



UNIVERSIDADE ESTADUAL PAULISTA
“JÚLIO DE MESQUITA FILHO”
Faculdade de Ciências e Tecnologia
Câmpus de Presidente Prudente

Construção algébrica de reticulados via corpos biquadráticos

Marina Colle

Orientador: Prof. Dr. Agnaldo José Ferrari

Programa: Matemática Aplicada e Computacional

Presidente Prudente, agosto de 2025

UNIVERSIDADE ESTADUAL PAULISTA

Programa de Pós-Graduação em Matemática Aplicada e Computacional

Construção algébrica de reticulados via corpos biquadráticos

Marina Colle

Orientador: Prof. Dr. Agnaldo José Ferrari

Defesa apresentada ao Programa de Pós-Graduação em Matemática Aplicada e Computacional da UNESP para obtenção do título de Mestra em Matemática Aplicada e Computacional.

Presidente Prudente, agosto de 2025

| | |
|-------|---|
| C697c | <p>Colle, Marina</p> <p>Construção algébrica de reticulados via corpos biquadráticos / Marina Colle. -- Presidente Prudente, 2025</p> <p>71 f.</p> <p>Dissertação (mestrado) - Universidade Estadual Paulista (UNESP), Faculdade de Ciências e Tecnologia, Presidente Prudente</p> <p>Orientador: Agnaldo José Ferrari</p> <p>1. Reticulados. 2. Reticulados Algébricos. 3. Corpos Biquadráticos. 4. Densidade de Centro. 5. Bem Arredondados. I. Título.</p> |
|-------|---|

ATA DA DEFESA PÚBLICA DA DISSERTAÇÃO DE MESTRADO DE MARINA COLLE, DISCENTE DO PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA APLICADA E COMPUTACIONAL, DA FACULDADE DE CIÊNCIAS E TECNOLOGIA.

Aos 27 dias do mês de agosto do ano de 2025, às 15h30min, por meio de Videoconferência, realizou-se a defesa de DISSERTAÇÃO DE MESTRADO de MARINA COLLE, intitulada **Construção algébrica de reticulados via corpos biquadráticos**. A Comissão Examinadora foi constituída pelos seguintes membros: Prof. Dr. AGNALDO JOSÉ FERRARI (Orientador(a) - Participação Virtual) do(a) Departamento de Matemática / UNESP/Câmpus de Bauru, Prof. Dr. ANTONIO APARECIDO DE ANDRADE (Participação Virtual) do(a) Departamento de Matemática / UNESP/Câmpus de São José do Rio Preto, Profa. Dra. GRASIELE CRISTIANE JORGE (Participação Virtual) do(a) Câmpus de São José dos Campos / Universidade Federal de São Paulo-UNIFESP. Após a exposição pela mestrande e arguição pelos membros da Comissão Examinadora que participaram do ato, de forma presencial e/ou virtual, a discente recebeu o conceito final: APROVADA. Nada mais havendo, foi lavrada a presente ata, que após lida e aprovada, foi assinada pelo(a) Presidente(a) da Comissão Examinadora.

Prof. Dr. AGNALDO JOSÉ FERRARI



Documento assinado digitalmente

AGNALDO JOSE FERRARI

Data: 01/09/2025 09:07:01-0300

Verifique em <https://validar.iti.gov.br>

Agradecimentos

Este trabalho representa muito mais do que uma conquista individual, é o fruto do apoio e incentivo de diversas pessoas que acompanharam minha trajetória acadêmica e pessoal. Se hoje chego a esta etapa, devo isso à generosidade de muitos que, de diferentes formas, contribuíram para meu crescimento.

Em primeiro lugar, manifesto minha gratidão à minha noiva, Bruna, seu amor incondicional foi a base fundamental que sustentou minha trajetória acadêmica, enquanto sua paciência e generosidade iluminaram nosso caminho. Esta jornada, embora formalmente individual, foi desde seu início uma construção nossa, transformando madrugadas de estudo em diálogos enriquecedores e desafios acadêmicos em conquistas conjuntas.

Aos meus pais, Sandra e Roberto, pelo amor incondicional, apoio inestimável e por sempre acreditarem em meu potencial, mesmo nos momentos mais desafiadores. Vocês são minha base e minha maior inspiração. Em especial, dedico minha mais profunda homenagem à memória de minha querida mãe, Sandra, cujo amor e incentivo permanecem vivos em cada página desta dissertação. Embora sua partida precoce tenha ocorrido durante o desenvolvimento deste trabalho, seus ensinamentos, valores e o orgulho que sempre demonstrou por meus estudos foram o farol que me guiou mesmo nos momentos mais difíceis.

Ao Professor Agnaldo, pela orientação, paciência incomparável e apoio ao longo de todo o desenvolvimento desta pesquisa. Seu profundo conhecimento na área e incentivo constante foram determinantes para a conclusão deste trabalho.

Aos meus familiares e amigos que, de diversas formas, contribuíram para que eu chegasse até aqui. Obrigada pelo apoio emocional, pelas palavras de incentivo .

Por fim, agradeço a todas as pessoas que, direta ou indiretamente, participaram desta trajetória e contribuíram para a realização deste trabalho.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

“Continue a nadar”
Dory

Resumo

Esta dissertação aborda a construção de reticulados via corpos biquadráticos, estruturas fundamentais na teoria dos números e na análise combinatória. Os reticulados são definidos como conjuntos discretos de pontos em espaços euclidianos que apresentam propriedades específicas de simetria e periodicidade, e suas relações com extensões de corpos e a estrutura algébrica subjacente são exploradas. A pesquisa analisa detalhadamente os métodos de construção desses reticulados, utilizando ferramentas da álgebra linear e da teoria dos grupos, e apresenta exemplos que ilustram sua aplicação em problemas de empacotamento esférico e otimização de processos algébricos.

Palavras-Chave: *Reticulados, Reticulados Algébricos, Corpos Biquadráticos, Densidade de Centro, Bem Arredondados.*

Abstract

This dissertation focuses on the construction of lattices via biquadratic fields, which are fundamental structures in number theory and combinatorial analysis. Lattices are defined as discrete sets of points in Euclidean spaces that exhibit specific properties of symmetry and periodicity, and their relationships with field extensions and the underlying algebraic structure are explored. The research provides a detailed analysis of the construction methods for these lattices, utilizing tools from linear algebra and group theory, and presents examples that illustrate their application in spherical packing problems and the optimization of algebraic processes.

Keywords: *Lattices, Algebraic Lattices, Biquadratic Fields, Center Density.*

Sumário

| | |
|--|-----------|
| Resumo | 5 |
| Abstract | 7 |
| Introdução | 11 |
| 1 Conceitos básicos de álgebra | 13 |
| 1.1 Grupos | 13 |
| 1.2 Anéis e Corpos | 14 |
| 1.3 Ideais | 15 |
| 1.4 Anéis de Polinômios | 18 |
| 2 Teoria algébrica dos números | 21 |
| 2.1 Extensões de corpos finitas | 21 |
| 2.2 Extensões algébricas | 22 |
| 2.3 Corpo de raízes | 25 |
| 2.4 Extensões separáveis e inseparáveis | 26 |
| 2.5 Corpo Fixo | 28 |
| 2.6 Norma, traço e discriminante | 29 |
| 2.7 Corpos Quadráticos | 30 |
| 2.8 Corpos Biquadráticos | 32 |
| 3 Introdução aos reticulados | 35 |
| 3.1 Reticulado | 35 |
| 3.2 Empacotamento esférico | 38 |
| 3.3 Principais reticulados conhecidos na literatura | 41 |
| 4 Reticulados via corpos biquadráticos | 45 |
| 4.1 Construção | 45 |
| 4.2 Base reduzida de Minkowski | 51 |
| 4.3 Testes computacionais | 54 |
| 4.4 Reticulados bem arredondados | 56 |
| 4.5 Família de reticulados \mathbb{Z}^4 rotacionados | 60 |
| 5 Conclusão | 67 |
| Referências | 68 |

Introdução

O estudo dos reticulados no contexto da teoria dos números tem ocupado um papel fundamental na matemática moderna, em especial devido às suas conexões com a geometria e suas aplicações em áreas como criptografia e teoria da informação. Os reticulados surgem naturalmente em problemas que envolvem otimização geométrica, como o empacotamento esférico e a busca de estruturas com densidade máxima. Esses aspectos são de grande interesse tanto para a teoria algébrica dos números quanto para a teoria dos reticulados, oferecendo métodos para explorar propriedades algébricas e geométricas com aplicações relevantes.

Neste trabalho, focamos na construção de reticulados via corpos biquadráticos e na análise de suas propriedades fundamentais, como norma mínima, raio de empacotamento e densidade. O objetivo principal é desenvolver uma abordagem algébrica para a construção desses reticulados utilizando corpos biquadráticos, o que permite a construção de reticulados com características específicas e controláveis. Este estudo contribui para a análise da eficiência de tais características dentro do contexto teórico.

A pesquisa conduzida neste trabalho se destaca pela inovação em explorar a construção de reticulados a partir de corpos biquadráticos, fornecendo novas perspectivas sobre as propriedades geométricas e algébricas desses reticulados. Assim, este estudo busca ampliar a compreensão sobre as relações entre propriedades algébricas de corpos e as estruturas geométricas de reticulados, oferecendo uma visão integrada entre a teoria algébrica dos Números e a teoria dos reticulados.

A dissertação é organizada nos capítulos seguintes, cada um tratando de um aspecto específico do estudo:

- **Capítulo 2: Conceitos básicos de álgebra** – Apresentamos conceitos fundamentais como grupos, anéis, ideais, anéis de polinômios, extensões de corpos finitas, extensões algébricas, corpos de raízes e extensões separáveis e inseparáveis.
- **Capítulo 3: Teoria algébrica dos números** – Aborda temas como corpo fixo, normas, traços, discriminantes, corpos quadráticos e conceitos de corpos biquadráticos.
- **Capítulo 4: Introdução aos reticulados** – São apresentados os conceitos iniciais sobre reticulados, como região fundamental, matriz de Gram, matriz geradora e volume, além de tópicos sobre empacotamento esférico e os principais reticulados conhecidos na literatura.
- **Capítulo 5: Reticulados via corpos biquadráticos** – Apresenta a construção de reticulados via esses corpos.

A metodologia adotada neste trabalho é predominantemente teórica e se baseia na utilização de corpos biquadráticos como ferramenta para a construção de reticulados, o que envolve o desenvolvimento de técnicas algébricas e geométricas específicas para esse tipo de estrutura. Além disso, o uso do grupo de Galois e do teorema do elemento

primitivo é fundamental para estabelecer as bases teóricas que sustentam as construções propostas.

Em resumo, esta dissertação busca contribuir para a teoria dos reticulados com uma abordagem que integra conceitos algébricos e geométricos, oferecendo percepções que podem abrir caminho para estudos mais aplicados ou para avanços na compreensão da densidade e das propriedades estruturais de reticulados.

Conceitos básicos de álgebra

Neste capítulo, abordaremos as definições de grupos, anéis e corpos, além das noções de extensões de corpos e suas propriedades fundamentais. Esses conceitos servem como base para a compreensão das condições necessárias e suficientes para que uma extensão finita de corpos seja gerada por um único elemento, culminando na formulação e demonstração do Teorema do Elemento Primitivo. Para este capítulo utilizamos as referências [3] e [4].

1.1 Grupos

Definição 1. *Um conjunto não vazio G , munido de uma operação binária $*$: $G \times G \rightarrow G$ é chamado de grupo, denotado por $(G, *)$, se as seguintes propriedades forem satisfeitas para quaisquer $a, b, c \in G$:*

1. *Associatividade: $(a * b) * c = a * (b * c)$.*
2. *Existência do elemento neutro: Há um elemento $e \in G$ tal que $a * e = e * a = a$ para todo $a \in G$. O elemento e é chamado de neutro em relação à operação.*
3. *Existência do elemento inverso: Para cada $a \in G$, existe $a' \in G$ tal que $a * a' = a' * a = e$. O elemento a' é denominado inverso ou simétrico de a .*

Se, adicionalmente, a operação $$ for comutativa (isto é, $a * b = b * a$ para todos $a, b \in G$), o grupo é chamado de abeliano ou comutativo.*

Um subconjunto não vazio $H \subseteq G$ é chamado de subgrupo de G se H , munido da mesma operação $$, também satisfizer as condições de grupo.*

Denotamos os grupos G dotados das operações aditiva e multiplicativa por $(G, +)$ e (G, \cdot) , respectivamente. Como exemplos de grupos aditivos, temos $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$ e $(\mathbb{Z}, +)$; e como grupos multiplicativos, temos (\mathbb{R}^*, \cdot) e (\mathbb{Q}^*, \cdot) , onde as notações \mathbb{R}^* e \mathbb{Q}^* denotam os conjuntos $\mathbb{R} - \{0\}$ e $\mathbb{Q} - \{0\}$, respectivamente. Note que o conjunto \mathbb{Z}^* com a operação multiplicativa não possui uma estrutura de grupo.

Definição 2. *Seja G um grupo.*

1. *Dizemos que G é um grupo finito (respec. infinito) se G for um conjunto finito (respec. infinito).*
2. *Se G for um grupo finito, o número de elementos de G é chamado a ordem de G e é denotada por $o(G)$.*

Um importante grupo finito que introduzimos agora é o grupo dos inteiros módulo n , que denotamos por \mathbb{Z}_n e que é muito utilizado na geração de alfabetos de códigos corretores de erros, em sistemas criptográficos, processamento de sinais, etc. A operação de adição módulo n é definida da seguinte forma: dizemos que um inteiro r é a soma de dois inteiros s e t , módulo n , se r for o resto da divisão de $s + t$ por n . Desta forma, tem-se que $\mathbb{Z}_n = \{0, 1, 2, \dots, n - 1\}$, onde $n \geq 2$. De maneira análoga, define-se a operação produto módulo n , para $n \geq 2$. Denotamos as operações de adição módulo n e multiplicação módulo n por \oplus e \odot , respectivamente.

Teorema 1. *O conjunto \mathbb{Z}_n é um grupo sob a operação de adição módulo n .*

Teorema 2. *Se p é um número primo, então o conjunto $\mathbb{Z}_p^* = \{1, 2, \dots, p - 1\}$ é um grupo sob a operação de multiplicação módulo p .*

Observação 1. *Para se obter uma estrutura de grupo multiplicativo em $\mathbb{Z}_n - \{0\} = \{1, 2, \dots, n - 1\}$, é essencial a hipótese de que n seja primo, ou seja, não é possível construir grupos multiplicativos $\mathbb{Z}_n - \{0\}$ para n que não seja um número primo.*

Definição 3. *Seja G um grupo multiplicativo. Um subconjunto S de G com a propriedade de que todo elemento de G pode ser escrito como um produto de elementos de S é denominado conjunto de geradores de G . Denota-se por $G = \langle S \rangle$ e diz-se que G é gerado por S .*

Definição 4. *Um grupo G é dito cíclico se existir pelo menos um elemento $a \in G$, chamado de gerador, tal que todos os elementos do grupo podem ser obtidos como potências de a (no caso multiplicativo) ou como múltiplos inteiros de a (no caso aditivo).*

Formalmente, para um grupo multiplicativo temos $G = \{a^m \mid m \in \mathbb{Z}\}$, e para um grupo aditivo temos $G = \{ma \mid m \in \mathbb{Z}\}$. O elemento gerador a é dito gerador do grupo G , e denotamos $G = \langle a \rangle$. Um grupo cíclico pode possuir vários geradores distintos.

Definição 5. *Considere os grupos $(G, *)$ e (G', \circ) . Uma aplicação $\phi : G \rightarrow G'$, tal que*

$$\phi(a * b) = \phi(a) \circ \phi(b), \quad \text{para todo } a, b \in G,$$

*é chamada de homomorfismo de G em G' . Se esta aplicação for bijetiva, diremos que ϕ é um isomorfismo. Se $(G, *) = (G', \circ)$ e ϕ é um isomorfismo, diremos que ϕ é um automorfismo.*

1.2 Anéis e Corpos

Definição 6. *Seja A um grupo aditivo, e considere as seguintes propriedades:*

1. *Distributiva da multiplicação com relação à adição (à esquerda), isto é,*

$$a(b + c) = ab + ac, \quad \text{para todos } a, b, c \in A.$$

2. *Distributiva da multiplicação com relação à adição (à direita), isto é,*

$$(b + c)a = ba + ca, \quad \text{para todos } a, b, c \in A.$$

3. *Associativa, isto é, $a(bc) = (ab)c$, para todos $a, b, c \in A$.*

4. *Comutativa, isto é, $ab = ba$, para todos $a, b \in A$.*

Se as propriedades 1), 2) e 3) forem satisfeitas, diremos que o grupo $(A, +)$ é um anel e o denotamos por $(A, +, \cdot)$. Se, além disso, a propriedade 4) for satisfeita, diremos que A é um anel comutativo. Quando existir uma identidade multiplicativa 1_A em A que satisfaça a relação $1_A x = x 1_A$ para todo $x \in A$, diremos que A é um anel com unidade.

Definição 7. Um subconjunto não vazio S de um anel A é chamado de subanel de A quando S é fechado em relação às operações de adição e multiplicação definidas em A e, munido dessas operações, constitui ele próprio um anel.

Proposição 1. Um subconjunto não vazio $S \subseteq A$ é um subanel de A se, e somente se, para quaisquer $x, y \in S$, tem-se que $x - y \in S$ e $xy \in S$.

Definição 8. Seja A um anel e $a \in A$ não-nulo.

(a) O elemento $a \in A$ é denominado divisor de zero se existe $b \in A$ não-nulo tal que $ab = 0$.

(b) Seja A um anel com unidade. O elemento $a \in A$ é dito inversível se existir $a^{-1} \in A$ tal que $aa^{-1} = 1 = a^{-1}a$.

Definição 9. Um anel comutativo com unidade é chamado de domínio de integridade se não tiver divisores de zeros.

Por exemplo, o conjunto dos números inteiros \mathbb{Z} é um domínio de integridade uma vez que forma um anel comutativo com unidade e não contém divisores de zeros.

Definição 10. Um anel com unidade em que todo elemento não nulo seja inversível é chamado de anel de divisão.

Definição 11. Se A é um anel comutativo com unidade, dizemos que A é um corpo se, para todo $0 \neq x \in A$, existe $y \in A$ tal que $xy = 1$.

Um subconjunto não vazio de um corpo é um subcorpo se ele é também um corpo. Veremos ao longo deste capítulo resultados importantes relativos aos corpos. Uma propriedade importante dos anéis é sua característica. Para defini-la, utilizamos a ordem de um elemento do anel, considerada sobre seu grupo aditivo. Dado $a \in A$, a ordem $o(a)$ é definida como o menor inteiro positivo m tal que $a + a + \cdots + a = m \cdot a = 0$. Se não existe tal inteiro positivo, temos $o(a) = \infty$. Para todo $n \in \mathbb{Z}$, temos que $n \cdot a = 0$ se, e somente se, $o(a)$ divide n . Dado qualquer $a \in A$, vale que se $o(1) \neq \infty$, então $o(a)$ divide $o(1)$.

Além disso, se $o(a) \neq o(1)$ então a é um divisor de zero de A . Assim, definimos:

Definição 12. A característica de um anel A é dada por

$$\text{char}(A) = \begin{cases} 0, & \text{se } o(1) = \infty \\ n, & \text{se } o(1) = n \neq \infty \end{cases}$$

sendo chamadas característica zero e característica positiva, respectivamente.

1.3 Ideais

Definição 13. Sejam $(A, +, \cdot)$ um anel e $I \subset A$, com $I \neq \emptyset$. Diremos que I é um Ideal de A se $(I, +)$ for um subgrupo de $(A, +)$ e, para todo $r \in A$ e $a \in I$, temos $ra \in I$.

Proposição 2. Se A for um anel e $I \subset A$, com $I \neq \emptyset$, então I é um ideal de A se, e somente se, para todo $a, b \in I$ e $r \in A$, temos $ra + b \in I$.

Definição 14. *Seja A um anel e $a \in A$. O conjunto $\langle a \rangle := \{ra \mid r \in A\}$ é um ideal de A , chamado de ideal principal gerado por a .*

Definição 15. *Seja A um anel e I um ideal de A , definimos $a + I = \{a + x, x \in I\}$*

Definição 16. *Sejam A um anel e I um ideal de A , definimos $A/I = \{a + I, a \in A\}$*

Definição 17. *No conjunto A/I a operação*

$$(a + I) + (b + I) = (a + b) + I, \quad \text{para todo } a, b \in A,$$

está bem definida e as seguintes condições são verificadas:

(i) *A classe $0 + I$ é o elemento neutro para esta operação.*

(ii) *$a + I = b + I$ se, e somente se, $a - b \in I$. Neste caso, dizemos que $a \equiv b \pmod{I}$.*

Proposição 3. *O conjunto $A/I = \{a + I, a \in A\}$ com a operação de adição definida acima é um grupo.*

Assim, dotamos A/I com uma estrutura de grupo aditivo. A notação $a \equiv b \pmod{I}$ significa que os elementos a e b de A estão na mesma classe lateral, isto é, representam o mesmo elemento em A/I . Agora, definimos a operação de multiplicação de classes laterais:

$$(a + I)(b + I) = (ab) + I, \quad \text{para todo } a, b \in A.$$

Proposição 4. *O conjunto A/I com as operações de adição e multiplicação acima definidas é um anel, chamado de anel quociente de A sobre I*

Definição 18. *Dado um subconjunto M de um anel A , definimos o **subanel de A gerado por M** como a intersecção*

$$[M] = \bigcap A'$$

com $A' \in S_M$, em que S_M representa o conjunto de todos os subanéis de A que contêm M . Desse modo, temos que $[M]$ é o menor subanel de A que contém M . Além disso, $S_\emptyset = S_{\{0\}} = S_{\{1\}}$ é o conjunto de todos os subanéis de A . Então $[\emptyset] = [\{0\}] = [\{1\}]$ é o menor subanel de A , denominado subanel primo de A .

