigos de bloco espaço-temporais quadráticos baseados em extensões quadráticas imaginárias dos racionais. Para isso, inicialmente fizemos um estudo sobre alguns tópicos de teoria dos números algébricos e álgebras dos quatérnios. O conceito de norma serviu de base para a construção dos códigos do Capítulo 5. O fato de nossos códigos serem associados a uma álgebra de divisão dos quatérnios, garante a linearidade dos códigos e satisfazem $det(X) \neq 0$, para todo $X \in \mathcal{C}$. Com isso, segue que os códigos possuem diversidade máxima e consequentemente, maior confiabilidade na transmissão do sinal.

Em seguida, apresentamos um estudo sobre reticulados e densidade de empacotamento. Ao estudar a densidade de empacotamento um dos principais problemas é a obtenção de reticulados com maior densidade de empacotamento. Reticulados com boa densidade de empacotamento podem ser construídos via álgebras dos quatérnios e existem na literatura várias construções de reticulados com boa densidade de empacotamento via ferramentas algébricas.

Dando continuidade ao trabalho, estudamos o Lema de Hensel, que possibilitou mostrar que certos elementos do anel de inteiros algébricos de $\mathbb{Q}(\sqrt{d})$ não é uma norma algébrica de certas extensões dos racionais.

Por fim, apresentamos uma estrutura de códigos de bloco espaço-temporais $\mathcal{C}(\mathbb{F}, \alpha_1, \alpha_2, \gamma)$ baseado no artigo [24], que possui diversidade máxima e determinante mínimo igual a 1, quando definido sobre uma extensão quadrática imaginária dos racionais. Um dos critérios utilizados para avaliar esses códigos, proposto em [23], é o módulo do determinante da matriz geradora do código quando visto como um reticulado real. Quanto menor o módulo do determinante da matriz geradora, maior será o ganho de codificação e maior será a densidade de centro do código, isto significa que podemos empacotar mais palavras códigos dentro de um mesmo espaço e com isso as chances de decodificarmos corretamente serão maiores.

Para construir um código de bloco espaço-temporal quadrático sobre um corpo de números $\mathbb{F}$, precisamos tomar elementos α_1, α_2, e γ de modo que α_1 e α_2 sejam raízes de um polinômio $x^2 + px + q \in \mathcal{O}_{\mathbb{F}}[x]$ irredutível em $\mathbb{F}$, e $\gamma \in \mathcal{O}_{\mathbb{F}}$, com γ não sendo norma algébrica de $\mathbb{F}(\alpha_1)$ sobre $\mathbb{F}$. Para provar que γ não é norma algébrica de $\mathbb{F}(\alpha_1)$ sobre $\mathbb{F}$ usamos duas ferramentas: a caracterização dos elementos de $(1+i)\mathbb{Z}[i]$ e de $\sqrt{-3}\mathbb{Z}\left[\frac{1-\sqrt{-3}}{2}\right]$; e os corolários do Lema de Hensel, que estuda a norma mergulhada em $Q_p(\alpha_1)$. Apresentamos os melhores códigos baseados nos corpos bases $\mathbb{Q}(\sqrt{d})$, com $d = -1, -2, -3, -7$ e -11, e a partir do monomorfismo canônico, provamos que o código $\mathcal{C}(\mathbb{Q}(\zeta_3), \frac{-p+\sqrt{p^2-4q}}{2}, \frac{-p-\sqrt{p^2-4q}}{2}, \zeta_6)$, com $p = -1 - \zeta_6$ e $q = \sqrt{3}i$, é o melhor código dentre todos os códigos de bloco espaço-temporais quadráticos baseados em extensões quadráticas imaginárias dos racionais.

Os códigos de bloco espaço-temporais estão sendo estudados para transmitir informações utilizando antenas. Quando $|\gamma| \neq 1$ há um desbalanceamento de energia entre as antenas, no entanto, pela Referência [21], a transformação

$$\begin{pmatrix} a+b\sqrt{\beta} & \sqrt{\gamma}(c+d\sqrt{\beta}) \\ \sqrt{\gamma}(c-d\sqrt{\beta}) & a-b\sqrt{\beta} \end{pmatrix} \leftrightarrow \begin{pmatrix} a+b\sqrt{\beta} & c+d\sqrt{\beta} \\ \gamma(c-d\sqrt{\beta}) & a-b\sqrt{\beta} \end{pmatrix},$$

ajusta o desbalanceamento de energia entre as antenas.

Neste contexto, ainda existem muitas questões em aberto, como por exemplo, mudar o grau da extensão de $\mathbb{F}$ sobre os racionais, mudar o grau do polinômio irredutível, estudar outros critérios para avaliar a eficiência de um código, construir reticulados via as álgebras associadas aos códigos apresentados.