Definição 19. *Dado um subconjunto $P \subseteq K$, o subcorpo de K gerado por P é definido pela intersecção $\bigcap K'$, com $K' \in J_P$, tal que J_P representa o conjunto dos subcorpos de K que contêm P . Este é o menor subcorpo de K contendo P . Além disso, $J_\emptyset = J_{\{0\}} = J_{\{1\}}$ é o conjunto de todos os subcorpos de K e, portanto, o subcorpo gerado por $\{1\}$ (ou $\{0\}$) é o menor subcorpo de K , denominado subcorpo primo de K .*

Todo subanel de A tem a mesma característica de A . Além disso, se A for um domínio, então

$$\text{char}(A) = 0 \quad \text{ou} \quad \text{char}(A) = p,$$

sendo p um número primo, com $o(a) = \infty$ ou $o(a) = p$, respectivamente, para qualquer $a \in A$.

Pela característica, podemos determinar o subanel primo S de qualquer anel A . Tomando o homomorfismo de \mathbb{Z} em A , dado por $m \mapsto m \cdot 1$, temos que se $\text{char}(A) = 0$, então

$$S = \{m \cdot 1 \mid m \in \mathbb{Z}\}$$

é isomorfo a \mathbb{Z} e, se $\text{char}(A) = n \neq 0$, então

$$S = \{m \cdot 1 \mid m = 0, 1, \dots, n - 1\}$$

é isomorfo a $\mathbb{Z}/n\mathbb{Z}$.

De forma análoga, pela característica de um corpo \mathbb{K} , necessariamente igual a zero ou a um primo p , podemos determinar o subcorpo primo de \mathbb{K} . Denotando este último por K_0 , se $\text{char}(\mathbb{K}) = 0$, então K_0 é isomorfo a \mathbb{Q} . Se $\text{char}(\mathbb{K}) = p$, então K_0 coincide com o subanel primo de \mathbb{K} , pois este é um corpo isomorfo a $\mathbb{Z}/p\mathbb{Z}$.

Se o anel A/I for finito, então o número de elementos A/I é chamado de norma do ideal I .

Se A é um anel comutativo, então A/I também é comutativo, pois $(a + I)(b + I) = ab + I = ba + I = (b + I)(a + I)$. Por outro lado, se A possui unidade 1 , então A/I possui unidade $1 + I$. Além disso, podemos aplicar aos anéis quocientes um resultado conhecido em grupos. Existe um homomorfismo sobrejetor ϕ de A em A/I , dado por $\phi(a) = a + I$, para todo $a \in A$, cujo núcleo é I . Isto nos leva ao seguinte lema.

Lema 1. *Se A é um anel com ideal I , então A/I é uma imagem homomorfa de A .*

A partir desta construção de anel quociente, podemos transpor para anéis um resultado visto para grupos, que descreve a imagem de um anel sob um homomorfismo sobrejetor. Este resultado é dado pelo seguinte teorema.

Teorema 3. *Seja $\phi : A \rightarrow R$ um homomorfismo sobrejetor de anéis, com núcleo I . Então, R é isomorfo a A/I . Além disso, existe uma correspondência biunívoca entre o conjunto dos ideais de R e o conjunto dos ideais de A que contêm I , que associa a um ideal U de R o ideal W de A , dado por $W = \{x \in A \mid \phi(x) \in U\}$. Nesse caso, A/W é isomorfo a R/U .*

A seguir, consideramos dois casos de ideais I de um anel A , de modo que A/I seja um domínio ou um corpo. Para isso, precisamos definir dois tipos particulares de ideais, como segue.

Definição 20. *Um ideal U de um anel A é chamado de ideal primo de A se $U \neq A$ e, dados quaisquer $x, y \in A$, então $xy \in U$ implica $x \in U$ ou $y \in U$.*

Definição 21. *Um ideal $M \neq A$ de A é chamado de ideal maximal de A se, dado um ideal U de A tal que $M \subset U \subset A$, então $M = U$ ou $A = U$.*

Assim, um ideal M de A é maximal se não existe nenhum ideal entre ele e o anel A . Em outras palavras, M é maximal quando é o maior elemento do conjunto $I_A \setminus \{A\}$, que consiste nos ideais de A , exceto o próprio A .

Proposição 5. *O ideal U de A é primo se, e somente se, A/U é um domínio.*

Proposição 6. *O ideal M de um anel A é maximal se, e somente se, A/M é um corpo.*

Corolário 1. *O ideal $\langle 0 \rangle$ de A é primo (respectivamente maximal) se, e somente se, o anel A é um domínio (respectivamente um corpo).*

Corolário 2. *Todo ideal maximal é um ideal primo.*

1.4 Anéis de Polinômios

Um polinômio sobre o corpo \mathbb{F} é uma expressão da forma

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

onde os coeficientes a_n, a_{n-1}, \dots, a_0 são elementos de \mathbb{F} e o índice e os expoentes são números inteiros positivos. O polinômio nulo é dado por $f(x) = 0$, ou seja, todos os seus coeficientes são iguais a 0, e é o elemento neutro em relação à adição do corpo \mathbb{F} . Dizemos que dois polinômios $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ e $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ são iguais se, e somente se, $a_i = b_i$ em \mathbb{F} , para todo $i \in \mathbb{N}$.

Um polinômio é dito mônico se o coeficiente que multiplica o termo x^n é igual a 1. O grau de um polinômio não nulo $f(x)$, denotado por $\partial(f)$, é o índice do coeficiente a_n , se este for não-nulo, e por convenção, o grau do polinômio nulo é $-\infty$.

Seja $\mathbb{F}[x]$ o conjunto de todos os polinômios na variável x sobre \mathbb{F} . Sejam $f(x) = \sum_{i=0}^n a_i x^i$ e $g(x) = \sum_{i=0}^m b_i x^i$ tal que $f(x), g(x) \in \mathbb{F}[x]$. A soma de $f(x)$ e $g(x)$ é definida por $f(x) + g(x) = \sum_{i=0}^{\max\{n,m\}} (a_i + b_i) x^i$. Assim, a soma de polinômios também é um polinômio. O produto de $f(x)$ e $g(x)$ é definido por $f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k$, onde $c_k = \sum_{i+j=k} a_i b_j$, onde $0 \leq i \leq n, 0 \leq j \leq m$. Assim, o produto de polinômios também é um polinômio. Logo, pode ser mostrado que o conjunto $\mathbb{F}[x]$ de todos os polinômios sobre \mathbb{F} forma um anel comutativo com unidade sob as operações de adição e multiplicação de polinômios.

Definição 22. *Dados dois polinômios $f(x), g(x) \in \mathbb{F}[x]$, tem-se que:*

$$\partial(f + g) \leq \max\{\partial(f), \partial(g)\} \quad e \quad \partial(fg) = \partial(f) + \partial(g).$$

Dizemos que um polinômio $f(x) \in \mathbb{F}[x]$ é divisível pelo polinômio $g(x) \in \mathbb{F}[x]$ se existir um polinômio $h(x) \in \mathbb{F}[x]$ tal que $f(x) = g(x)h(x)$, e denota-se por $g(x) \mid f(x)$. Um polinômio $p(x) \in \mathbb{F}[x]$ que é divisível somente por elementos $\alpha \in \mathbb{F}$, ou seja, somente por polinômios de grau zero em \mathbb{F} , é dito polinômio irredutível sobre \mathbb{F} .

Definição 23. *O máximo divisor comum de dois polinômios $f(x), g(x) \in \mathbb{F}[x]$, denotado por $\text{mdc}(f(x), g(x))$, é um polinômio $d(x)$ que satisfaz as seguintes condições:*

1. $d(x) \mid f(x)$ e $d(x) \mid g(x)$,
2. Se $d'(x) \mid f(x)$ e $d'(x) \mid g(x)$, para algum $d'(x) \in \mathbb{F}[x]$, então $d'(x) \mid d(x)$.

O mínimo múltiplo comum de dois polinômios $f(x), g(x) \in \mathbb{F}[x]$, denotado por $\text{mmc}(f(x), g(x))$, é um polinômio $m(x)$ que satisfaz as seguintes condições:

1. $f(x) \mid m(x)$ e $g(x) \mid m(x)$,
2. Se $f(x) \mid m'(x)$ e $g(x) \mid m'(x)$, para algum $m'(x) \in \mathbb{F}[x]$, então $m(x) \mid m'(x)$.

Além disso, se $f(x), g(x) \in \mathbb{F}[x]$ satisfazem a condição de que $f(x) \mid g(x)$ e $g(x) \mid f(x)$, então $f(x) = \alpha g(x)$, onde $\alpha \in \mathbb{F}$. De fato, se $f(x) = r(x)g(x)$ e $g(x) = s(x)f(x)$, onde $r(x), s(x) \in \mathbb{F}[x]$, então $f(x) = s(x)r(x)f(x)$. Logo, $\partial(sr) = 0$, ou seja, $s(x)r(x)$ é um elemento de \mathbb{F} .

Teorema 4. *Para todo par de polinômios não nulos $f(x), g(x) \in \mathbb{F}[x]$, existe um único par de polinômios $q(x), r(x) \in \mathbb{F}[x]$ (quociente e resto, respectivamente) tal que*

$$g(x) = f(x)q(x) + r(x),$$

com $r(x) = 0$ ou $\partial(r) < \partial(g)$.

Teorema 5 (Fatoração única). *Se $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{F}[x]$ com $n \geq 1$, então $p(x)$ fatora-se de forma única (salvo a ordem dos fatores) como o produto de polinômios irredutíveis em $\mathbb{F}[x]$, salvo constante $\alpha \in \mathbb{F}$.*

Teorema 6. *Sejam $f(x)$ e $g(x)$ polinômios em $\mathbb{F}[x]$ tal que $\partial(f) \geq \partial(g) \geq 0$. Se*

$$\begin{aligned} f(x) &= q_1(x)g(x) + r_1(x) \\ g(x) &= q_2(x)r_1(x) + r_2(x) \\ &\dots \\ r_{n-3}(x) &= q_{n-1}(x)r_{n-2}(x) + r_{n-1}(x) \\ r_{n-2}(x) &= q_n(x)r_{n-1}(x) + r_n(x) \\ r_{n-1}(x) &= q_{n+1}(x)r_n(x), \end{aligned}$$

é uma sequência de divisões, onde o processo termina quando é obtido um resto zero. Então, $r_n(x) = \alpha \text{mdc}(f(x), g(x))$, com $\alpha \in \mathbb{F}$.

Corolário 3. *Seja $p(x), g(x) \in \mathbb{F}[x]$, então existem $a(x), b(x) \in \mathbb{F}[x]$ tais que*

$$\text{mdc}(p(x), g(x)) = a(x)p(x) + b(x)g(x). \quad (1.1)$$

Definição 24. *Um elemento $\beta \in \mathbb{F}$ é uma raiz ou zero do polinômio $f(x) \in \mathbb{F}[x]$ se $f(\beta) = 0$.*

Teorema 7. *Sejam $\beta \in \mathbb{F}$ e $f(x) \in \mathbb{F}[x]$, então $f(\beta) = 0$ se, e somente se, $(x - \beta)$ é um fator de $f(x)$, ou seja, $f(x) = (x - \beta)q(x)$, para algum $q(x) \in \mathbb{F}[x]$. Mais ainda, se $\partial(f) = n$, então existem no máximo n zeros em $f(x)$.*

Dado um polinômio $f(x) \in \mathbb{F}_p[x]$, onde \mathbb{F}_p denota o corpo finito com p elementos (sendo p primo), tem-se que o conjunto

$$\langle f(x) \rangle = \{g(x)f(x) : g(x) \in \mathbb{F}_p[x]\} = I \quad (1.2)$$

é um ideal em $\mathbb{F}_p[x]$. Podemos então formar o anel quociente $\mathbb{F}_p[x]/I$, cujos elementos são classes laterais de I em $\mathbb{F}_p[x]$. O conjunto dos representantes de todas essas classes laterais consiste de todos os polinômios de grau menor do que o grau de $f(x)$. As operações em $\mathbb{F}_p[x]/I$ são, respectivamente, a soma e o produto módulo I .

Exemplo 1. *Para o corpo \mathbb{F}_2 e o polinômio $f(x) = x^2 + x$ sobre \mathbb{F}_2 , tem-se que os elementos $0, 1, x, 1 + x$ formam o anel $\mathbb{F}_2[x]/\langle x^2 + x \rangle$, ou seja, são os representantes das classes laterais de $f(x) = x^2 + x$ em $\mathbb{F}_2[x]$. Esses representantes formam um anel com as operações de soma e produto módulo $x^2 + x$.*

Definição 25. *Dizemos que um polinômio sobre um subanel K de \mathbb{C} é redutível se for produto de dois polinômios de menor grau sobre K . Caso contrário, o polinômio é dito irredutível.*

Teorema 8. *O anel $\mathbb{F}_p[x]/\langle p(x) \rangle$ é um corpo se, e somente se, $p(x)$ é um polinômio irredutível.*

O Teorema [8](#) é a base para construir um corpo finito \mathbb{F} . Tomando $p(x)$ um polinômio irredutível de grau m sobre \mathbb{F}_p , tem-se que os elementos de \mathbb{F} podem ser considerados como todos os polinômios de grau menor ou igual a $m - 1$ com coeficientes em \mathbb{F}_p , e existem p^m de tais polinômios. Esses polinômios também podem ser vistos como todas as m -uplas sobre \mathbb{F}_p , e em ambas representações têm adição e multiplicação módulo $p(x)$.

Fazendo uso apenas da estrutura aditiva, tem-se que o conjunto de todas as m -uplas é um espaço vetorial sobre \mathbb{F}_p de dimensão m , e portanto este espaço vetorial tem p^m elementos. Finalmente, fazendo uso da estrutura aditiva e multiplicativa, tem-se que \mathbb{F} é um corpo com p^m elementos.

Queremos mostrar que o grupo multiplicativo $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$ de todo corpo finito é um grupo cíclico, ou seja, existe um elemento não nulo $\alpha \in \mathbb{F}_q$ que gera os elementos de $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$.

Exemplo 2. Em $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$, o elemento 2 gera o grupo multiplicativo $\mathbb{F}_5^* = \mathbb{F}_5 - \{0\}$.

Teorema 9. Se $\beta_1, \dots, \beta_{q-1}$ são os elementos não nulos de \mathbb{F}_q , então

$$x^{q-1} - 1 = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_{q-1}). \quad (1.3)$$

Definição 26. Um gerador do grupo multiplicativo de \mathbb{F}_q é chamado de elemento primitivo de \mathbb{F}_q .

Teorema 10 (Elemento primitivo). Todo corpo finito \mathbb{F} possui um elemento primitivo.

Demonstração. Suponha que \mathbb{F} tenha q elementos. Como $x^{q-1} = 1$, para todo $x \in \mathbb{F}^*$, segue que todos os elementos de \mathbb{F}^* têm ordem menor ou igual a $q-1$. Queremos mostrar que \mathbb{F}^* possui um elemento de ordem $q-1$. Seja $a \in \mathbb{F}^*$ um elemento de ordem máxima m . Portanto, devemos provar que $m = q-1$. Afirmamos que, se $b \in \mathbb{F}^*$, então a ordem de b divide a ordem de a . De fato, se $ds = o(b)$, onde $d = \text{mdc}(ds, m)$, então $\text{mdc}(s, m) = 1$. Devemos então mostrar que $s = 1$. Se $s > 1$, então teríamos que a ordem de b^d seria $s > 1$, e portanto a ordem de ab^d seria $ms > m$, contradizendo a maximalidade da ordem de a . Logo, todo elemento de \mathbb{F}^* satisfaz a equação $x^m - 1 = 0$, e assim, $q-1 = |\mathbb{F}^*| \leq m$. Como $m \leq q-1$, segue que $m = o(a) = q-1$, o que prova o teorema. ■

Pelo Teorema [10](#), conclui-se que existe $\alpha \in \mathbb{F}_q^*$ tal que

$$\mathbb{F}_q^* = \{\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{q-2}\}.$$

Além disso, $\alpha^{q-1} = 1$, e, portanto, nesta representação, a operação de multiplicação fica extremamente simplificada. Mais precisamente,

$$\alpha^i \alpha^j = \alpha^{[i+j]},$$

onde $[i+j]$ representa o resto da divisão de $i+j$ por $q-1$. Em contrapartida, nesta representação, a operação de adição se torna mais complicada. Para efetuar a adição, usam-se certas tabelas chamadas de tabelas logarítmicas de Zech, que descrevemos a seguir. Para $n \leq m$ tem-se que

$$\alpha^n + \alpha^m = \alpha^n(1 + \alpha^{m-n}).$$

Para cada r , se determinarmos o inteiro $z(r)$ tal que $1 + \alpha^r = \alpha^{z(r)}$, teremos que

$$\alpha^n + \alpha^m = \alpha^n \alpha^{z(m-n)}.$$

Portanto, para efetuar a adição em \mathbb{F}_q , escolhe-se um elemento primitivo $\alpha \in \mathbb{F}_q^*$ e utilizam-se as propriedades da representação exponencial dos elementos do corpo.

Teoria algébrica dos números

Este capítulo trata de importantes conceitos ligados às extensões de corpos. Exploramos estruturas fundamentais como o Grupo de Galois e o Corpo Fixo, além de ferramentas como a Norma, o Traço e o Discriminante, que fornecem informações valiosas sobre essas extensões. Também discutimos a relevância dos corpos ciclotômicos, quadráticos e biquadráticos, analisando suas propriedades dentro desse contexto teórico. As referências utilizadas nesse capítulo são [1] e [3].

2.1 Extensões de corpos finitas

Definição 27. *Seja \mathbb{K} um corpo. Uma extensão de \mathbb{K} é um par (\mathbb{L}, ι) onde \mathbb{L} é um corpo e $\iota : \mathbb{K} \rightarrow \mathbb{L}$ um monomorfismo.*

Uma extensão \mathbb{L} de \mathbb{K} pode ser interpretada como um \mathbb{K} -espaço vetorial, com as operações definidas no corpo \mathbb{L} . Em outras palavras, \mathbb{L} é um espaço vetorial sobre o corpo \mathbb{K} . Assim, podemos definir o grau dessa extensão a partir da dimensão desse espaço vetorial, conforme a seguir.

Definição 28. *O grau da extensão $\mathbb{L}|\mathbb{K}$, denotado por $[\mathbb{L} : \mathbb{K}]$, é definido como a dimensão do espaço vetorial \mathbb{L} sobre o corpo \mathbb{K} , isto é, $[\mathbb{L} : \mathbb{K}] := \dim_{\mathbb{K}} \mathbb{L}$.*

Dizemos que a extensão é finita se $[\mathbb{L} : \mathbb{K}]$ for finito; caso contrário, a extensão é dita infinita. Quando um conjunto $\{\beta_1, \beta_2, \dots, \beta_n\} \subseteq \mathbb{L}$ for uma base de \mathbb{L} como um \mathbb{K} -espaço vetorial, então dizemos que este conjunto é uma base da extensão $\mathbb{L}|\mathbb{K}$.

Proposição 7. *Dada uma extensão $\mathbb{L}|\mathbb{K}$, temos que $[\mathbb{L} : \mathbb{K}] = 1$ se, e somente se, $\mathbb{L} = \mathbb{K}$.*

Demonstração. Suponha que $[\mathbb{L} : \mathbb{K}] = 1$. O conjunto $\{1\}$ é linearmente independente e, portanto, é uma base de $\mathbb{L}|\mathbb{K}$. Logo, se $a \in \mathbb{L}$, então $a = d \cdot 1$ com $d \in \mathbb{K}$, ou seja, $a \in \mathbb{K}$. Portanto, $\mathbb{L} \subseteq \mathbb{K}$, de onde segue que $\mathbb{L} = \mathbb{K}$. Reciprocamente, se $\mathbb{L} = \mathbb{K}$, então $\{1\}$ é uma base da extensão $\mathbb{L}|\mathbb{K}$, e portanto $[\mathbb{L} : \mathbb{K}] = 1$. ■

O próximo resultado nos apresenta uma importante propriedade de extensões finitas, no que diz respeito à multiplicidade dos graus de uma extensão contida em outra.

Teorema 11 (Multiplicidade dos graus). *Sejam $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ corpos. Então $[\mathbb{L}|\mathbb{K}]$ é finita, se, e somente se, $[\mathbb{L}|\mathbb{M}]$ e $[\mathbb{M}|\mathbb{K}]$ são finitas. Neste caso, $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{M}][\mathbb{M} : \mathbb{K}]$.*

Demonstração. Sejam $[\mathbb{L} : \mathbb{K}] < \infty$ e B uma base de \mathbb{L} sobre \mathbb{K} . Temos que $\mathbb{M}|\mathbb{K}$ é finita, uma vez que \mathbb{M} é um subespaço de um espaço vetorial de dimensão finita. Para mostrar a

finitude de $\mathbb{L}|\mathbb{M}$, basta observar que existe $B' \subset B$ que é linearmente independente sobre \mathbb{M} .

Suponha que $[\mathbb{L} : \mathbb{M}] = m$, $[\mathbb{M} : \mathbb{K}] = n$ e sejam $\{v_1, \dots, v_m\}$ uma base de \mathbb{L} sobre \mathbb{M} e $\{w_1, \dots, w_n\}$ uma base de \mathbb{M} sobre \mathbb{K} . Mostraremos que $\tilde{B} := \{v_i w_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ é uma base de \mathbb{L} sobre \mathbb{K} . De fato, se $\alpha \in \mathbb{L}$, então existem $\alpha_1, \dots, \alpha_m \in \mathbb{M}$ tais que $\alpha = \sum_{i=1}^m \alpha_i v_i$, onde cada α_i é da forma:

$$\alpha_i = \sum_{j=1}^n \beta_{ij} w_j, \quad \beta_{ij} \in \mathbb{K}, \quad 1 \leq j \leq n.$$

Logo,

$$\alpha = \sum_{i=1}^m \left(\sum_{j=1}^n \beta_{ij} w_j \right) v_i = \sum_{i=1}^m \sum_{j=1}^n \beta_{ij} (v_i w_j).$$

Portanto, \tilde{B} gera \mathbb{L} como \mathbb{K} -espaço vetorial. Para mostrar a \mathbb{K} -independência linear dos elementos de \tilde{B} , seja:

$$\sum_{i=1}^m \sum_{j=1}^n \beta_{ij} (v_i w_j) = 0 \Rightarrow \sum_{j=1}^n \left(\sum_{i=1}^m \beta_{ij} v_i \right) w_j = 0.$$

Como w_1, \dots, w_n são linearmente independentes, para cada j , temos:

$$\sum_{i=1}^m \beta_{ij} v_i = 0.$$

Pela independência linear de v_1, \dots, v_m , concluímos que $\beta_{ij} = 0$, para todos $1 \leq i \leq m$ e $1 \leq j \leq n$. Portanto, \tilde{B} é uma base de \mathbb{L} sobre \mathbb{K} . Para finalizar, observamos que:

$$|\tilde{B}| = [\mathbb{L} : \mathbb{K}] = mn = [\mathbb{L} : \mathbb{M}][\mathbb{M} : \mathbb{K}].$$

■

2.2 Extensões algébricas

Seja \mathbb{K} um corpo.

Definição 29. *Sejam $\mathbb{L}|\mathbb{K}$ uma extensão e $\alpha \in \mathbb{L}$. Diremos que α é algébrico sobre \mathbb{K} se existir $f \in \mathbb{K}[x] \setminus \{0\}$ tal que $f(\alpha) = 0$. Caso contrário, diremos que α é transcendente sobre \mathbb{K} . Se $\mathbb{K} = \mathbb{Q}$, diremos simplesmente que α é algébrico ou transcendente.*

Para garantir a existência de elementos algébricos em qualquer extensão, basta observar que todos os elementos de \mathbb{K} são algébricos sobre \mathbb{K} : se $\alpha \in \mathbb{K}$, então α é raiz de $f(x) = x - \alpha$.

Definição 30. *Seja $\mathbb{L}|\mathbb{K}$ uma extensão e α algébrico sobre \mathbb{K} . O polinômio mônico $f(x) \in \mathbb{K}[x]$ de menor grau tal que $f(\alpha) = 0$ é chamado do polinômio minimal de α sobre \mathbb{K} denotado por $\min(\alpha, \mathbb{K})$ ou $\min_{\mathbb{K}}(\alpha)$.*

Proposição 8. *Sejam $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ corpos, $\alpha \in \mathbb{L}$ algébrico sobre \mathbb{K} , com $\min_{\mathbb{K}}(\alpha) = p$ e $\min_{\mathbb{M}}(\alpha) = q$. Então vale:*

- p é irredutível em $\mathbb{K}[x]$;

- se $f \in \mathbb{K}[x]$ e $f(\alpha) = 0$, então $p \mid f$;
- $q \mid p$.

Demonstração. Para provar a irredutibilidade de p , suponha que p é redutível, ou seja, $p = fg$, com $f, g \in \mathbb{K}[x] \setminus \mathbb{K}$. Então, como $p(\alpha) = 0$, devemos ter $f(\alpha) = 0$ ou $g(\alpha) = 0$, isto contradiz o fato de p ser o polinômio de menor grau. Portanto p é irredutível.

Para o segundo item, pelo algoritmo de divisão, existem $q, r \in \mathbb{K}[x]$ tais que $f = pq + r$, com $r = 0$ ou $\partial(r) < \partial(p)$. Por hipótese $p(\alpha) = f(\alpha) = 0$, então $r(\alpha) = 0$, o que só é válido se $r = 0$, pois p é minimal. Portanto $p \mid f$.

O fato de que $q \mid p$ é consequência do segundo item, visto que $p \in \mathbb{M}[x]$. ■

Teorema 12 (Critério de Eisenstein). *Seja $f(x) = a_n x^n + \dots + a_1 x + a_0$ um polinômio sobre \mathbb{Z} . Se existe um número primo p tal que*

1. $p \nmid a_n$,
2. $p \mid a_i$ para $i = 0, \dots, n-1$,
3. $p^2 \nmid a_0$,

então f é irredutível sobre \mathbb{Q} .

Demonstração. Utilizando o Lema de Gauss, basta mostrar que f é irredutível sobre \mathbb{Z} . Para isto, suponha que f é redutível sobre \mathbb{Z} , ou seja, $f = gh$, onde

$$g = b_0 + b_1 x + \dots + b_r x^r \quad \text{e} \quad h = c_0 + c_1 x + \dots + c_s x^s$$

são polinômios de menor grau sobre \mathbb{Z} , com $r + s = n$. Temos que $a_0 = b_0 c_0$ e, pelo segundo item, $p \mid b_0$ ou $p \mid c_0$. Pelo terceiro item, p não pode dividir b_0 e c_0 ao mesmo tempo. Então, sem perda de generalidade, podemos supor que $p \mid b_0$ e $p \nmid c_0$. Se todos os coeficientes b_j são divisíveis por p , então $p \mid a_n$, o que contradiz o primeiro item. Então, seja b_j o primeiro coeficiente de g não divisível por p . Então

$$a_j = b_j c_0 + \dots + b_0 c_j, \quad \text{com } j < n.$$

Isto implica que $p \mid c_0$, pois p divide a_j, b_1, \dots, b_{j-1} , mas não b_j , o que é uma contradição. Portanto, f é irredutível sobre \mathbb{Z} e, por consequência, sobre \mathbb{Q} . ■

Exemplo 3. *Determine o polinômio $\min_{\mathbb{Q}}(\sqrt[3]{2})$.*

Seja $\alpha = \sqrt[3]{2}$. Então, $\alpha^3 - 2 = 0$, ou seja, α é raiz da equação $x^3 - 2 = 0$. Pelo critério de Eisenstein, $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ é irredutível sobre \mathbb{Z} e, portanto, sobre \mathbb{Q} . Então,

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

Exemplo 4. *Determine o polinômio $\min_{\mathbb{Q}}(\sqrt{2} + \sqrt{3})$.*

Seja $\alpha = \sqrt{2} + \sqrt{3}$. Então,

$$\alpha^2 = 5 + 2\sqrt{6} \implies (\alpha^2 - 5)^2 = 24 \implies x^4 - 10x^2 + 1 = 0.$$

Ou seja, α é raiz de $f = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$. Este polinômio não possui raiz em \mathbb{Q} , uma vez que $f(\pm 1) \neq 0$ e $f(x) = (x^2 - (5 + 2\sqrt{6}))(x^2 + (5 + 2\sqrt{6}))$. Essas observações mostram que f é irredutível sobre \mathbb{Q} , portanto,

$$\min_{\mathbb{Q}}(\sqrt{2} + \sqrt{3}) = x^4 - 10x^2 + 1.$$

Proposição 9. *Sejam $\mathbb{L}|\mathbb{K}$ uma extensão e $\alpha \in \mathbb{L}$ algébrico sobre \mathbb{K} . Então $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$, ou seja o anel gerado por α sobre \mathbb{K} é igual ao corpo gerado por α sobre \mathbb{K} .*

Definição 31. *Um número complexo $\theta \in \mathbb{C}$ é denominado inteiro algébrico se existe um polinômio mônico $p(x) \in \mathbb{Z}[x]$ tal que $p(\theta) = 0$. Equivalentemente, θ é um inteiro algébrico se for raiz de uma equação polinomial cujos coeficientes são inteiros, ou ainda, se seu polinômio minimal $\text{irr}(\theta, \mathbb{Q})$ (o polinômio mônico irredutível de menor grau em $\mathbb{Q}[x]$ que tem θ como raiz) tiver coeficientes inteiros. O conjunto $\mathcal{B} = \{\alpha \in \mathbb{C} \mid \text{irr}(\alpha, \mathbb{Q}) \in \mathbb{Z}[x]\}$ de todos os inteiros algébricos complexos forma um subanel de \mathbb{C} , chamado anel dos inteiros algébricos de \mathbb{C} .*

Dado um corpo de números \mathbb{K} de grau n , o anel de inteiros algébricos de \mathbb{K} é o conjunto $\mathcal{O}_{\mathbb{K}} = \mathcal{B} \cap \mathbb{K}$ dos elementos de \mathbb{K} que são inteiros algébricos. Este conjunto pode ser caracterizado como $\mathcal{O}_{\mathbb{K}} = \{\alpha \in \mathbb{K} \mid \exists f(x) \in \mathbb{Z}[x] \text{ mônico com } f(\alpha) = 0\}$ e constitui um subanel de \mathbb{K} que contém todos os inteiros algébricos de \mathbb{K} .

Definição 32. *Seja \mathbb{K} um corpo de números. O conjunto*

$$\mathcal{O}_{\mathbb{K}} = \{x \in \mathbb{K} \mid x \text{ é inteiro algébrico sobre } \mathbb{Z}\}$$

é um anel, chamado de anel de inteiros de $\mathbb{K}|\mathbb{Q}$.

Teorema 13. *Sejam $\mathbb{L}|\mathbb{K}$ uma extensão e $\alpha \in \mathbb{L}$ algébrico sobre \mathbb{K} tal que $p = \min_{\mathbb{K}}(\alpha)$, $\partial(p) = n$, então*

1. $\mathbb{K}[x]/\langle p \rangle \simeq \mathbb{K}(\alpha)$;
2. $\{1, \alpha, \dots, \alpha^{n-1}\}$ é uma base de $\mathbb{K}(\alpha)$ sobre \mathbb{K} . Em particular $[\mathbb{K}(\alpha) : \mathbb{K}] = \partial(p)$.

Demonstração. Pela irredutibilidade de p , o ideal $\langle p \rangle$ é um ideal maximal de $\mathbb{K}[x]$. Então, $\mathbb{K}[x]/\langle p \rangle$ é um corpo. Seja $\phi : \mathbb{K}[x] \rightarrow \mathbb{K}(\alpha)$, definido por $\phi(f) = f(\alpha)$. Claramente, ϕ é um homomorfismo sobrejetivo. Afirmamos que $\ker(\phi) = \langle p \rangle$. Se $f \in \ker(\phi)$, então $f(\alpha) = 0$. Pelo item (2) da Proposição 8, temos que $p \mid f$, ou seja, $f \in \langle p \rangle$. Como $\langle p \rangle \subseteq \ker(\phi)$, concluímos que $\ker(\phi) = \langle p \rangle$. Pelo Teorema do Isomorfismo para anéis, temos que:

$$\mathbb{K}[x]/\langle p \rangle \simeq \mathbb{K}[\alpha] = \mathbb{K}(\alpha).$$

Pela proposição anterior, $\mathbb{K}(\alpha) = \mathbb{K}[\alpha] = \{f(\alpha) \mid f \in \mathbb{K}[x]\}$. Pelo algoritmo da divisão, existem $q, r \in \mathbb{K}[x]$ tais que $f = pq + r$, com $r = 0$ ou $\partial(r) < \partial(p) = n$, ou seja, $r = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{K}[x]$. Logo,

$$f(\alpha) = \sum_{i=0}^{n-1} a_i \alpha^i.$$

Isto é, $\{1, \alpha, \dots, \alpha^{n-1}\}$ gera $\mathbb{K}(\alpha)$ sobre \mathbb{K} . A independência linear deste conjunto segue do fato de que $\partial(p) = n$ e $p = \min_{\mathbb{K}}(\alpha)$. ■

Definição 33. *Uma extensão $\mathbb{L}|\mathbb{K}$ é algébrica se todo $\alpha \in \mathbb{L}$ é algébrico sobre \mathbb{K} .*

Teorema 14. *Toda extensão finita é algébrica.*

Demonstração. Sejam $\mathbb{L}|\mathbb{K}$ uma extensão finita e $\alpha \in \mathbb{L}$. Então $\mathbb{K} \subseteq \mathbb{K}(\alpha) \subseteq \mathbb{L}$. Pelo Teorema 11, $[\mathbb{K}(\alpha) : \mathbb{K}] < \infty$. Suponha que $[\mathbb{K}(\alpha) : \mathbb{K}] = m$, então $\{1, \alpha, \dots, \alpha^m\}$ é linearmente dependente sobre \mathbb{K} . Daí, existem $a_0, \dots, a_m \in \mathbb{K}$, não todos nulos, tais que $\sum_{i=0}^m a_i \alpha^i = 0$. Ou seja, α é raiz de $f = \sum_{i=0}^m a_i x^i \in \mathbb{K}[x]$, portanto é algébrico sobre \mathbb{K} . ■

Exemplo 5. Nesse exemplo, veremos que $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ e $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Temos que $x^2 - 2 = \min_{\mathbb{Q}}(\sqrt{2})$ e $x^2 - 3 = \min_{\mathbb{Q}}(\sqrt{3})$. Como $\min_{\mathbb{Q}}(\sqrt{3}) = (x - \sqrt{3})(x + \sqrt{3})$ e $x \pm \sqrt{3} \in \mathbb{Q}(\sqrt{2})[x]$, segue que $\min_{\mathbb{Q}(\sqrt{2})}(\sqrt{3}) = x^2 - 3$. Pela multiplicidade dos graus, considerando $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$, Concluímos que $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$. Como $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ e mais ainda, o polinômio minimal de α sobre \mathbb{Q} é $p(x) = x^4 - 10x^2 + 1$, que é irredutível e de grau 4. Assim, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Portanto, conclui-se que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

2.3 Corpo de raízes

Sejam \mathbb{K} um corpo e $f \in \mathbb{K}[x]$. Se quisermos falar das raízes de f , precisamos considerar extensões de \mathbb{K} . Nesta seção garantiremos a existência de uma extensão de \mathbb{K} onde f possui todas as raízes.

Teorema 15. *Seja $f \in \mathbb{K}[x]$ um polinômio irredutível. Então existe uma extensão $\mathbb{L}|\mathbb{K}$ tal que f possui ao menos uma raiz em \mathbb{L} .*

Demonstração. Pela irredutibilidade de f , $\mathbb{L} := \mathbb{K}[x]/\langle f \rangle$ como um corpo. Defina $\phi : \mathbb{K} \rightarrow \mathbb{L}$ por $\phi(a) = \bar{a} = a + \langle f \rangle$. Claramente, ϕ é um homomorfismo de anéis. Provemos que ϕ é injetora. Seja $a \in \text{Ker}(\phi)$, temos que $\bar{a} = \bar{0} \Rightarrow f \mid a \Rightarrow a = 0$. Pela injetividade de ϕ , podemos identificar \mathbb{K} como um subcorpo de \mathbb{L} e assumir que $\bar{a} = a$, se $a \in \mathbb{K}$. Verificaremos que $\alpha = \bar{x} = x + \langle f \rangle$ é uma raiz de f . Seja $f(x) = a_0 + a_1x + \dots + a_nx^n$, temos que:

$$f(\alpha) = \bar{a}_0 + \bar{a}_1\bar{x} + \dots + \bar{a}_n\bar{x}^n = \overline{a_0 + a_1x + \dots + a_nx^n} = 0.$$

Logo, \mathbb{L} é uma extensão de \mathbb{K} que contém α . ■

Definição 34. *Seja $f \in \mathbb{K}[x]$. Diremos que $\mathbb{L}|\mathbb{K}$ é um corpo de raízes de f , se \mathbb{L} é o menor corpo contendo \mathbb{K} e todas as raízes de f . Denotamos \mathbb{L} por $\mathbb{K}(R_f)$.*

Observação 2. *Se $\mathbb{L} = \mathbb{K}(R_f)$, temos que:*

1. *f se decompõe em produto de fatores lineares, ou seja, existem $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{L}$ tais que $f = c(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$ com $c \in \mathbb{K}$.*
2. *\mathbb{L} é o menor corpo contendo $\alpha_1, \alpha_2, \dots, \alpha_n$, ou seja, $\mathbb{L} \simeq \mathbb{K}(\alpha_1, \alpha_2, \dots, \alpha_n)$.*

Teorema 16 (Existência do corpo de raízes [3]). *Todo $f \in \mathbb{K}[x] \setminus \mathbb{K}$ possui um corpo de raízes.*

Demonstração. Seja $n = \partial(f)$. Provemos o teorema por indução sobre n . Se $\partial(f) = 1$, então f admite uma única raiz em \mathbb{K} , e portanto $\mathbb{K} = \mathbb{K}(R_f)$. Suponha que $\partial(f) > 1$ e que o teorema se verifica para todo polinômio g tal que $\partial(g) < n$. Pelo teorema anterior, existe uma extensão \mathbb{L} de \mathbb{K} contendo uma raiz α de f . Então, $f = (x - \alpha)g$, com $g \in \mathbb{L}[x]$ e $\partial(g) < \partial(f)$. Assim, pela hipótese de indução, existe um corpo contendo todas as raízes de g . Tomando \mathbb{F} como o menor nessas condições, $\mathbb{F}(\alpha)$ é um corpo de raízes de f . ■

2.4 Extensões separáveis e inseparáveis

Estudaremos elementos $\alpha \in \mathbb{L}$ que satisfazem duas condições de ser algébricos sobre \mathbb{K} e suas raízes no polinômio minimal $\min_{\alpha, \mathbb{K}}$ são simples. A multiplicidade de uma raiz α em um polinômio $f \in \mathbb{K}[x]$ é o maior inteiro m para o qual $(x - \alpha)^m$ divide f . Quando uma raiz tem multiplicidade 1, esta é dita uma raiz simples. Se a multiplicidade é maior que 1, a raiz recebe o nome de raiz múltipla de f .

Definição 35. *Seja $f \in \mathbb{K}[x]$ \mathbb{K} . Diremos que f é separável se todas as raízes de f são simples no seu corpo de raízes. Caso contrário, diremos que f é inseparável. Numa extensão algébrica $\mathbb{L}|\mathbb{K}$, um elemento $\alpha \in \mathbb{L}$ é dito separável se $p = \min_{\mathbb{K}} \alpha$ é separável. Uma extensão algébrica $\mathbb{L}|\mathbb{K}$ é separável se todo $\alpha \in \mathbb{L}$ é separável.*

Proposição 10. *Sejam $\mathbb{L}|\mathbb{K}$ algébrica e $\text{char}(\mathbb{K}) = 0$. Então $\mathbb{L}|\mathbb{K}$ é separável.*

Demonstração. Sejam $\alpha \in \mathbb{L}$ e $p = \min_{\mathbb{K}} \alpha$. De $\text{char}(\mathbb{K}) = 0$, concluímos que $\partial(p') = \partial(p) - 1$, onde p' é a derivada de p . Pela minimalidade do grau de p , $p'(\alpha) \neq 0$, ou seja, α é uma raiz simples de p . ■

Corolário 4. *Sejam $\mathbb{L}|\mathbb{K}$ algébrica e $\text{char}(\mathbb{K}) = 0$. Se $f \in \mathbb{K}[x]$ é irredutível sobre \mathbb{K} e $\partial(f) = n$, então f possui n raízes distintas em $\mathbb{K}(R_f)$.*

Demonstração. Seja α uma raiz de f . Pela irredutibilidade de f , $\min_{\mathbb{K}} \alpha = f$. Na demonstração da proposição anterior vimos que todas as raízes de f são simples, logo distintas. ■

Proposição 11. *Sejam $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ corpos e $\mathbb{L}|\mathbb{K}$ separável. Então $\mathbb{M}|\mathbb{K}$ e $\mathbb{L}|\mathbb{M}$ são separáveis.*

Demonstração. Claramente $\mathbb{M}|\mathbb{K}$ é separável. Provemos que $\mathbb{L}|\mathbb{M}$ é separável. Sejam $\alpha \in \mathbb{L}$, $p = \min_{\mathbb{K}} \alpha$ e $q = \min_{\mathbb{M}} \alpha$. Portanto, $q \mid p$ em $\mathbb{M}[x]$ e todas as raízes de q em \mathbb{M} são raízes de p . Como α é separável sobre \mathbb{K} , p é separável sobre \mathbb{K} e, portanto, q é separável sobre \mathbb{M} . Logo, $\mathbb{L}|\mathbb{M}$ é separável. ■

Definição 36. *Uma extensão $\mathbb{L}|\mathbb{K}$ é simples se $\mathbb{L} = \mathbb{K}(\alpha)$ para algum $\alpha \in \mathbb{L}$. Neste caso, α é chamado de elemento primitivo de \mathbb{L} .*

O teorema a seguir fornece uma condição para que uma extensão seja simples

Teorema 17 (Elemento primitivo). *Uma extensão finita $\mathbb{L}|\mathbb{K}$ é simples se, e somente se, existe um número finito de corpos \mathbb{F} tal que $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{L}$.*

A demonstração deste teorema pode ser vista no [6]. A seguir, daremos uma prova num caso particular.