Os STBC's vem sendo amplamente explorados, com isso o uso de ferramentas algébricas torna-se cada vez mais necessário para resolver problemas de transmissão sem fio.

Referências

[1] ALVES, C.; BELFIORE, J.-C. Lattices from maximal orders into quaternion algebras. *J. Pure Appl. Algebra*, p. 687–702, 2015.

[2] BELFIORE, J.-C.; CIPRIANO, A. M. *Space-time coding for non-coherent channels*. [S.l.]: Cambridge University Press, 2006.

[3] BELFIORE, J.-C.; OGGIER, F.; VITERBO, E. *Cyclic Division Algebras: a Tool for Space-Time Coding*. [S.l.]: now Publishers Inc., 2007.

[4] BELFIORE, J.-C.; REKAYA, G. Quaternionic lattices for space-time coding. *Proceedings Information Theory Workshop*, v. 01, p. 1–4, 2003.

[5] 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*, v. 51, n. 4, p. 1432–1436, 2005.

[6] COHN, H.; KUMAR, A. Optimality and uniqueness of the leech lattice among lattices. *Annals of Mathematics*, v. 170, n. 3, p. 1003–1050, 2009.

[7] CONWAY, J. H.; SLOANE, N. J. A. *Sphere Packings, Lattices and Groups*. [S.l.]: Springer, 1990.

[8] GOUVêA, F. Q. *p-adic Numbers, An Introduction*. Berlim: Springer-Verlag, 1993.

[9] HOCHWALD, B. M.; MARZETTA, T. L. Unitary space-time modulation for multiple-antenna communications in rayleigh flat fading. *IEEE Transactions on Information Theory*, v. 46, n. 2, p. 543–564, 2000.

[10] HOLLANTI, C. et al. On the algebraic structure of the silver code: a 2×2 perfect space-time block code. *IEEE Information Theory Workshop*, v. 01, p. 91–94, 2008.

[11] HOLLANTI, C. et al. On the densest mimo lattices from cyclic division algebras. *IEEE Trans. Inf. Theory*, v. 58, n. 8, p. 3751–3780, 2009.

[12] LAGRANGE, J. L. *Recherches d'arithmétique*. Berlim: C.F. Voss, 1775.

[13] MARCUS, D. A. *Numbers Fields*. New York: Springer-Verlag, 1977.

[14] MOLLIN, R. A. *Algebraic Number Theory*. Alberta: CRC Press, University of Calgary, 2011.

[15] OGGIER, F. E. et al. Perfect space-time block codes. *IEEE Transactions on Information Theory*, v. 52, n. 9, p. 3885–3902, 2006.

[16] SAMUEL, P. *Algebraic Theory of Numbers*. Paris: Hermann, 1970.

[17] SLOANE, N. J. A.; CONWAY, J. H. *Sphere Packings, Lattices and Groups*. 3. ed. [S.l.]: Springer-Verlag New York, 1999.

[18] STEVENS, S. Local fields. *Anais da Escola de Matemática da Universidade de East Anglia*, p. http://www.mth.uea.ac.uk/∼h008/teaching/4A22/local.pdf, último acesso em junho de 2016.

[19] STEWART, I.; TALL, D. *Algebric Number Theory*. New York: Chapman & Hall, 1987.

[20] TAROKH, V.; SESHADRI, N.; CALDERBANK, A. R. Space-time block codes from orthogonal design. *IEEE Transactions on Information Theory*, v. 45, n. 5, p. 1456–1467, 1999.

[21] UNGER, T.; MARKIN, N. Quadratic forms and space-time block codes from generalized quaternion and biquaternion algebras. *IEEE Transactions on Information Theory*, v. 57, n. 9, p. 6148–6156, 2011.

[22] VOIGHT, J. *The arithmetic of quaternion algebra*. [S.l.]: book in preparation.

[23] WANG, G.; XIA, X.-G. On optimal multilayer cyclotomic space–time code designs. *IEEE Transactions on Information Theory*, v. 51, n. 3, p. 1102–1135, 2005.

[24] WANG, G.; ZHANG, J. K.; AMIN, M. Space-time block code designs based on quadratic field extension for two-transmitter antennas. *IEEE Transaction on Information Theory*, v. 58, n. 6, p. 4005–4013, 2012.

Índice Remissivo

UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Campus de São José do Rio Preto

TERMO DE REPRODUÇÃO XEROGRÁFICA

Autorizo a reprodução xerográfica do presente Trabalho de Conclusão, na íntegra ou em partes, para fins de pesquisa.

São José do Rio Preto, _____/_____/____

_____

Assinatura do autor