Teorema 18. *Sejam $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{C}$ corpos. Se $\mathbb{L}|\mathbb{K}$ é finita, então existe $\gamma \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\gamma)$.*

Demonstração. Pela finitude de $\mathbb{L}|\mathbb{K}$, existe uma base de elementos algébricos $\{\alpha_1, \dots, \alpha_n\}$ de \mathbb{L} sobre \mathbb{K} e $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$. Por indução sobre n , basta mostrarmos o caso $n = 2$: se $\mathbb{L} = \mathbb{K}(\alpha, \beta)$, então existe $\gamma \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\gamma)$.

Sejam $p = \min_{\mathbb{K}} \alpha$ e $q = \min_{\mathbb{K}} \beta$ com $\partial(p) = r$ e $\partial(q) = s$. Pelo Corolário (4), p (resp. q) tem r raízes distintas (resp. s) em \mathbb{C} . Suponha que $R_p = \{\alpha_1 = \alpha, \dots, \alpha_r\}$ e $R_q = \{\beta_1 = \beta, \dots, \beta_s\}$. Sejam $\lambda_{ij} = \frac{\alpha_i - \alpha}{\beta - \beta_i} \in \mathbb{C}$, $i = 1, \dots, r$ e $j = 2, \dots, s$. Como \mathbb{K} é um conjunto infinito, existe $\lambda \in \mathbb{K}$ $\{\lambda_{ij} \mid 1 \leq i \leq r, 2 \leq j \leq s\}$.

Defina $\gamma := \alpha + \lambda\beta$ e $f(x) := p(\gamma - \lambda x)$. Temos que $f \in \mathbb{K}(\gamma)[x]$ e $f(\beta) = p(\gamma - \lambda\beta) = p(\alpha) = 0$. Afirmamos que para todo j , $f(\beta_j) \neq 0$. Caso contrário, se $f(\beta_j) = 0$ para algum $j \neq 1$, então $p(\gamma - \lambda\beta_j) = 0$, ou, $\gamma - \lambda\beta_j = \alpha_i$ para algum i . Então

$$\alpha + \lambda\beta - \lambda\beta_j = \alpha_i - \alpha, \quad \text{ou seja,} \quad \lambda_{ij} = \frac{\alpha_i - \alpha}{\beta - \beta_j},$$

o que contradiz a escolha de λ . Isso garante que $\text{mdc}_{\mathbb{C}[x]}(f, q) = (x - \beta)$.

Claramente, $\text{mdc}_{\mathbb{K}(\gamma)[x]}(f, q) \mid \text{mdc}_{\mathbb{C}[x]}(f, q)$. Então

$$\text{mdc}_{\mathbb{K}(\gamma)[x]}(f, q) = 1 \quad \text{ou} \quad (x - \beta).$$

Se $\text{mdc}_{\mathbb{K}(\gamma)}(f, q) = 1$, teríamos $\text{mdc}_{\mathbb{C}[x]}(f, q) = 1$, pois $\mathbb{K}[\gamma] \subseteq \mathbb{C}$. Logo, $\text{mdc}_{\mathbb{K}(\gamma)}(f, q) = (x - \beta)$ e isso ocorre se $\beta \in \mathbb{K}(\gamma)$. Sendo $\alpha = \gamma - \lambda\beta$, concluímos que $\alpha, \beta \in \mathbb{K}(\gamma)$ e daí, $\mathbb{L} = \mathbb{K}(\alpha, \beta) \subseteq \mathbb{K}(\gamma)$. Por outro lado, $\gamma \in \mathbb{L}$ e $\mathbb{K} \subseteq \mathbb{L}$ implica em $\mathbb{K}(\gamma) \subseteq \mathbb{L}$. Portanto, $\mathbb{L} = \mathbb{K}(\gamma)$. ■

A demonstração do teorema nos fornece um algoritmo para determinar o elemento primitivo. Veja o exemplo a seguir.

Exemplo 6. $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\sqrt{2} + \sqrt{5})$ Pela demonstração do Teorema (18), para cada $\lambda \neq 0$, $\frac{\sqrt{2}}{\sqrt{5}}$, temos que $\gamma = \sqrt{2} + \lambda\sqrt{5}$ é um elemento primitivo de $\mathbb{Q}(\sqrt{2}, \sqrt{5})$. Em particular, $\lambda = 1$.

Teorema 19. Sejam \mathbb{K} e \mathbb{K}' corpos tais que $\mathbb{Q} \subseteq \mathbb{K}, \mathbb{K}' \subseteq \mathbb{C}$ e $\sigma : \mathbb{K} \rightarrow \mathbb{K}'$ um isomorfismo. Seja $f \in \mathbb{K}[x]$ irredutível sobre \mathbb{K} . Então para cada par $\alpha \in R_f$ e $\beta \in R_{f^\sigma}$ existe um único isomorfismo $\tilde{\sigma} : \mathbb{K}(\alpha) \rightarrow \mathbb{K}'(\beta)$ tal que $\tilde{\sigma}(\alpha) = \beta$ e $\tilde{\sigma}|_{\mathbb{K}} = \sigma$.

Demonstração. Seja $r : \partial(f) = \partial(f^\sigma)$. Pela irredutibilidade de f sobre \mathbb{K} , para todo $\alpha \in R_f$, temos que $[\mathbb{K}(\alpha) : \mathbb{K}] = r$, e analogamente $[\mathbb{K}'(\beta) : \mathbb{K}'] = r$ para $\beta \in R_{f^\sigma}$.

Pelo Teorema 13, $\{1, \alpha, \dots, \alpha^{r-1}\}$ é uma base de $\mathbb{K}(\alpha)$ sobre \mathbb{K} e $\{1, \beta, \dots, \beta^{r-1}\}$ é uma base de $\mathbb{K}'(\beta)$ sobre \mathbb{K}' . Definamos o homomorfismo $\tilde{\sigma} : \mathbb{K}(\alpha) \rightarrow \mathbb{K}'(\beta)$ tal que

$$\tilde{\sigma}(\alpha^i) = \beta_i, \quad i = 1, \dots, r-1.$$

Claramente, $\tilde{\sigma}$ é sobrejetivo. Mostremos que $\tilde{\sigma}$ é injetiva. Seja $p(\alpha) = \sum_{i=0}^{r-1} a_i \alpha^i$ tal que $\tilde{\sigma}(p(\alpha)) = 0$. Então $\sum_{i=0}^{r-1} \sigma(a_i) \beta^i = 0$, portanto, para todo i , temos $\sigma(a_i) = 0$, que implica $a_i = 0$, ou seja, $p(\alpha) = 0$.

A unicidade segue do fato de que $\{1, \alpha, \dots, \alpha^{r-1}\}$ é uma base de $\mathbb{K}(\alpha)$ sobre \mathbb{K} e $\tilde{\sigma}$ é um homomorfismo tal que $\tilde{\sigma}(\alpha) = \beta$. ■

Teorema 20. Sejam \mathbb{K} e \mathbb{K}' corpos tais que $\mathbb{Q} \subseteq \mathbb{K}, \mathbb{K}' \subseteq \mathbb{C}$ e $\sigma : \mathbb{K} \rightarrow \mathbb{K}'$ um isomorfismo. Se $f \in \mathbb{K}[x]$, $\mathbb{L} = \mathbb{K}(R_f)$ e $\mathbb{L}' = \mathbb{K}'(R_{f^\sigma})$, então existe um isomorfismo $\hat{\sigma} : \mathbb{L} \rightarrow \mathbb{L}'$ tal que $\hat{\sigma}|_{\mathbb{K}} = \sigma$.

Demonstração. Seja $R_f = \{\alpha_1, \dots, \alpha_r\}$, então $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_r)$. Claramente, $\mathbb{L}|\mathbb{K}$ é finita. Demonstraremos o teorema por indução sobre $n = [\mathbb{L} : \mathbb{K}]$.

Se $n = 1$, temos $\mathbb{L} = \mathbb{K}$ e

$$R_f \subseteq \mathbb{K} \Rightarrow R_{f^\sigma} \subseteq \mathbb{K}' \Rightarrow \mathbb{K}(R_{f^\sigma}) \subseteq \mathbb{K}' \Rightarrow \mathbb{L}' = \mathbb{K}'.$$

Nesse caso, tome $\hat{\sigma} = \sigma$.

Suponha $n > 1$ e que o teorema se verifica para todo \mathbb{M} tal que $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ com $[\mathbb{L} : \mathbb{M}] < n$. Como $n > 1$, temos $\mathbb{K} \subseteq \mathbb{L}$, então existe $\alpha \in R_f \setminus \mathbb{K}$. Seja $p = \min_{\mathbb{K}} \alpha$, então $[\mathbb{K}(\alpha) : \mathbb{K}] = \partial(p) > 1$ e $p|_f$, daí $p^\sigma |_{f^\sigma}$ então existe $\beta \in R_{f^\sigma}$ tal que $p^\sigma(\beta) = 0$. Pelo teorema anterior, existe $\tilde{\sigma} : \mathbb{K}(\alpha) \rightarrow \mathbb{K}'(\beta)$ tal que $\tilde{\sigma}(\alpha) = \beta$ e $\tilde{\sigma}|_{\mathbb{K}} = \sigma$.

Como $\mathbb{L} = \mathbb{K}(\alpha)(R_f)$ e $\mathbb{L}' = \mathbb{K}'(\beta)(R_{f^\sigma})$ e $[\mathbb{L} : \mathbb{K}(\alpha)] < n$, existe um isomorfismo $\hat{\sigma} : \mathbb{L} \rightarrow \mathbb{L}'$ tal que $\hat{\sigma}|_{\mathbb{K}(\alpha)} = \tilde{\sigma}$. Logo, existe um isomorfismo $\hat{\sigma} : \mathbb{L} \rightarrow \mathbb{L}'$ tal que $\hat{\sigma}|_{\mathbb{K}} = \sigma$. ■

2.5 Corpo Fixo

Uma das ideias principais da Teoria de Galois é poder estudar as extensões de corpos a partir de grupos e vice-versa. Agora veremos como definir um corpo a partir de um grupo, que no caso será um subgrupo do grupo de Galois da extensão.

Definição 37. Um automorfismo em um corpo \mathbb{L} é definido como um isomorfismo de anéis de \mathbb{L} em \mathbb{L} . O conjunto de todos os automorfismos de \mathbb{L} é denotado por $\text{Aut}(\mathbb{L})$.

Definição 38. Seja \mathbb{L} uma extensão do corpo \mathbb{K} . O grupo de Galois de $\mathbb{L}|\mathbb{K}$, denotado por $\text{Gal}(\mathbb{L}|\mathbb{K})$, é definido pelo conjunto de todos os \mathbb{K} -automorfismos de \mathbb{L} , ou seja,

$$\text{Gal}(\mathbb{L}|\mathbb{K}) = \{\sigma \in \text{Aut}(\mathbb{L}); \sigma|_{\mathbb{K}} = \text{Id}\}.$$

Proposição 12. Sejam $\mathbb{L}|\mathbb{K}$ uma extensão e $H \subseteq \text{Aut}(\mathbb{L})$. Defina

$$\mathcal{F}(H) := \{\alpha \in \mathbb{L} \mid \sigma(\alpha) = \alpha, \text{ para todo } \sigma \in H\}.$$

Então $\mathcal{F}(H)$ é um subcorpo de \mathbb{L} . Se $H = \text{Gal}(\mathbb{L}|\mathbb{K})$, então $\mathbb{K} \subseteq \mathcal{F}(H)$.

Demonstração. Sejam $\alpha, \beta \in \mathcal{F}(H)$ e $\sigma \in H$. Temos:

$$\sigma(\alpha \pm \beta) = \sigma(\alpha) \pm \sigma(\beta) = \alpha \pm \beta,$$

e

$$\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \alpha\beta.$$

Além disso, se $0 \neq \alpha \in \mathcal{F}(H)$, temos:

$$\sigma(\alpha^{-1}) = (\sigma(\alpha))^{-1} = \alpha^{-1}.$$

Portanto, $\mathcal{F}(H)$ é um subcorpo de \mathbb{L} . A segunda afirmação segue da definição de grupo de Galois. ■

Definição 39. O subcorpo $\mathcal{F}(H)$ é chamado de corpo fixo associado a H .

Definição 40. Uma \mathbb{Z} -base para o grupo aditivo $\mathcal{O}_{\mathbb{L}}$ é chamada de base integral \mathbb{L} ou de $\mathcal{O}_{\mathbb{L}}$.

Lema 2. Seja $\mathbb{L}|\mathbb{K}$ uma extensão finita, separável e simples, ou seja, existe $\alpha \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\alpha)$. Se $H = \{\sigma_1, \dots, \sigma_n\}$ é um subgrupo de $G = \text{Gal}(\mathbb{L}|\mathbb{K})$ e $f = (x - \sigma_1(\alpha)) \cdots (x - \sigma_n(\alpha))$, então $f \in \mathcal{F}(H)[x]$ e $[\mathbb{L} : \mathcal{F}(H)] \leq |H|$.

Demonstração. Para todo $\sigma \in H$, considere

$$f_{\sigma} = (x - (\sigma \circ \sigma_1)(\alpha)) \cdots (x - (\sigma \circ \sigma_n)(\alpha)) = f,$$

pois pela Proposição 12 concluímos que $\{\sigma_1, \dots, \sigma_n\} = \{\sigma \circ \sigma_1, \dots, \sigma \circ \sigma_n\}$ para todo $\sigma \in H$. Colocando $f = \sum_{i=0}^n a_i x^i$ e considerando $f_{\sigma} = f$, obtemos:

$$\sum_{i=0}^n a_i x^i = \sum_{i=0}^n \sigma(a_i) x^i,$$

ou seja, $\sigma(a_i) = a_i$ para todo $\sigma \in H$. Logo, $a_i \in \mathcal{F}(H)$ para todo i , então $f \in \mathcal{F}(H)[x]$.

Temos $\mathbb{L} = \mathcal{F}(H)(\alpha)$, pois $\mathbb{L} = \mathbb{K}(\alpha) \subseteq \mathcal{F}(H)(\alpha) \subseteq \mathbb{L}$. De $f \in \mathcal{F}(H)[x]$ e $f(\alpha) = 0$, obtemos $[\mathbb{L} : \mathcal{F}(H)] = [\mathcal{F}(H)(\alpha) : \mathcal{F}(H)] \leq \partial(f) = |H|$. Portanto, $[\mathbb{L} : \mathcal{F}(H)] \leq |H|$. ■

Demonstração. Seja $f = \min_{\mathbb{K}}(\alpha)$. Como $\alpha \in \mathbb{L} \setminus \mathbb{K}$, temos que $\partial(f) \geq 2$. Seja $\beta \in \mathbb{K}(R_f)$ com $\beta \neq \alpha$. Temos que $\mathbb{L}|\mathbb{K}$ é uma extensão normal, portanto $\beta \in \mathbb{L}$. Agora, pelos Teoremas 19 e 20, existe um isomorfismo $\sigma : \mathbb{L} \rightarrow \mathbb{L}$ tal que $\sigma(\alpha) = \beta$ e $\sigma|_{\mathbb{K}} = \text{id}_{\mathbb{K}}$. Portanto, $\sigma \in \text{Gal}(\mathbb{L}|\mathbb{K})$ e $\sigma(\alpha) = \beta \neq \alpha$. ■

2.6 Norma, traço e discriminante

Definição 41. Sejam $\mathbb{K} \subseteq \mathbb{L}$ corpos de números, com $n = [\mathbb{L} : \mathbb{K}]$, e $\sigma_1, \dots, \sigma_n$ os monomorfismos de \mathbb{L} em \mathbb{C} . Dado um elemento $\alpha \in \mathbb{L}$, define-se a norma e o traço de α relativamente à extensão $\mathbb{L}|\mathbb{K}$, como sendo respectivamente:

$$\mathcal{N}_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha);$$

$$\text{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha).$$

Observação 3. Quando não houver dúvida quanto a extensão que contém o elemento α , usaremos $\mathcal{N}(\alpha)$ no lugar de $\mathcal{N}_{\mathbb{L}/\mathbb{K}}(\alpha)$

Definição 42. O discriminante de \mathbb{K} é definido por:

$$\Delta(\mathbb{K}) = \det(\text{Tr}_{\mathbb{K}}(\theta_i \theta_j))_{i,j=1}^n = \det(B^t B) = \det(B)^2,$$

onde

$$B = \det \begin{pmatrix} \sigma_1(\theta_1) & \sigma_1(\theta_2) & \cdots & \sigma_1(\theta_n) \\ \sigma_2(\theta_1) & \sigma_2(\theta_2) & \cdots & \sigma_2(\theta_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\theta_1) & \sigma_n(\theta_2) & \cdots & \sigma_n(\theta_n) \end{pmatrix},$$

onde $\{\theta_1, \theta_2, \dots, \theta_n\}$ é uma base integral de \mathbb{K} .

Definição 43. Seja $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ um polinômio sobre \mathbb{R} com $a_n \neq 0$. Sejam $\theta_1, \theta_2, \dots, \theta_n$ as raízes de $p(x)$ em \mathbb{C} . O discriminante de $p(x)$ é definido por

$$\Delta(p) = a_n^{2n-2} \sum_{\substack{i,j=1 \\ i < j}}^n (\theta_i - \theta_j)^2.$$

Definição 44. O discriminante de um elemento $\theta \in \mathbb{K}$ é definido por

$$\Delta(\theta) = \Delta(\mathbb{Z}[\theta]) = \Delta(p) = \prod_{1 \leq i < j \leq n} (\sigma_i(\theta) - \sigma_j(\theta))^2,$$

onde $p(x) \in \mathbb{Q}[x]$ é o polinômio minimal de θ .

Como $\Delta(p) = a_n^{2n-2} \delta^2$, onde

$$\delta = \det(A) = \prod_{i < j, i,j=1}^n (\theta_i - \theta_j), \text{ para } i \neq j,$$

com

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \theta_1 & \theta_2 & \cdots & \theta_n \\ \vdots & \vdots & \ddots & \vdots \\ \theta_1^{n-1} & \theta_2^{n-1} & \cdots & \theta_n^{n-1} \end{pmatrix},$$

segue que

$$\det(A)^2 = \det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \theta_1 & \theta_2 & \cdots & \theta_n \\ \vdots & \vdots & \ddots & \vdots \\ \theta_1^{n-1} & \theta_2^{n-1} & \cdots & \theta_n^{n-1} \end{pmatrix} \det \begin{pmatrix} 1 & \theta_1 & \cdots & \theta_1^{n-1} \\ 1 & \theta_2 & \cdots & \theta_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \cdots & \theta_n^{n-1} \end{pmatrix}$$

e

$$\Delta(p) = a_n^{2n-2} \det \begin{pmatrix} n & \cdots & \sum_{i=1}^n \theta_i^{n-1} \\ \sum_{i=1}^n \theta_i & \cdots & \sum_{i=1}^n \theta_i^n \\ \vdots & \ddots & \vdots \\ \sum_{i=1}^n \theta_i^{n-1} & \cdots & \sum_{i=1}^n \theta_i^{2n-2} \end{pmatrix}.$$

Portanto,

$$\Delta(\theta) = \det \begin{pmatrix} \text{Tr}_{\mathbb{K}}(1) & \text{Tr}_{\mathbb{K}}(\theta) & \text{Tr}_{\mathbb{K}}(\theta^2) & \text{Tr}_{\mathbb{K}}(\theta^3) \\ \text{Tr}_{\mathbb{K}}(\theta) & \text{Tr}_{\mathbb{K}}(\theta^2) & \text{Tr}_{\mathbb{K}}(\theta^3) & \text{Tr}_{\mathbb{K}}(\theta^4) \\ \text{Tr}_{\mathbb{K}}(\theta^2) & \text{Tr}_{\mathbb{K}}(\theta^3) & \text{Tr}_{\mathbb{K}}(\theta^4) & \text{Tr}_{\mathbb{K}}(\theta^5) \\ \text{Tr}_{\mathbb{K}}(\theta^3) & \text{Tr}_{\mathbb{K}}(\theta^4) & \text{Tr}_{\mathbb{K}}(\theta^5) & \text{Tr}_{\mathbb{K}}(\theta^6) \end{pmatrix}.$$

2.7 Corpos Quadráticos

Definição 45. Um corpo quadrático é um corpo de números \mathbb{L} de grau 2 sobre \mathbb{Q} . Mais especificamente, $\mathbb{L} = \mathbb{Q}(\theta)$, onde θ é um inteiro algébrico, e θ é um zero de um polinômio $x^2 + ax + b$, com $a, b \in \mathbb{Z}$.

Proposição 13. [1] Os corpos quadráticos são precisamente aqueles da forma $\mathbb{Q}(\sqrt{d})$, para d um inteiro livre de quadrados.

Exemplo 7. O corpo $\mathbb{L} = \mathbb{Q}(\sqrt{13})$ é um corpo quadrático, pois $\theta = \sqrt{13}$ é um zero do polinômio $f(x) = x^2 - 13$.

Teorema 21. [1] Se $\mathbb{L} = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados, então o anel dos inteiros algébricos de \mathbb{L} , (veja definição em [32]) é dado por:

1. $\mathbb{Z}[\sqrt{d}]$, se $d \not\equiv 1 \pmod{4}$,
2. $\mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{d}\right]$, se $d \equiv 1 \pmod{4}$.

Assim, os inteiros algébricos em corpos quadráticos $\mathbb{Q}(\sqrt{d})$ apresentam comportamentos distintos conforme o valor de d módulo 4. Veja o seguinte exemplo:

Exemplo 8. Para $d = 2$, onde $2 \not\equiv 1 \pmod{4}$, os inteiros algébricos são da forma $a + b\sqrt{2}$ com $a, b \in \mathbb{Z}$. Por exemplo, $1 + 3\sqrt{2}$ tem polinômio minimal $x^2 - 2x - 17 \in \mathbb{Z}[x]$. Para $d = 5$, onde $5 \equiv 1 \pmod{4}$, os inteiros algébricos são da forma $\frac{a+b\sqrt{5}}{2}$ com $a \equiv b \pmod{2}$. O elemento $\theta = \frac{1+\sqrt{5}}{2}$, com polinômio minimal $x^2 - x - 1$, é um exemplo válido, assim como $\frac{3+\sqrt{5}}{2}$, enquanto $\frac{1+2\sqrt{5}}{2}$ não é inteiro algébrico.

Teorema 22. [1] Seja $\mathbb{Q}(\sqrt{d})$ um corpo quadrático, onde d é um inteiro livre de quadrados.

- (a) Se $d \not\equiv 1 \pmod{4}$, então o corpo $\mathbb{Q}(\sqrt{d})$ tem uma base integral, da forma $\{1, \sqrt{d}\}$ e discriminante $4d$.
- (b) Se $d \equiv 1 \pmod{4}$, então o corpo $\mathbb{Q}(\sqrt{d})$ tem uma base integral da forma $\left\{1, \frac{1}{2} + \frac{1}{2}\sqrt{d}\right\}$ e discriminante d .

Exemplo 9. Seja o corpo quadrático $\mathbb{Q}(\sqrt{d})$.

Supondo $d = 2 \not\equiv 1 \pmod{4}$. Sua base integral é $\{1, \sqrt{2}\}$.

Calculando o discriminante Δ , temos

$$\begin{aligned}\Delta &= \det \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\sqrt{2}) & \sigma_2(\sqrt{2}) \end{pmatrix}^2 = \det \begin{pmatrix} 1 & 1 \\ \sqrt{2} & -\sqrt{2} \end{pmatrix}^2 \\ &= \left[1 \cdot (-\sqrt{2}) - 1 \cdot \sqrt{2}\right]^2 = (-2\sqrt{2})^2 = 8 = 4d.\end{aligned}$$

Agora, supondo $d = 5 \equiv 1 \pmod{4}$. Sua base integral é $\{1, \omega\}$ onde $\omega = \frac{1}{2} + \frac{1}{2}\sqrt{5}$

Cálculo do discriminante Δ :

$$\begin{aligned}\Delta &= \det \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\omega) & \sigma_2(\omega) \end{pmatrix}^2 = \det \begin{pmatrix} 1 & 1 \\ \frac{1}{2} + \frac{1}{2}\sqrt{5} & \frac{1}{2} - \frac{1}{2}\sqrt{5} \end{pmatrix}^2 \\ &= \left[1 \cdot \left(\frac{1}{2} - \frac{1}{2}\sqrt{5}\right) - 1 \cdot \left(\frac{1}{2} + \frac{1}{2}\sqrt{5}\right)\right]^2 \\ &= \left(-\sqrt{5}\right)^2 = 5 = d.\end{aligned}$$

Portanto, para $d = 2$, obtemos $\Delta = 8 = 4d$ e para $d = 5$, obtemos $\Delta = 5 = d$ conforme o Teorema [22](#).

Exemplo 10. Consideremos o corpo quadrático $\mathbb{L} = \mathbb{Q}(\sqrt{2})$. Tome a base \mathbb{Q} -linear $\{1, \sqrt{2}\}$ de \mathbb{L} . Para calcular o discriminante $D(1, \sqrt{2})$ segundo a proposição, começamos construindo a matriz de traços $(\text{Tr}(\alpha_i \alpha_j))_{i,j}$, onde $\text{Tr} = \text{Tr}_{\mathbb{L}/\mathbb{Q}}$.

O elemento $1 \cdot 1 = 1$ tem traço 2, pois ambos seus \mathbb{Q} -conjugados são iguais a 1. O produto $1 \cdot \sqrt{2} = \sqrt{2}$ possui traço zero, já que seus conjugados $\sqrt{2}$ e $-\sqrt{2}$ se cancelam. Analogamente, $\sqrt{2} \cdot \sqrt{2} = 2$ tem traço 4, sendo 2 invariante pelos automorfismos de \mathbb{L} .

Assim, obtemos a matriz diagonal:

$$\begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}$$

cujos determinantes são 8. Portanto, o discriminante da base $\{1, \sqrt{2}\}$ em $\mathbb{Q}(\sqrt{2})$ é $D(1, \sqrt{2}) = 8$, um inteiro não quadrado que preserva propriedades fundamentais desta extensão quadrática.

Observação 4. Considerando $\mathbb{K} = \mathbb{Q}(\sqrt{m}, \sqrt{n})$, temos que $\{1, \theta, \theta^2, \theta^3\}$, onde $\theta = \sqrt{m} + \sqrt{n}$, é uma base de \mathbb{K} sobre \mathbb{Q} como espaço vetorial. Nosso objetivo agora é calcular o discriminante de $\mathbb{Z}[\theta]$, que será útil no capítulo final do nosso trabalho.

2.8 Corpos Biquadráticos

Corpos biquadráticos são extensões de grau 4 sobre \mathbb{Q} . Os corpos biquadráticos desempenham um papel central dentro deste trabalho.

Definição 46. [9] *Seja \mathbb{Q} o corpo dos números racionais. Se m, n são inteiros distintos, livres de quadrados, o corpo formado pela adjunção de \sqrt{m} e \sqrt{n} a \mathbb{Q} denotado por $\mathbb{Q}(\sqrt{m}, \sqrt{n})$, é chamado de corpo biquadrático.*

Proposição 14. [9] $\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m} + \sqrt{n})$, e $\sqrt{m} + \sqrt{n}$ possui como polinômio minimal $x^4 - 2(m+n)x^2 + (m-n)^2$.

Demonstração. Sejam m e n inteiros distintos e livres de quadrados, e considere a extensão $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ sobre \mathbb{Q} . Sejam $\alpha = \sqrt{m}$ e $\beta = \sqrt{n}$, cujos polinômios mínimos sobre \mathbb{Q} são respectivamente $p(x) = x^2 - m = (x - \sqrt{m})(x + \sqrt{m})$ e $q(x) = x^2 - n = (x - \sqrt{n})(x + \sqrt{n})$.

Pelo Teorema do Elemento Primitivo, sabemos que existe $u \in \mathbb{Q}(\sqrt{m}, \sqrt{n})$ tal que $\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(u)$. Para construir explicitamente tal elemento, consideramos as raízes $\alpha_1 = \sqrt{m}$, $\alpha_2 = -\sqrt{m}$ de $p(x)$ e $\beta_1 = \sqrt{n}$, $\beta_2 = -\sqrt{n}$ de $q(x)$. Calculamos os valores:

$$\lambda_{12} = \frac{\alpha_1 - \alpha}{\beta - \beta_2} = \frac{\sqrt{m} - \sqrt{m}}{\sqrt{n} - (-\sqrt{n})} = 0$$

$$\lambda_{22} = \frac{\alpha_2 - \alpha}{\beta - \beta_2} = \frac{-\sqrt{m} - \sqrt{m}}{2\sqrt{n}} = -\frac{\sqrt{m}}{\sqrt{n}}$$

Como \mathbb{Q} é infinito e $-\frac{\sqrt{m}}{\sqrt{n}} \notin \mathbb{Q}$ (pois \sqrt{mn} é irracional quando m e n são livres de quadrados distintos), podemos escolher $\lambda = 1$, obtendo assim o elemento primitivo $u = \sqrt{m} + \sqrt{n}$.

Para verificar que $\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(u)$, observamos primeiramente que a inclusão $\mathbb{Q}(u) \subset \mathbb{Q}(\sqrt{m}, \sqrt{n})$ é válida, pois $u = \sqrt{m} + \sqrt{n} \in \mathbb{Q}(\sqrt{m}, \sqrt{n})$. Para a inclusão inversa, notamos que:

$$u^2 = m + n + 2\sqrt{mn} \implies \sqrt{mn} = \frac{u^2 - m - n}{2} \in \mathbb{Q}(u)$$

Além disso, da identidade $(\sqrt{m} + \sqrt{n})(\sqrt{m} - \sqrt{n}) = m - n$, obtemos:

$$\sqrt{m} - \sqrt{n} = \frac{m - n}{u} \in \mathbb{Q}(u)$$

Resolvendo o sistema linear:

$$\begin{cases} \sqrt{m} + \sqrt{n} = u \\ \sqrt{m} - \sqrt{n} = \frac{m-n}{u} \end{cases}$$

encontramos expressões racionais em u para ambos os geradores:

$$\sqrt{m} = \frac{u + \frac{m-n}{u}}{2} \quad \text{e} \quad \sqrt{n} = \frac{u - \frac{m-n}{u}}{2}$$

o que mostra que $\sqrt{m}, \sqrt{n} \in \mathbb{Q}(u)$. ■

Neste trabalho assumimos m e n como inteiros estritamente positivos, onde $l = \text{mdc}(m, n)$ representa seu máximo divisor comum. Sendo assim, podemos escrever $m = lm_1$ e $n = ln_1$, com m_1 e n_1 inteiros coprimos.

Teorema 23. [9] *Uma base integral para $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ é dada por:*

- (i) $\left\{1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m_1n_1}}{4}\right\}$ se $(m, n) \equiv (1, 1), (m_1, n_1) \equiv (1, 1) \pmod{4}$,
- (ii) $\left\{1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1-\sqrt{m}+\sqrt{n}+\sqrt{m_1n_1}}{4}\right\}$ se $(m, n) \equiv (1, 1), (m_1, n_1) \equiv (3, 3) \pmod{4}$,
- (iii) $\left\{1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{m_1n_1}}{4}\right\}$ se $(m, n) \equiv (1, 2) \pmod{4}$,
- (iv) $\left\{1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{m}+\sqrt{m_1n_1}}{2}\right\}$ se $(m, n) \equiv (2, 3) \pmod{4}$,
- (v) $\left\{1, \sqrt{m}, \frac{\sqrt{m}+\sqrt{n}}{2}, \frac{1+\sqrt{m_1n_1}}{2}\right\}$ se $(m, n) \equiv (3, 3) \pmod{4}$.

Exemplo 11. [9] Uma base integral para $\mathbb{Q}(\sqrt{5}, \sqrt{13})$ é

$$\{\alpha_0, \alpha_1, \alpha_2, \alpha_3\} = \left\{1, \frac{1+\sqrt{5}}{2}, \frac{1+\sqrt{13}}{2}, \frac{1+\sqrt{5}+\sqrt{13}+\sqrt{65}}{4}\right\}$$

e o inteiro $\frac{1}{4}(5 + 3\sqrt{5} + \sqrt{13} + 3\sqrt{65})$ é expresso em termos desta base integral como $\alpha_0 - \alpha_2 + 3\alpha_3$.

Teorema 24. [9] O discriminante de $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ é dado por:

- (i) $l^2m_1^2n_1^2$, se $(m, n) \equiv (1, 1) \pmod{4}$,
- (ii) $16l^2m_1^2n_1^2$, se $(m, n) \equiv (1, 2)$ ou $(3, 3) \pmod{4}$,
- (iii) $64l^2m_1^2n_1^2$, se $(m, n) \equiv (2, 3) \pmod{4}$.

Observação 5. Considerando $\mathbb{K} = \mathbb{Q}(\sqrt{m}, \sqrt{n})$, temos que $\{1, \theta, \theta^2, \theta^3\}$, onde $\theta = \sqrt{m} + \sqrt{n}$, é uma base de \mathbb{K} sobre \mathbb{Q} como espaço vetorial. Nosso objetivo agora é calcular o discriminante de $\mathbb{Z}[\theta]$, que será útil no capítulo final do trabalho.

Assim,

$$\begin{cases} \theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_4^2 = 4m + 4n, \\ \theta_1^2\theta_2^2 + \theta_1^2\theta_3^2 + \theta_1^2\theta_4^2 + \theta_2^2\theta_3^2 + \theta_2^2\theta_4^2 + \theta_3^2\theta_4^2 = 6m^2 + 4mn + 6n^2 \\ \theta_1^2\theta_2^2\theta_3^2 + \theta_1^2\theta_2^2\theta_4^2 + \theta_1^2\theta_3^2\theta_4^2 + \theta_2^2\theta_3^2\theta_4^2 = 4m^3 - 4m^2n - 4mn^2 + 4n^3 \\ \theta_1^2\theta_2^2\theta_3^2\theta_4^2 = (m-n)^4 \\ \theta_1^3 + \theta_2^3 + \theta_3^3 + \theta_4^3 = 0 \\ \theta_1^4 + \theta_2^4 + \theta_3^4 + \theta_4^4 = 4m^2 + 24mn + 4n^2 \\ \theta_1^5 + \theta_2^5 + \theta_3^5 + \theta_4^5 = 0 \\ \theta_1^6 + \theta_2^6 + \theta_3^6 + \theta_4^6 = 4m^3 + 60m^2n + 60mn^2 + 4n^3. \end{cases} \quad (2.1)$$

onde $\theta_1, \theta_2, \theta_3$ e θ_4 são as raízes do polinômio minimal de θ sobre \mathbb{Q} .

Da equação correspondente, segue que:

$$\Delta(\mathbb{Z}[\theta]) = (2^6mn(m-n))^2.$$

Introdução aos reticulados

Neste capítulo, examinamos a teoria dos reticulados, focando em suas definições e propriedades fundamentais. Apresentamos conceitos relacionados ao empacotamento esférico e discutimos os principais reticulados conhecidos na literatura, oferecendo uma visão geral que fundamenta as investigações subsequentes. Neste capítulo foram usadas as referências [1] e [2].

3.1 Reticulado

Definição 47. *Seja $\{v_1, v_2, \dots, v_m\}$ um conjunto de vetores linearmente independentes sobre \mathbb{R} no espaço vetorial \mathbb{R}^n , tal que $m \leq n$. O conjunto*

$$\Lambda = \left\{ \sum_{i=1}^m \alpha_i v_i : \alpha_i \in \mathbb{Z} \right\}$$

é chamado um reticulado de posto m , e o conjunto $\{v_1, v_2, \dots, v_m\}$ é chamado uma base do reticulado Λ .

Exemplo 12. *O reticulado $\Lambda_1 = \{\alpha_1(-1, 1, 0) + \alpha_2(0, -1, 1); \alpha_1, \alpha_2 \in \mathbb{Z}\}$ e o reticulado $\Lambda_2 = \{\alpha_1(1, 0, 0) + \alpha_2(0, 1, 0) + \alpha_3(0, 0, 1); \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}\}$.*

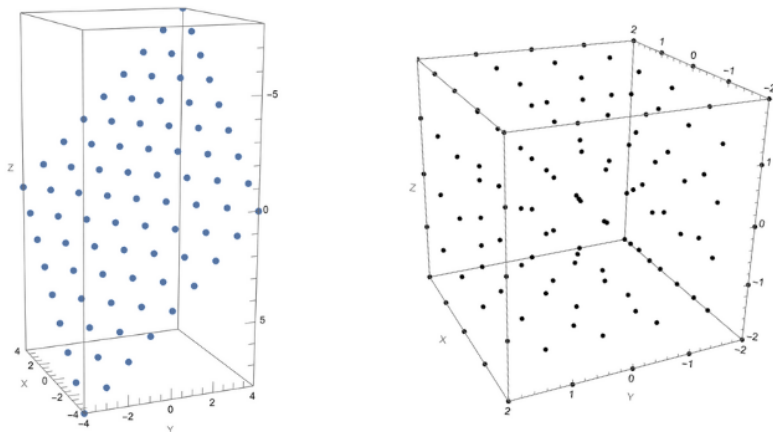


Figura 3.1: Reticulados Λ_1 e Λ_2 .

Definição 48. Chamamos de posto de um reticulado Λ o número de vetores de uma base de Λ , isto é, a dimensão do subespaço gerado por Λ em \mathbb{R}^n .

Definição 49. Seja $\Lambda \subseteq \mathbb{R}^n$ um reticulado com base $B = \{v_1, v_2, \dots, v_m\}$. O conjunto

$$\mathcal{P}_B = \left\{ x \in \mathbb{R}^n : x = \sum_{i=1}^n \lambda_i v_i, 0 \leq \lambda_i < 1 \right\}$$

é chamado de paralelepípedo fundamental ou região fundamental de Λ com relação à base B .

Exemplo 13. Tomando $v_1 = (1, 0, 0)$, $v_2 = (0, 1, 0)$ e $v_3 = (0, 0, 1)$, temos

$$\Lambda = \{ \alpha_1(1, 0, 0) + \alpha_2(0, 1, 0) + \alpha_3(0, 0, 1), \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z} \} = \mathbb{Z}^3$$

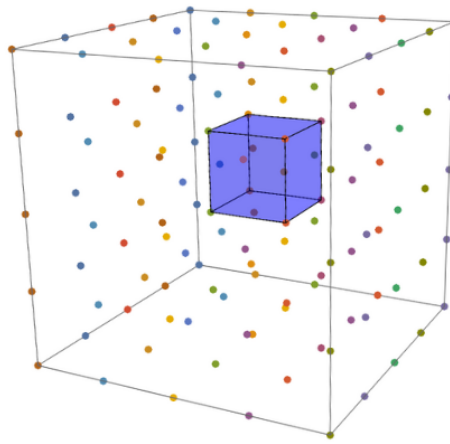


Figura 3.2: Região fundamental.

Definição 50. Seja $\{v_1, v_2, \dots, v_m\}$ uma base para o reticulado Λ tal que $v_i = (v_{i1}, \dots, v_{in})$, para $i = 1, \dots, m$. A matriz $M = (v_{ij})$ é chamada uma matriz geradora para o reticulado Λ , ou seja,

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

Assim, Λ pode ser escrito na forma matricial como:

$$\Lambda = \{ xM \mid x \in \mathbb{Z}^m \}.$$

Proposição 15. Duas matrizes M_1 e M_2 geram o mesmo reticulado se, e somente se, $M_1 = AM_2$, na qual A é uma matriz com elementos inteiros e determinante ± 1 . A matriz A é chamada mudança de base.

Exemplo 14. Faremos a demonstração para um reticulado de dimensão 3. Sejam $B = \{u_1, u_2, u_3\}$ e $C = \{v_1, v_2, v_3\}$ duas bases distintas de um reticulado Λ , então cada vetor de B é escrito como combinação linear inteira dos vetores da base C , isto é:

$$\begin{cases} u_1 = \alpha_{11}v_1 + \alpha_{12}v_2 + \alpha_{13}v_3 \\ u_2 = \alpha_{21}v_1 + \alpha_{22}v_2 + \alpha_{23}v_3 \\ u_3 = \alpha_{31}v_1 + \alpha_{32}v_2 + \alpha_{33}v_3 \end{cases} \quad ; \quad \alpha_{ij} \in \mathbb{Z}$$

As equações podem ser escritas na forma matricial:

$$\begin{pmatrix} u_{11} & u_{12} & u_{13} \\ u_{21} & u_{22} & u_{23} \\ u_{31} & u_{32} & u_{33} \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix} \begin{pmatrix} v_{11} & v_{12} & v_{13} \\ v_{21} & v_{22} & v_{23} \\ v_{31} & v_{32} & v_{33} \end{pmatrix}; \quad A = (\alpha_{ij}) \in M_3(\mathbb{Z})$$

Para expressar os vetores de C como combinação linear de B , teríamos:

$$A^{-1}B = A^{-1}AC \Rightarrow C = A^{-1}B$$

Logo, A^{-1} também teria entradas inteiras, como B e C são bases do mesmo reticulado, Se $B = AC$ com A de entradas inteiras, então $C = A^{-1}B$ também deve ter coeficientes inteiros. Isso só é possível se A^{-1} for inteira, o que exige $\det(A) = \pm 1$.

Reciprocamente, seja C uma base do reticulado Λ , logo C é um conjunto linearmente independente, logo $\det(C) \neq 0$. Assim,

$$\det(B) = \det(AC) = \det(A)\det(C) \neq 0$$

Portanto, B é um conjunto linearmente independente. Basta mostrar que B e C geram o mesmo conjunto.

Sejam $L(B) = \{\sum_{j=1}^3 \gamma_j u_j, \gamma_j \in \mathbb{Z}\}$ e $\Lambda = L(C) = \{\sum_{j=1}^3 \gamma_j v_j, \gamma_j \in \mathbb{Z}\}$. Dado $\omega \in L(C)$, então $\omega = \gamma_1 v_1 + \gamma_2 v_2 + \gamma_3 v_3$, logo como $C = A^{-1}B$, $A^{-1} \in M_3(\mathbb{Z})$, então cada $v_j \in C$ pode ser escrito como combinação linear inteira dos vetores, assim $C \subseteq L(B)$ e consequentemente $L(C) \subseteq L(B)$.

Analogamente, dado $\omega \in L(C)$, então $\omega = \gamma_1 u_1 + \gamma_2 u_2 + \gamma_3 u_3$ e como $B = AC$, $A \in M_3(\mathbb{Z})$, então cada $u_j \in B$ pode ser escrito como combinação linear inteira dos vetores de C , assim $B \subseteq L(C)$ e consequentemente $L(B) \subseteq L(C)$.

Portanto, os conjuntos B e C são linearmente independentes e geram o mesmo reticulado, ou seja, B e C são bases do mesmo reticulado.

Definição 51. Seja M uma matriz geradora para o reticulado Λ . A matriz $G = MM^t$ é chamada de matriz de Gram para o reticulado e M^t representa a transposta de M .

Observação 6. Considerando que a matriz geradora M contém os vetores $\{v_1, v_2, \dots, v_n\}$, que constituem a base do reticulado, a entrada na posição (i, j) da matriz de Gram G é dada pelo produto interno $\langle v_i, v_j \rangle$. Portanto, os elementos da matriz G armazenam informações métricas importantes, uma vez que estão associados às posições relativas dos vetores que formam a base do reticulado.

Definição 52. O determinante de um reticulado Λ é definido como o determinante da matriz de Gram de Λ , ou seja, $\det(\Lambda) = \det(G)$

Definição 53. O volume do reticulado Λ é definido por $\text{Vol}(\Lambda) = \sqrt{\det(\Lambda)}$. Esse é o volume da região fundamental do reticulado Λ .

Exemplo 15. Considere um reticulado em \mathbb{R}^2 gerado pelos vetores:

$$\mathbf{v}_1 = \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \quad \mathbf{v}_2 = \begin{pmatrix} 1 \\ 3 \end{pmatrix}.$$

Calculando a matriz de Gram G tem-se:

$$G = \begin{pmatrix} 4 & 2 \\ 2 & 10 \end{pmatrix}$$

e o determinante de G é dado por

$$\det(G) = 36$$

logo, o volume do reticulado Λ é:

$$\text{Vol}(\Lambda) = \sqrt{36} = 6$$

Definição 54. *Seja B uma matriz de ordem $m, m \leq n$, com entradas inteiras, um sub-reticulado Λ' de Λ possui matriz geradora $M' = BM$, onde M é a matriz geradora do reticulado Λ .*

Definição 55. *Dois reticulados são considerados equivalentes na métrica euclidiana se um deles puder ser obtido do outro através de uma combinação de rotação ou reflexão, juntamente com uma multiplicação por um fator de escala.*

Em outras palavras, os reticulados Λ_1 e Λ_2 , com matrizes geradoras M_1 e M_2 , são equivalentes se, e somente se, $M_1 = cAM_2R$, onde A é uma matriz de mudança de base (com entradas inteiras e determinante ± 1), R é uma matriz ortogonal, e \sqrt{c} é o fator de escala.

3.2 Empacotamento esférico

Um empacotamento esférico é uma distribuição de esferas de mesmo raio no espaço euclidiano n -dimensional de forma que a interseção de quaisquer duas esferas tenha no máximo um ponto. Pode-se descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio. Denotaremos $B_r[x]$ como sendo a bola fechada de raio r centrada em $x \in \mathbb{R}^n$ e $B_r(x)$ representando a bola aberta de raio r centrada em $x \in \mathbb{R}^n$.

Definição 56. *Um empacotamento reticulado é um empacotamento no \mathbb{R}^n tal que o conjunto dos centros das esferas formam um reticulado $\Lambda \subset \mathbb{R}^n$.*

Definição 57. *O raio de empacotamento de um reticulado Λ é definido como o maior raio ρ tal que as bolas $B_\rho(u)$ e $B_\rho(v)$ não se intersectam para quaisquer $u, v \in \Lambda$ onde $u \neq v$.*

Uma definição relevante relacionada ao raio de empacotamento é a norma mínima de um vetor não nulo do reticulado, que corresponde à distância mínima entre dois pontos distintos desse reticulado.

Definição 58. *A norma mínima η de um reticulado Λ é definida por*

$$\eta = \min\{\|x\|^2 : x \in \Lambda, x \neq 0.\}$$

Assim, a norma mínima é igual ao quadrado da menor distância entre dois pontos do reticulado, estabelecendo o raio de empacotamento como a metade da raiz quadrada da norma mínima, ou seja, $\rho = \frac{\sqrt{\eta}}{2}$.

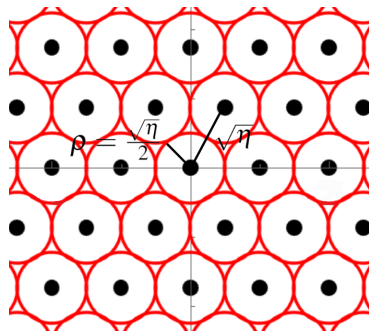


Figura 3.3: Região fundamental.

Definição 59. *O conjunto dos vetores mínimos de Λ é dada por $S(\Lambda) = \{x \in \Lambda : \|x\|^2 = \eta\}$.*

Outro parâmetro relevante associado aos empacotamentos, particularmente no contexto do empacotamento reticulado, é sua densidade, a qual será definida a seguir.

Definição 60. Dado um empacotamento no \mathbb{R}^n associado ao reticulado Λ com base $\{v_1, v_2, \dots, v_n\}$ e raio de empacotamento ρ , a densidade de empacotamento de Λ é dada por:

$$\Delta(\Lambda) = \frac{\text{Vol}(B(\rho))}{\text{Vol}(\Lambda)}$$

em que $B(\rho)$ denota a esfera de centro na origem e raio ρ na dimensão n e $\text{Vol}(\Lambda) = \sqrt{\det(\Lambda)}$ é o volume da região fundamental do reticulado Λ .

Podemos simplificar $\text{Vol}(B(\rho)) = \text{Vol}(B(1))\rho^n$, tal que $B(1)$ denota a esfera de raio 1 centrada na origem. Assim, a densidade de empacotamento é dada por

$$\frac{\text{Vol}(B(1))\rho^n}{\text{Vol}(\Lambda)}.$$

Ao investigar a densidade de empacotamento, uma das questões centrais é encontrar reticulados que possuam alta densidade e, ao mesmo tempo, manipuláveis. Deste modo, podemos reduzir o problema ao estudo de um outro parâmetro, chamado densidade de centro, dado por

$$\delta(\Lambda) = \frac{\rho^n}{\text{Vol}(\Lambda)},$$

e, portanto, a densidade de empacotamento de Λ é $\Delta(\Lambda) = \text{Vol}(B(1))\delta(\Lambda)$.

Exemplo 16. Considere os reticulados Λ_1 e Λ_2 com as respectivas bases. $\beta = \{(1, 0), (1, \frac{\sqrt{3}}{2})\}$ e $\beta' = \{(1, 0), (0, 1)\}$, os quais são representados pelas figuras.

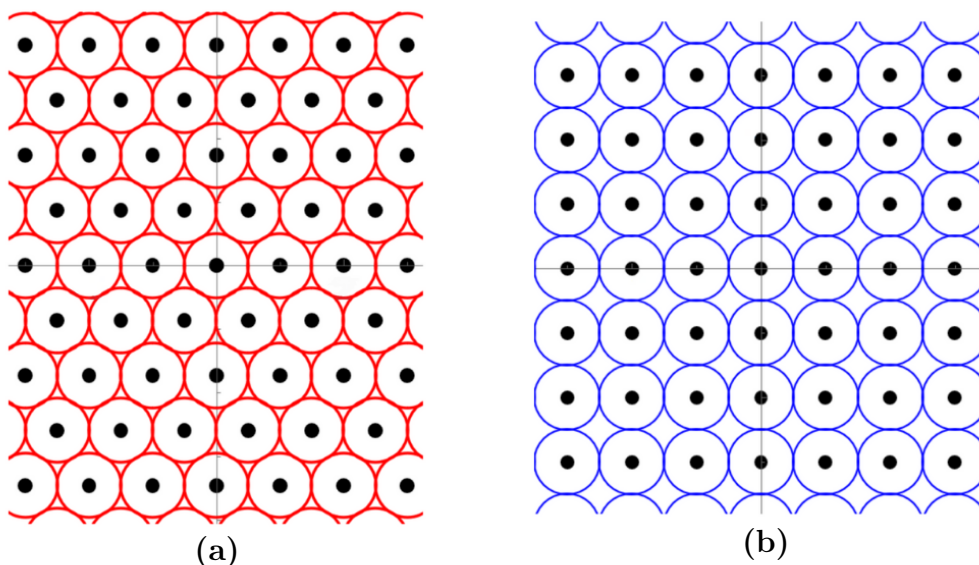


Figura 3.4: (a) $\Delta(\Lambda_1) = \frac{\pi\sqrt{3}}{6} \approx 0,9069$ e (b) $\Delta(\Lambda_2) = \frac{\pi}{4} \approx 0,7854$.

Definição 61. Considere um conjunto de esferas com raio R , centradas nos pontos do reticulado Λ , cobrindo todo o espaço \mathbb{R}^n . A densidade de cobertura Θ é dada por:

$$\Theta = \frac{\text{Volume da esfera de raio } R}{\text{Volume do reticulado } \Lambda} = \frac{\text{Vol}(B(R))}{\text{Vol}(\Lambda)} = \frac{\text{Vol}(B(1))R^n}{\text{Vol}(\Lambda)}$$

onde R é o raio de cobertura.

O objetivo do empacotamento esférico é encontrar os empacotamentos mais densos formados por esferas abertas que não se tocam, enquanto a cobertura visa identificar os empacotamentos menos densos, compostos por esferas que cobrem todo o espaço. Em um reticulado, a densidade de cobertura é determinada pelas esferas de menor raio que, quando centralizadas nos pontos do reticulado, cobrem todo o espaço. As densidades de empacotamento e de cobertura obedecem à relação:

$$\Delta \leq 1 \leq \Theta.$$

Isso significa que o volume de uma esfera com raio de empacotamento ρ é sempre menor ou igual ao determinante do reticulado, enquanto o volume de uma esfera com raio de cobertura R é sempre maior ou igual ao determinante do reticulado.

Outro parâmetro relevante a ser considerado é o número de vizinhos de um empacotamento esférico, que será definido a seguir.

Definição 62. *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado. Para cada $x \in \Lambda$, o número de vetores $y \in \Lambda$ tais que $x \neq y$ e $\|x - y\|$ seja mínima, que denotaremos por $\tau(x)$, é chamado de número de vizinhos de x .*

Teorema 25. *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado. Dados $x, y \in \Lambda$, o número de vizinhos de x é igual ao número de vizinhos de y .*

O teorema afirma que, para determinar a quantidade de vetores que são vizinhos de um elemento x em um reticulado Λ , é necessário considerar os elementos que são vizinhos da origem. Esses são os vetores do reticulado que têm a menor norma. Além disso, se w_1, \dots, w_k são esses vetores de menor norma, então $x + w_1, \dots, x + w_k$ são os vizinhos de x . Em resumo, adicionamos os vetores de menor norma a x para encontrar todos os seus vizinhos.

Definição 63. *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado. O número $\tau(0)$ é chamado de número de vizinhos ou kissing number de Λ , ou seja, é a quantidade de vetores de distância mínima do reticulado.*

Exemplo 17. *Podemos observar na figura a seguir que o reticulado Λ_1 possui kissing number 6 e o reticulado Λ_2 possui kissing number 4 na métrica euclidiana.*

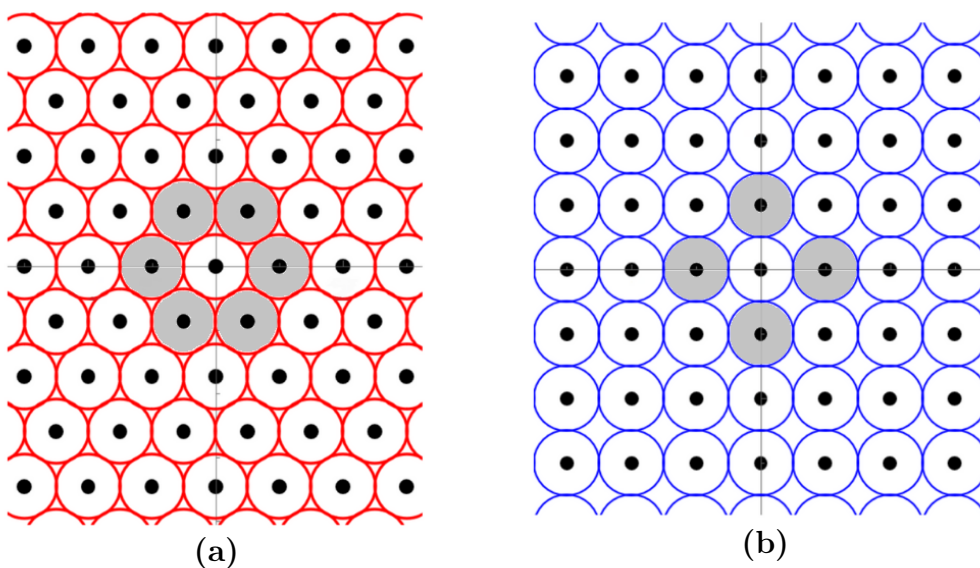


Figura 3.5: Kissing number. (a) Λ_1 e (b) Λ_2

3.3 Principais reticulados conhecidos na literatura

Nesta seção, apresentamos alguns dos reticulados mais conhecidos e utilizados na literatura.

Definição 64 (Reticulado \mathbb{Z}^n). *Definido por*

$$\mathbb{Z}^n = \{(x_1, x_2, \dots, x_n); x_i \in \mathbb{Z}\}, n \geq 2$$

é um reticulado n -dimensional e possui a matriz identidade de ordem n como uma matriz geradora $M = I_n$.

Propriedades: $\det(\mathbb{Z}^n) = 1$, norma mínima $\eta = 1$, raio de empacotamento $\rho = \frac{1}{2}$, densidade de centro $\delta = \frac{1}{2^n}$, densidade de empacotamento

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

raio de cobertura $R = \sqrt{n}/2$, e kissing number $\tau = 2n$.

Definição 65 (Reticulado A_n). *Definido por*

$$A_n = \{(x_0, x_1, \dots, x_n) \in \mathbb{Z}^{n+1}; x_0 + x_1 + \dots + x_n = 0\}, n \geq 2$$

é um reticulado n -dimensional em \mathbb{R}^{n+1} e possui uma matriz geradora,

$$M = \begin{pmatrix} -1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & -1 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & -1 & 1 \end{pmatrix}.$$

Propriedades: $\det(A_n) = n + 1$, norma mínima $\eta = 2$, raio de empacotamento, $\rho = \sqrt{2}/2$, densidade de centro $\delta = \frac{2^{-n/2}}{\sqrt{n+1}}$, kissing number $\tau = n(n + 1)$, densidade de empacotamento

$$\Delta = \begin{cases} \frac{\pi^{n/2} 2^{-n/2}}{(\frac{n}{2})! \sqrt{n+1}}, & \text{se } n \text{ é par.} \\ \frac{2^n \pi^{(n-1)/2} ((n-1)/2)! 2^{-n/2}}{n! \sqrt{n+1}}, & \text{se } n \text{ é ímpar.} \end{cases}$$

Definição 66 (Reticulado D_n). *Definido por*

$$D_n = \{(x_1, x_2, \dots, x_n) \in \mathbb{Z}^n; x_1 + x_2 + \dots + x_n \text{ é par}\}, n \geq 3$$

Uma matriz geradora é dada por

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

Propriedades: $\det(D_n) = 4$, norma mínima $\eta = 2$, raio de empacotamento $\rho = \frac{\sqrt{2}}{2}$, densidade de centro $\delta = 2^{-\frac{n+2}{2}}$, kissing number $\tau = 2n(n - 1)$ e densidade de empacotamento

$$\Delta = \begin{cases} \frac{\pi^{n/2} 2^{-(n+2)/2}}{(\frac{n}{2})!}, & \text{se } n \text{ é par,} \\ \frac{2^n \pi^{(n-1)/2} ((n-1)/2)! 2^{-(n+2)/2}}{n!}, & \text{se } n \text{ é ímpar.} \end{cases}$$

O reticulado D_n é o mais denso nas dimensões $n = 3, 4$ e 5 .

Definição 67 (Reticulado E_8). O reticulado E_8 é um reticulado de dimensão 8, definido por

$$E_8 = \left\{ (x_1, x_2, \dots, x_8) \in \mathbb{R}^8; \forall x_i, x_i \in \mathbb{Z} \text{ ou } x_i \in \mathbb{Z} + \frac{1}{2}, \sum x_i \equiv 0 \pmod{2} \right\}.$$

Uma de suas matrizes geradoras é dada por

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

Propriedades: $\det(E_8) = 1$, norma mínima $\eta = 2$, raio de empacotamento $\rho = \frac{\sqrt{2}}{2}$, densidade de centro $\delta(E_8) = \frac{1}{16}$, $\tau = 240$ e densidade de empacotamento

$$\Delta(E_8) = \frac{\pi^4}{384}.$$

Esse é o reticulado de maior densidade conhecida no espaço euclidiano \mathbb{R}^8 .

Definição 68 (Reticulado E_7). O reticulado E_7 é um reticulado 7-dimensional, definido por

$$E_7 = \left\{ (x_1, x_2, \dots, x_8) \in E_8; \sum_{i=1}^8 x_i = 0 \right\}.$$

ou seja, E_7 é um reticulado de dimensão 7 no espaço 8-dimensional e mais, é um sub-reticulado de E_8 . Uma das matrizes geradoras de E_7 é dada por

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

Propriedades: $\det(E_7) = 2$, norma mínima $\eta = 2$, raio de empacotamento $\rho = \frac{\sqrt{2}}{2}$, densidade de centro $\delta(E_7) = \frac{1}{16}$, kissing number $\tau = 126$ e

$$\Delta(E_7) = \frac{\pi^3}{105}.$$

Esse reticulado é o de maior densidade conhecida na dimensão 7.

Definição 69 (Reticulado E_6). O reticulado E_6 , também sub-reticulado de E_8 , é um reticulado de dimensão 6 no espaço 8-dimensional, definido por

$$E_6 = \{(x_1, x_2, \dots, x_8) \in E_8; x_1 + x_8 = 0 \text{ e } x_2 + x_3 + x_4 + x_5 + x_6 + x_7 = 0\}.$$

Reticulados via corpos biquadráticos

Neste capítulo, investigamos a construção sistemática de reticulados em \mathbb{R}^n através de \mathbb{Z} -módulos e ideais do anel de inteiros de corpos biquadráticos. Apresentamos um método completo que engloba a caracterização das quatro bases integrais dadas pelo Teorema 23 via homomorfismos canônicos, a redução de Minkowski para estas bases, utilizando o algoritmo apresentado em 8 e uma análise computacional das densidades de centro utilizando Wolfram Mathematica 14.0.

4.1 Construção

Apresentamos um método para a geração de reticulados no \mathbb{R}^n via \mathbb{Z} -módulos e ideais do anel de inteiros de um corpo de números.

Seja \mathbb{K} um corpo de números algébricos de grau n e $\mathcal{O}_{\mathbb{K}}$ seu anel de inteiros algébricos. Existem exatamente n \mathbb{Q} -monomorfismos distintos $\sigma_i : \mathbb{K} \rightarrow \mathbb{C}$, para $i = 1, 2, \dots, n$. Um \mathbb{Q} -monomorfismo σ_i é dito real se $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$ e imaginário caso contrário. Dizemos que \mathbb{K} é totalmente real se σ_i é real para todo $i = 1, 2, \dots, n$ e totalmente imaginário se σ_i é imaginário para todo $i = 1, 2, \dots, n$. Se r_1 é o número de índices tais que $\sigma_i(\mathbb{K}) \subset \mathbb{R}$, então $n - r_1$ é um número par, ou seja, $2r_2$ e vale a relação

$$r_1 + 2r_2 = n.$$

Renumeramos os \mathbb{Q} -monomorfismos $\sigma_1, \sigma_2, \dots, \sigma_n$ de forma que $\sigma_1, \dots, \sigma_{r_1}$ são os \mathbb{Q} -monomorfismos reais e $\sigma_{r_1+2j} = \overline{\sigma_{r_1+j}}$, onde $\overline{\sigma_{r_1+j}}$ é a conjugação complexa de σ_{r_1+j} , para $j = 1, 2, \dots, r_2$.

Definição 73. [1] *Seja $x \in \mathbb{L}$ um elemento. O homomorfismo $\sigma_{\mathbb{L}} : \mathbb{L} \rightarrow \mathbb{R}^n$ definido por*

$$\sigma_{\mathbb{L}}(x) = (\sigma_1(x), \dots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \dots, \Re\sigma_{r_1+2r_2}(x), \Im\sigma_{r_1+2r_2}(x)),$$

é um homomorfismo injetivo de módulos, onde as notações $\Re(x)$ e $\Im(x)$ representam as partes real e imaginária do número complexo x , respectivamente.

Definição 74. *Um reticulado obtido a partir do homomorfismo de $\sigma_{\mathbb{L}}$ associado a um corpo de números \mathbb{L} é chamado de reticulado algébrico.*

Definição 75. *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ um corpo biquadrático, onde m e n são positivos, inteiros e livres de quadrados. O homomorfismo $\sigma : \mathbb{K} \rightarrow \mathbb{R}^4$ que fundamenta nossa construção está associado aos quatro mergulhos canônicos, a saber:*

$$\sigma(x) = (\sigma_1(x), \sigma_2(x), \sigma_3(x), \sigma_4(x)) \tag{4.1}$$

onde cada σ_i corresponde a uma combinação distinta dos automorfismos do corpo:

$$\begin{aligned}\sigma_1 : \sqrt{m} &\mapsto +\sqrt{m}, & \sqrt{n} &\mapsto +\sqrt{n} \\ \sigma_2 : \sqrt{m} &\mapsto +\sqrt{m}, & \sqrt{n} &\mapsto -\sqrt{n} \\ \sigma_3 : \sqrt{m} &\mapsto -\sqrt{m}, & \sqrt{n} &\mapsto +\sqrt{n} \\ \sigma_4 : \sqrt{m} &\mapsto -\sqrt{m}, & \sqrt{n} &\mapsto -\sqrt{n}\end{aligned}\tag{4.2}$$

Proposição 16. [1] *Seja \mathbb{L} um corpo de números de grau n . Se $M \subseteq \mathbb{L}$ é um \mathbb{Z} -módulo livre de posto n e se $(x_j)_{1 \leq j \leq n}$ é uma \mathbb{Z} -base de M , então $\sigma_{\mathbb{L}}(M)$ é um reticulado em \mathbb{R}^n , com volume*

$$\text{Vol}(\sigma_{\mathbb{L}}(M)) = 2^{-r_2} |\det_{1 \leq j, k \leq n} (\sigma_j(x_k))|.$$

Proposição 17. [1] *Seja \mathbb{L} um corpo de números de grau n , $\mathcal{D}_{\mathbb{L}}$ o discriminante de \mathbb{L} , $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros algébricos de \mathbb{L} , A um ideal não nulo de $\mathcal{O}_{\mathbb{L}}$ e r_2 a metade do número de monomorfismos imaginários. Então, $\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}})$ e $\sigma_{\mathbb{L}}(A)$ são reticulados, com respectivos volumes:*

$$\begin{aligned}\text{Vol}(\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}})) &= 2^{-r_2} |\mathcal{D}_{\mathbb{L}}|^{\frac{1}{2}}, \\ \text{Vol}(\sigma_{\mathbb{L}}(A)) &= \text{Vol}(\sigma_{\mathbb{L}}(\mathcal{O}_{\mathbb{L}})) \mathcal{N}(A).\end{aligned}$$

Proposição 18. [1] *Seja \mathbb{L} um corpo de números de grau n , $\mathcal{D}_{\mathbb{L}}$ o discriminante de \mathbb{L} , $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros algébricos de \mathbb{L} , A um ideal não nulo de $\mathcal{O}_{\mathbb{L}}$ e r_2 metade do número de monomorfismos imaginários. Então, a densidade de centro do reticulado $\sigma_{\mathbb{L}}(A)$ é dada por*

$$\delta(\sigma_{\mathbb{L}}(A)) = \frac{2^{r_2} (\rho(\sigma_{\mathbb{L}}(A)))^n}{|\mathcal{D}_{\mathbb{L}}|^{\frac{1}{2}} \mathcal{N}(A)}.$$

Proposição 19. *Seja \mathbb{L} um corpo de números abeliano e $x \in \mathbb{L}$, então,*

$$|\sigma_{\mathbb{L}}(x)|^2 = c_{\mathbb{L}} \text{Tr}_{\mathbb{L}/\mathbb{Q}}(x\bar{x}),$$

onde

$$c_{\mathbb{L}} = \begin{cases} 1, & \text{se } \mathbb{L} \text{ for totalmente real.} \\ \frac{1}{2}, & \text{se } \mathbb{L} \text{ for totalmente imaginário.} \end{cases}$$

Exemplo 18. *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ um corpo biquadrático, onde m e n são inteiros estritamente positivos e livres de quadrados, isto é, \mathbb{K} é um corpo totalmente real, então $c_{\mathbb{K}} = 1$. Considere a base (iv) apresentada no enunciado do Teorema [23]. Seja α o gerador do ideal e y um elemento genérico de $\mathcal{O}_{\mathbb{K}}$, ambos dados por*

$$\begin{aligned}\alpha &= a \cdot 1 + b\sqrt{m} + c\sqrt{n} + d \left(\frac{\sqrt{m} + \sqrt{m_1 n_1}}{2} \right), \\ y &= a_1 \cdot 1 + a_2\sqrt{m} + a_3\sqrt{n} + a_4 \left(\frac{\sqrt{m} + \sqrt{m_1 n_1}}{2} \right).\end{aligned}$$

Podemos calcular x , um elemento genérico do ideal, pelo seguinte produto

$$\begin{aligned}x = \alpha y &= a_1 a + a_2 a \sqrt{m} + a_3 a \sqrt{n} + a_4 a \left(\frac{\sqrt{m} + \sqrt{m_1 n_1}}{2} \right) + a_1 b \sqrt{m} + a_2 b m \\ &+ a_3 b \sqrt{m} \sqrt{n} + a_4 b \sqrt{m} \left(\frac{\sqrt{m} + \sqrt{m_1 n_1}}{2} \right) + a_1 c \sqrt{n} + a_2 c \sqrt{m} \sqrt{n} + a_3 c n \\ &+ a_4 c \sqrt{n} \left(\frac{\sqrt{m} + \sqrt{m_1 n_1}}{2} \right) + a_1 d \left(\frac{\sqrt{m} + \sqrt{m_1 n_1}}{2} \right) + a_2 d \sqrt{m} \left(\frac{\sqrt{m} + \sqrt{m_1 n_1}}{2} \right) \\ &+ a_3 d \sqrt{n} \left(\frac{\sqrt{m} + \sqrt{m_1 n_1}}{2} \right) + a_4 d \left(\frac{\sqrt{m} + \sqrt{m_1 n_1}}{2} \right)^2.\end{aligned}$$

Considerando as igualdades a seguir

$$\begin{aligned}\sqrt{m}\sqrt{n} &= 2l \left(\frac{\sqrt{m} + \sqrt{m_1 n_1}}{2} \right) - l\sqrt{m} \\ \sqrt{m} \left(\frac{\sqrt{m} + \sqrt{m_1 n_1}}{2} \right) &= \frac{m}{2} + \frac{m}{2l} \sqrt{n} \\ \sqrt{n} \left(\frac{\sqrt{m} + \sqrt{m_1 n_1}}{2} \right) &= l \left(\frac{\sqrt{m} + \sqrt{m_1 n_1}}{2} \right) - \frac{l}{2} \sqrt{m} + \frac{n}{2l} \sqrt{m} \\ \left(\frac{\sqrt{m} + \sqrt{m_1 n_1}}{2} \right)^2 &= \frac{m}{4} + \frac{m_1 n_1}{4} + \frac{m}{2l} \sqrt{n}\end{aligned}$$

e, substituindo-as na equação anterior, obtemos

$$\begin{aligned}x &= \left(a_1 a + a_2 b m + \frac{a_2 d m}{2} + a_3 c n + \frac{a_4 b m}{2} + \frac{a_4 d m}{4} + \frac{a_4 d m_1 n_1}{4} \right) \cdot 1 \\ &+ \left(a_1 b + a_2 a - a_2 c l - a_3 b l - \frac{a_3 d l}{2} + \frac{a_4 c n}{2l} - \frac{a_4 c l}{2} \right) \sqrt{m} \\ &+ \left(a_1 c + \frac{a_2 d m}{2l} + a_3 a + \frac{a_3 d m}{2l} + \frac{a_4 b m}{2l} + \frac{a_4 d m}{2l} \right) \sqrt{n} \\ &+ (a_1 d + 2a_2 c l + 2a_3 b l + a_3 d l + a_4 a + a_4 c l) \left(\frac{\sqrt{m} + \sqrt{m_1 n_1}}{2} \right).\end{aligned}\tag{4.3}$$

Tomando

$$\begin{aligned}A &= a_1 a + a_2 b m + \frac{a_2 d m}{2} + a_3 c n + \frac{a_4 b m}{2} + \frac{a_4 d m}{4} + \frac{a_4 d m_1 n_1}{4} \\ B &= a_1 b + a_2 a - a_2 c l - a_3 b l - \frac{a_3 d l}{2} + \frac{a_4 c n}{2l} - \frac{a_4 c l}{2} \\ C &= a_1 c + \frac{a_2 d m}{2l} + a_3 a + \frac{a_3 d m}{2l} + \frac{a_4 b m}{2l} + \frac{a_4 d m}{2l} \\ D &= a_1 d + 2a_2 c l + 2a_3 b l + a_3 d l + a_4 a + a_4 c l\end{aligned}$$

podemos reescrever (4.3) de modo que

$$x = A + B\sqrt{m} + C\sqrt{n} + D \left(\frac{\sqrt{m} + \sqrt{m_1 n_1}}{2} \right).$$

Logo, é possível encontrar a seguinte expressão para x^2

$$\begin{aligned}x^2 &= A^2 + B^2 m + B D m + C^2 n + \frac{D^2 m}{4} + \frac{D^2 m_1 n_1}{4} + \left(2AB + AD + \frac{CDn}{l} \right) \sqrt{m} \\ &+ \left(2AC + \frac{BDm}{l} + \frac{D^2 m}{2l} \right) \sqrt{n} + \left(\frac{AD}{l} + 2BC + CD \right) \sqrt{m}\sqrt{n}.\end{aligned}$$

Pela Definição 4.1, conseguimos calcular o traço utilizando os automorfismos (4.2) definidos em 7.5

$$\begin{aligned}\text{Tr}(x^2) &= \sigma_1(x^2) + \sigma_2(x^2) + \sigma_3(x^2) + \sigma_1(x^2) \\ &= 4 \left(A^2 + B^2 m + B D m + C^2 n + \frac{D^2 m}{4} + \frac{D^2 m_1 n_1}{4} \right)\end{aligned}$$

Portanto, a partir dos automorfismos (4.2), concluímos que

$$|\sigma_{\mathbb{K}}(x)|^2 = c_{\mathbb{K}} \text{Tr}(x^2)$$

Proposição 20. [1] *Seja \mathbb{L} um corpo de números de grau n , totalmente real ou totalmente imaginário. Seja $\mathcal{O}_{\mathbb{L}}$ o anel dos inteiros algébricos de \mathbb{L} e \mathcal{A} um ideal não nulo de $\mathcal{O}_{\mathbb{L}}$. Então, a densidade de centro do reticulado $\sigma_{\mathbb{L}}(\mathcal{A})$ é dada por:*

$$\delta(\sigma_{\mathbb{L}}(\mathcal{A})) = \frac{1}{2^n |\mathcal{D}_{\mathbb{L}}|^{\frac{1}{2}}} t^{\frac{n}{2}}, \quad (4.4)$$

onde $t = \min\{\text{Tr}_{\mathbb{L}/\mathbb{Q}}(x\bar{x}) \mid x \in \mathcal{A}, x \neq 0\}$.

A partir da proposição anterior, apresentamos o seguinte resultado.

Proposição 21. *Considere o corpo biquadrático $\mathbb{K} = \mathbb{Q}(\sqrt{m}, \sqrt{n})$, onde $m, n > 0$, distintos e livres de quadrado, sendo $l = \text{mdc}(m, n)$, com $m = lm_1$ e $n = ln_1$. A densidade de centro do reticulado $\sigma(\mathcal{O}_{\mathbb{K}})$, pela Proposição [20], utilizando os valores dos discriminantes apresentados no Teorema [24] é dada por*

$$\delta(\Lambda) = \begin{cases} \frac{1}{lm_1n_1}, & se(m, n) \equiv (1, 1) \pmod{4} \\ \frac{1}{4lm_1n_1}, & se(m, n) \equiv (1, 2) \text{ ou } (3, 3) \pmod{4} \\ \frac{1}{8lm_1n_1}, & se(m, n) \equiv (2, 3) \pmod{4} \end{cases} \quad (4.5)$$

Demonstração. Como $\mathbb{K} = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ onde $m, n > 0$ distintos e livres de quadrado, temos que \mathbb{K} é um corpo totalmente real de grau 4 cuja densidade de centro do reticulado $\sigma(\mathcal{O}_{\mathbb{K}})$ é dada pela Equação (4.4) apresentada na Proposição [20]. O valor t definido como $t = \min\{\text{Tr}_{\mathbb{K}/\mathbb{Q}}(x\bar{x}) \mid x \in \mathcal{O}_{\mathbb{K}}, x \neq 0\}$, para $x = 1 \in \mathcal{O}_{\mathbb{K}}$, temos $\text{Tr}_{\mathbb{K}/\mathbb{Q}}(1 \cdot \bar{1}) = \text{Tr}_{\mathbb{K}/\mathbb{Q}}(1) = [\mathbb{K} : \mathbb{Q}] = 4$, pois a forma traço de 1 é igual ao grau da extensão e a norma do ideal $\mathcal{A} = \mathcal{O}_{\mathbb{K}}$ é dada por $\mathcal{N}(\mathcal{O}_{\mathbb{K}}) = [\mathcal{O}_{\mathbb{K}} : \mathcal{O}_{\mathbb{K}}] = 1$, pois o índice do anel de inteiros em si mesmo é trivialmente 1. Substituindo os valores t e $\mathcal{N}(\mathcal{A})$ obtemos

$$\delta(\sigma(\mathcal{O}_{\mathbb{K}})) = \frac{1}{|\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}}}$$

logo, substituindo os valores dos discriminantes apresentados no Teorema [24], temos que a densidade de centro do reticulado $\sigma(\mathcal{O}_{\mathbb{K}})$ é dada pela Equação [4.5]

$$\delta(\sigma(\mathcal{O}_{\mathbb{K}})) = \begin{cases} \frac{1}{lm_1n_1}, & se(m, n) \equiv (1, 1) \pmod{4} \\ \frac{1}{4lm_1n_1}, & se(m, n) \equiv (1, 2) \text{ ou } (3, 3) \pmod{4} \\ \frac{1}{8lm_1n_1}, & se(m, n) \equiv (2, 3) \pmod{4} \end{cases} \quad (4.6)$$

■

A partir das cinco bases integrais distintas do Teorema [23] para o anel de inteiros $\mathcal{O}_{\mathbb{K}}$, construímos as matrizes geradoras M aplicando o homomorfismo σ , apresentado na Definição [75], a conjuntos específicos de elementos algébricos.

Para base (i), $\left\{1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m_1n_1}}{4}\right\}$, obtemos as imagens via homomorfismo σ [4.1]:

$$\begin{aligned} \sigma(1) &= (1, 1, 1, 1) \\ \sigma\left(\frac{1+\sqrt{m}}{2}\right) &= \left(\frac{1}{2} + \frac{\sqrt{m}}{2}, \frac{1}{2} + \frac{\sqrt{m}}{2}, \frac{1}{2} - \frac{\sqrt{m}}{2}, \frac{1}{2} - \frac{\sqrt{m}}{2}\right) \\ \sigma\left(\frac{1+\sqrt{n}}{2}\right) &= \left(\frac{1}{2} + \frac{\sqrt{n}}{2}, \frac{1}{2} - \frac{\sqrt{n}}{2}, \frac{1}{2} + \frac{\sqrt{n}}{2}, \frac{1}{2} - \frac{\sqrt{n}}{2}\right) \\ \sigma\left(\frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m_1n_1}}{4}\right) &= \left(\frac{1}{4} + \frac{\sqrt{m}}{4} + \frac{\sqrt{n}}{4} + \frac{\sqrt{m}\sqrt{n}}{4k}, \frac{1}{4} + \frac{\sqrt{m}}{4} - \frac{\sqrt{n}}{4} \right. \\ &\quad \left. - \frac{\sqrt{m}\sqrt{n}}{4k}, \frac{1}{4} - \frac{\sqrt{m}}{4} + \frac{\sqrt{n}}{4} - \frac{\sqrt{m}\sqrt{n}}{4k}, \frac{1}{4} - \frac{\sqrt{m}}{4} - \frac{\sqrt{n}}{4} + \frac{\sqrt{m}\sqrt{n}}{4k}\right) \end{aligned}$$

A matriz geradora M_i correspondente é dada por

$$M_i = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix},$$

onde $v_1 = \sigma(1)$, $v_2 = \sigma\left(\frac{1+\sqrt{m}}{2}\right)$, $v_3 = \sigma\left(\frac{1+\sqrt{n}}{2}\right)$ e $v_4 = \sigma\left(\frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m_1n_1}}{4}\right)$, cuja matriz de Gram associada é

$$G_i = \begin{pmatrix} 4 & 2 & 2 & 1 \\ 2 & m+1 & 1 & \frac{m}{2} + \frac{1}{2} \\ 2 & 1 & n+1 & \frac{n}{2} + \frac{1}{2} \\ 1 & \frac{m}{2} + \frac{1}{2} & \frac{n}{2} + \frac{1}{2} & \frac{mn}{4k^2} + \frac{m}{4} + \frac{n}{4} + \frac{1}{4} \end{pmatrix}. \quad (4.7)$$

Para base (ii), $\left\{1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1-\sqrt{m}+\sqrt{n}+\sqrt{m_1n_1}}{4}\right\}$, obtemos

$$\sigma(1) = (1, 1, 1, 1)$$

$$\sigma\left(\frac{1+\sqrt{m}}{2}\right) = \left(\frac{1}{2} + \frac{\sqrt{m}}{2}, \frac{1}{2} + \frac{\sqrt{m}}{2}, \frac{1}{2} - \frac{\sqrt{m}}{2}, \frac{1}{2} - \frac{\sqrt{m}}{2}\right)$$

$$\sigma\left(\frac{1+\sqrt{n}}{2}\right) = \left(\frac{1}{2} + \frac{\sqrt{n}}{2}, \frac{1}{2} - \frac{\sqrt{n}}{2}, \frac{1}{2} + \frac{\sqrt{n}}{2}, \frac{1}{2} - \frac{\sqrt{n}}{2}\right)$$

$$\sigma\left(\frac{1-\sqrt{m}+\sqrt{n}+\sqrt{m_1n_1}}{4}\right) = \left(\frac{1}{4} - \frac{\sqrt{m}}{4} + \frac{\sqrt{n}}{4} + \frac{\sqrt{m}\sqrt{n}}{4k}, \frac{1}{4} - \frac{\sqrt{m}}{4} - \frac{\sqrt{n}}{4} - \frac{\sqrt{m}\sqrt{n}}{4k}, \frac{1}{4} + \frac{\sqrt{m}}{4} + \frac{\sqrt{n}}{4} - \frac{\sqrt{m}\sqrt{n}}{4k}, \frac{1}{4} + \frac{\sqrt{m}}{4} - \frac{\sqrt{n}}{4} + \frac{\sqrt{m}\sqrt{n}}{4k}\right)$$

A matriz geradora M_{ii} correspondente é dada por

$$M_{ii} = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix},$$

onde $v_1 = \sigma(1)$, $v_2 = \sigma\left(\frac{1+\sqrt{m}}{2}\right)$, $v_3 = \sigma\left(\frac{1+\sqrt{n}}{2}\right)$ e $v_4 = \sigma\left(\frac{1-\sqrt{m}+\sqrt{n}+\sqrt{m_1n_1}}{4}\right)$, cuja matriz de Gram associada é

$$G_{ii} = \begin{pmatrix} 4 & 2 & 0 & 0 \\ 2 & m+1 & 0 & 0 \\ 0 & 0 & 4n & 2n \\ 0 & 0 & 2n & \frac{mn}{k^2} + n \end{pmatrix}. \quad (4.8)$$

Para base (iii), $\left\{1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{m_1n_1}}{4}\right\}$, obtemos

$$\sigma(1) = (1, 1, 1, 1)$$

$$\sigma\left(\frac{1+\sqrt{m}}{2}\right) = \left(\frac{1}{2} + \frac{\sqrt{m}}{2}, \frac{1}{2} + \frac{\sqrt{m}}{2}, \frac{1}{2} - \frac{\sqrt{m}}{2}, \frac{1}{2} - \frac{\sqrt{m}}{2}\right)$$

$$\sigma(\sqrt{n}) = (\sqrt{n}, -\sqrt{n}, \sqrt{n}, -\sqrt{n})$$

$$\sigma\left(\frac{\sqrt{n}+\sqrt{m_1n_1}}{4}\right) = \left(\frac{1}{2} \left(\sqrt{n} + \frac{\sqrt{m}\sqrt{n}}{k}\right), \frac{1}{2} \left(-\sqrt{n} - \frac{\sqrt{m}\sqrt{n}}{k}\right), \frac{1}{2} \left(\sqrt{n} - \frac{\sqrt{m}\sqrt{n}}{k}\right), \frac{1}{2} \left(-\sqrt{n} + \frac{\sqrt{m}\sqrt{n}}{k}\right)\right)$$

A matriz geradora M_{iii} correspondente é dada por

$$M_{iii} = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix},$$

onde $v_1 = \sigma(1)$, $v_2 = \sigma\left(\frac{1+\sqrt{m}}{2}\right)$, $v_3 = \sigma(\sqrt{n})$ e $v_4 = \sigma\left(\frac{\sqrt{n}+\sqrt{m_1n_1}}{4}\right)$, cuja matriz de Gram associada é

$$G_{iii} = \begin{pmatrix} 4 & 2 & 0 & 0 \\ 2 & m+1 & 0 & 0 \\ 0 & 0 & 4n & 2n \\ 0 & 0 & 2n & \frac{mn}{k^2} + n \end{pmatrix}. \quad (4.9)$$

Para base (iv) , $\left\{1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{m}+\sqrt{m_1n_1}}{2}\right\}$, obtemos

$$\sigma(1) = (1, 1, 1, 1)$$

$$\sigma(\sqrt{m}) = (\sqrt{m}, \sqrt{m}, -\sqrt{m}, -\sqrt{m})$$

$$\sigma(\sqrt{n}) = (\sqrt{n}, -\sqrt{n}, \sqrt{n}, -\sqrt{n})$$

$$\sigma\left(\frac{\sqrt{m} + \sqrt{m_1n_1}}{2}\right) = \left(\frac{\sqrt{m}}{2} + \frac{\sqrt{m}\sqrt{n}}{2k}, \frac{\sqrt{m}}{2} - \frac{\sqrt{m}\sqrt{n}}{2k}, -\frac{\sqrt{m}}{2} - \frac{\sqrt{m}\sqrt{n}}{2k}, -\frac{\sqrt{m}}{2} + \frac{\sqrt{m}\sqrt{n}}{2k}\right)$$

A matriz geradora M_{iv} correspondente é dada por

$$M_{iv} = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix},$$

onde $v_1 = \sigma(1)$, $v_2 = \sigma(\sqrt{m})$, $v_3 = \sigma(\sqrt{n})$ e $v_4 = \sigma\left(\frac{\sqrt{m}+\sqrt{m_1n_1}}{2}\right)$, cuja matriz de Gram associada é

$$G_{iv} = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4m & 2m & 0 \\ 0 & 2m & \frac{mn}{k^2} + m & 0 \\ 0 & 0 & 0 & 4n \end{pmatrix}. \quad (4.10)$$

Para base (v) , $\left\{1, \sqrt{m}, \frac{\sqrt{m}+\sqrt{n}}{2}, \frac{1+\sqrt{m_1n_1}}{2}\right\}$, obtemos

$$\sigma(1) = (1, 1, 1, 1)$$

$$\sigma(\sqrt{m}) = (\sqrt{m}, -\sqrt{m}, \sqrt{m}, -\sqrt{m})$$

$$\sigma\left(\frac{\sqrt{m} + \sqrt{n}}{2}\right) = \left(\frac{1}{2}(\sqrt{m} + \sqrt{n}), \frac{1}{2}(\sqrt{m} - \sqrt{n}), \frac{1}{2}(-\sqrt{m} + \sqrt{n}), \frac{1}{2}(-\sqrt{m} - \sqrt{n})\right)$$

$$\sigma\left(\frac{1 + \sqrt{m_1n_1}}{2}\right) = \left(\frac{1}{2}\left(1 + \frac{\sqrt{m}\sqrt{n}}{k}\right), \frac{1}{2}\left(1 - \frac{\sqrt{m}\sqrt{n}}{k}\right), \frac{1}{2}\left(1 - \frac{\sqrt{m}\sqrt{n}}{k}\right), \frac{1}{2}\left(1 + \frac{\sqrt{m}\sqrt{n}}{k}\right)\right)$$

A matriz geradora M_v correspondente é dada por

$$M_v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix},$$

onde $v_1 = \sigma(1)$, $v_2 = \sigma(\sqrt{m})$, $v_3 = \sigma\left(\frac{\sqrt{m}+\sqrt{n}}{2}\right)$ e $v_4 = \sigma\left(\frac{1+\sqrt{m_1n_1}}{2}\right)$, cuja matriz de Gram associada é

$$G_v = \begin{pmatrix} 4 & 0 & 0 & 2 \\ 0 & 4m & 2m & 0 \\ 0 & 2m & m+n & 0 \\ 2 & 0 & 0 & \frac{mn}{k^2} + 1 \end{pmatrix}. \quad (4.11)$$

4.2 Base reduzida de Minkowski

Nesta seção, aplicamos o algoritmo de redução de Minkowski apresentado em [8] às bases integrais do Teorema 23, visando determinar vetores de norma mínima nos reticulados associados. O método explora as propriedades da matriz de Gram para garantir que o primeiro vetor da base reduzida tenha norma mínima, otimizando assim a construção dos reticulados algébricos. Conforme apresentado em [8] encontrar uma base $\{v_1, \dots, v_n\}$ do reticulado n -dimensional \mathcal{L} , que para cada t , $1 \leq t \leq n$ verificamos se

$$\langle v_t, v_t \rangle \leq \langle v, v \rangle \quad (4.12)$$

para todo vetor $v \in \mathcal{L}$ de tal forma que v_1, \dots, v_{t-1}, v pode ser estendido a uma base de \mathcal{L} . Isso implica que a matriz de Gram satisfazer as condições:

$$0 \leq a_{11} \leq a_{22} \leq \dots \leq a_{nn} \quad (4.13)$$

$$2 \left(\sum_{s \in S} \epsilon_s a_{st} - \sum_{\substack{r, s \in S \\ r < s}} \epsilon_r \epsilon_s a_{rs} \right) \leq \sum_{s \in S} a_{ss}, \quad (4.14)$$

onde $t \in \{2, \dots, n\}$, $S \subset \{1, \dots, n-1\}$ e $\epsilon_i = \pm 1$.

Agora, fixado t tome um vetor $v = v_t - \sum_{s \in S} \epsilon_s v_s$ onde S é um conjunto e ϵ_i são constantes associadas a cada $s \in S$.

Iniciaremos analisando a condição (4.12), onde $\langle v_t, v_t \rangle \leq \langle v, v \rangle$ para $1 < t \leq 4$.

Para o item (i) (assumindo $m \geq 5$, $n \geq 13$ e $l \geq 1$)

- $\langle v_1, v_1 \rangle \leq \langle v_2, v_2 \rangle \implies 4 \leq 1 + m$
- $\langle v_2, v_2 \rangle \leq \langle v_3, v_3 \rangle \implies 1 + m \leq 1 + n$
- $\langle v_3, v_3 \rangle \leq \langle v_4, v_4 \rangle \implies 1 + n \leq \frac{1}{4} \left(1 + m + n + \frac{mn}{l^2} \right)$

logo, são satisfeitas.

Para o item (iii) (assumindo $m \geq 5$, $n \geq 6$ e $l \geq 1$)

- $\langle v_1, v_1 \rangle \leq \langle v_2, v_2 \rangle \implies 4 \leq 1 + m$

- $\langle v_2, v_2 \rangle \leq \langle v_3, v_3 \rangle \implies 1 + m \leq 4n$
- $\langle v_3, v_3 \rangle \leq \langle v_4, v_4 \rangle \implies 4n \leq n + \frac{mn}{l^2}$

Portanto, a condição é satisfeita para as bases integrais representadas nos itens (i) e (iii) o que implica analisarmos as condições a seguir.

Analisando a condição (4.13): $0 \leq a_{11} \leq a_{22} \leq a_{33} \leq a_{44}$, a partir das matrizes de Gram G_i (4.7) e G_{iii} (4.9) temos:

Para o item (i): $0 \leq 4 \leq m + 1 \leq n + 1 \leq \frac{1}{4} (1 + m + n + \frac{mn}{l^2})$

Para o item (iii): $0 \leq 4 \leq m + 1 \leq 4n \leq n + \frac{mn}{l^2}$

Assim, os itens (i) e (iii) satisfazem a condição (4.13).

Agora, analisando a condição (4.14) temos:

No item (i):

- Para $t = 2$, $S = \{1\}$ e $\epsilon_1 = \pm 1 \implies 4\epsilon_1 \leq 4$
- Para $t = 3$, $S \subset \{1, 2\}$ e $\epsilon_i = \pm 1, i = 1, 2 \implies (4\epsilon_1 + 2\epsilon_2 - (4\epsilon_1\epsilon_2)) \leq 4 + m + 1$
- Para $t = 4$, $S \subset \{1, 2, 3\}$ e $\epsilon_i = \pm 1, i = 1, 2, 3$

$$2\epsilon_1 + \frac{2m+2}{2}\epsilon_2 + \frac{2n+2}{2}\epsilon_3 - (4\epsilon_1\epsilon_2 + 4\epsilon_1\epsilon_3 + 2\epsilon_2\epsilon_3) \leq 4 + m + 1 + n + 1$$

No item (iii):

- Para $t = 2$, $S = \{1\}$ e $\epsilon_1 = \pm 1 \implies 4\epsilon_1 \leq 4$
- Para $t = 3$, $S \subset \{1, 2\}$ e $\epsilon_i = \pm 1, i = 1, 2 \implies -4\epsilon_1\epsilon_2 \leq 4 + m + 1$
- Para $t = 4$, $S \subset \{1, 2, 3\}$ e $\epsilon_i = \pm 1, i = 1, 2, 3 \implies 4n\epsilon_3 - 4\epsilon_1\epsilon_2 \leq 4 + m + 1 + 4n$

Logo, concluímos que as matrizes M_i e M_{iii} são Minkowski reduzida.

Para o item (ii) na verificação da condição (4.12) a desigualdade $\langle v_3, v_3 \rangle \leq \langle v_4, v_4 \rangle$ não é satisfeita, logo seguindo o algoritmo apresentado em [8] trocamos v_3 por v_4 , de modo que, $\langle v_3, v_3 \rangle \leq \langle v_4, v_4 \rangle$ seja satisfeito, ou seja

$$\begin{aligned} v_3 &= \left(\frac{1}{4} - \frac{\sqrt{m}}{4} + \frac{\sqrt{n}}{4} + \frac{\sqrt{m}\sqrt{n}}{4l}, \frac{1}{4} - \frac{\sqrt{m}}{4} - \frac{\sqrt{n}}{4} - \frac{\sqrt{m}\sqrt{n}}{4l}, \right. \\ &\quad \left. \frac{1}{4} + \frac{\sqrt{m}}{4} + \frac{\sqrt{n}}{4} - \frac{\sqrt{m}\sqrt{n}}{4l}, \frac{1}{4} + \frac{\sqrt{m}}{4} - \frac{\sqrt{n}}{4} + \frac{\sqrt{m}\sqrt{n}}{4l} \right), \\ v_4 &= \left(\frac{1}{2} + \frac{\sqrt{n}}{2}, \frac{1}{2} - \frac{\sqrt{n}}{2}, \frac{1}{2} + \frac{\sqrt{n}}{2}, \frac{1}{2} - \frac{\sqrt{n}}{2} \right), \end{aligned}$$

agora com a nova matriz de Gram,

$$G_{ii} = \begin{pmatrix} 4 & 2 & 1 & 2 \\ 2 & m+1 & \frac{1-m}{2} & 1 \\ 1 & \frac{1-m}{2} & \frac{1}{4} \left(\frac{mn}{l^2} + m + n + 1 \right) & \frac{n+1}{2} \\ 2 & 1 & \frac{n+1}{2} & n+1 \end{pmatrix} \quad (4.15)$$

Condição (4.13) do item (ii) (assumindo $m \geq 21$, $n \geq 33$ e $l \geq 3$)

$$0 \leq 4 \leq m + 1 \leq \frac{1}{4} \left(\frac{mn}{k^2} + m + n + 1 \right)$$

Condição (4.14) temos:

- Para $t = 2$, $S = \{1\}$, $\epsilon_1 = \pm 1 \Rightarrow 4\epsilon_1 \leq 4$
- Para $t = 3$, $S \subset \{1, 2\}$, $\epsilon_i = \pm 1, i = 1, 2 \Rightarrow 2\epsilon_1 + (1 - m)\epsilon_2 - 4\epsilon_1\epsilon_2 \leq 5 + m$
- Para $t = 4$, $S \subset \{1, 2, 3\}$, $\epsilon_i = \pm 1, i = 1, 2, 3 \Rightarrow 4\epsilon_1 + 2\epsilon_2 + (1 + n)\epsilon_3 - 4\epsilon_1\epsilon_2 - 2\epsilon_1\epsilon_3 - (1 - m)\epsilon_1\epsilon_3 \leq 4 + m + 1 + \frac{1}{4} \left(1 + m + n + \frac{mn}{l^2}\right)$

podemos verificar que as condições são satisfeitas. Assim, a base é Minkowski reduzida.

Para o item (iv) assim como para o item (ii) a verificação da condição (4.12) a desigualdade $\langle v_3, v_3 \rangle \leq \langle v_4, v_4 \rangle$ não é satisfeita, dessa forma trocamos v_3 por v_4 , de modo que $\langle v_3, v_3 \rangle \leq \langle v_4, v_4 \rangle$ seja satisfeito, ou seja

$$v_3 = \left(\frac{\sqrt{m}}{2} + \frac{\sqrt{m}\sqrt{n}}{2l}, \quad \frac{\sqrt{m}}{2} - \frac{\sqrt{m}\sqrt{n}}{2l}, \right. \\ \left. -\frac{\sqrt{m}}{2} - \frac{\sqrt{m}\sqrt{n}}{2l}, \quad -\frac{\sqrt{m}}{2} + \frac{\sqrt{m}\sqrt{n}}{2l} \right), \\ v_4 = (\sqrt{n}, -\sqrt{n}, \sqrt{n}, -\sqrt{n}).$$

a matriz de Gram reduzida é

$$\begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4m & 2m & 0 \\ 0 & 2m & \frac{mn}{l^2} + m & 0 \\ 0 & 0 & 0 & 4n \end{pmatrix} \quad (4.16)$$

Condição (4.12) do item (iv) (assumindo $m \geq 2$, $n \geq 3$ e $l \geq 3$) temos:

- $\langle v_1, v_1 \rangle \leq \langle v_2, v_2 \rangle \implies 4 \leq 4m$
- $\langle v_2, v_2 \rangle \leq \langle v_3, v_3 \rangle \implies 4m \leq \frac{mn}{l^2} + m$
- $\langle v_3, v_3 \rangle \leq \langle v_4, v_4 \rangle \implies \frac{mn}{l^2} + m \leq 4n$

Condição (4.13) do item (iv)

$$0 \leq a_{11} \leq a_{22} \leq a_{33} \leq a_{44} \implies 0 \leq 4 \leq 4m \leq \frac{mn}{l^2} + m \leq 4n$$

Condição (4.14) do item (iv)

- Para $t = 2$, $S = \{1\}$, $\epsilon_1 = \pm 1 \Rightarrow 0 \leq 4$
- Para $t = 3$, $S \subset \{1, 2\}$, $\epsilon_i = \pm 1, i = 1, 2 \Rightarrow 4m\epsilon_2 \leq 4 + 4m$
- Para $t = 4$, $S \subset \{1, 2, 3\}$, $\epsilon_i = \pm 1, i = 1, 2, 3 \Rightarrow -4m\epsilon_2\epsilon_3 \leq 4 + 5m + \frac{mn}{l^2}$

O item (v) na verificação da condição (4.12), a desigualdade $\langle v_2, v_2 \rangle \leq \langle v_3, v_3 \rangle$ não é satisfeita, dessa forma trocamos v_2 por v_3 , de modo que $\langle v_2, v_2 \rangle \leq \langle v_3, v_3 \rangle$ seja satisfeito, logo

$$v_2 = \left(\frac{1}{2}(\sqrt{m} + \sqrt{n}), \quad \frac{1}{2}(\sqrt{m} - \sqrt{n}), \quad \frac{1}{2}(-\sqrt{m} + \sqrt{n}), \quad \frac{1}{2}(-\sqrt{m} - \sqrt{n}) \right), \\ v_3 = (\sqrt{m}, -\sqrt{m}, \sqrt{m}, -\sqrt{m}).$$

Seguindo a verificação das próximas condições, consideramos a nova matriz de Gram

$$\begin{pmatrix} 4 & 0 & 0 & \frac{1}{2}(\sqrt{m}+3) \\ 0 & m+n & 2m & -\frac{1}{4}(\sqrt{m}-1)(\sqrt{m}+\sqrt{n}) \\ 0 & 2m & 4m & \frac{1}{2}(\sqrt{m}-m) \\ \frac{1}{2}(\sqrt{m}+3) & -\frac{1}{4}(\sqrt{m}-1)(\sqrt{m}+\sqrt{n}) & \frac{1}{2}(\sqrt{m}-m) & \frac{l^2(m+3)+2l(\sqrt{m}-1)\sqrt{m}\sqrt{n}+4mn}{4l^2} \end{pmatrix} \quad (4.17)$$

que satisfaz a condição (4.13), mas para a condição (4.14) não é satisfeita para $t = 3$ quando $(e_1, e_2) = (1, 1)$ e $(e_1, e_2) = (-1, 1)$. Logo substituímos v_3 por $v'_3 = v_3 - v_2$. Obtendo assim a nova base, seguindo as verificações, temos:

Condição (4.12) do item (v) (assumindo $m \geq 3$, $n \geq 7$ e $l \geq 1$)

- $\langle v_1, v_1 \rangle \leq \langle v_2, v_2 \rangle \implies 4 \leq m + n$
- $\langle v_2, v_2 \rangle \leq \langle v_3, v_3 \rangle \implies m + n \leq m + n$
- $\langle v_3, v_3 \rangle \leq \langle v_4, v_4 \rangle \implies m + n \leq \frac{l^2(m+3)+2l(\sqrt{m}-1)\sqrt{m}\sqrt{n}+4mn}{4l^2}$

Condição (4.13) do item (v): $0 \leq a_{11} \leq a_{22} \leq a_{33} \leq a_{44}$

$$0 \leq 4 \leq m + n \leq m + n \leq \frac{l^2(m+3) + 2l(\sqrt{m}-1)\sqrt{m}\sqrt{n} + 4mn}{4l^2}$$

Condição (4.14) do item (v)

- Para $t = 2, S = \{1\}, \epsilon_1 = \pm 1 \implies 0 \leq 4$
- Para $t = 3, S \subset \{1, 2\}, \epsilon_i = \pm 1, i = 1, 2 \implies 2(m-n)\epsilon_2 \leq 4 + m + n$
- Para $t = 4, S \subset \{1, 2, 3\}, \epsilon_i = \pm 1, i = 1, 2, 3 \implies (3 + \sqrt{m})\epsilon_1 - \frac{1}{2}(\sqrt{m}-1)(\sqrt{m} + \sqrt{n})\epsilon_2 - \frac{1}{2}(\sqrt{m}-1)(\sqrt{m}-\sqrt{n})\epsilon_3 - 2(m-n)\epsilon_2\epsilon_3 \leq 4 + 2m + 2n$

satisfazendo todas as condições, cuja matriz de Gram Minkowski reduzida é

$$\begin{pmatrix} 4 & 0 & 0 & \frac{1}{2}(\sqrt{m}+3) \\ 0 & m+n & m-n & -\frac{1}{4}(\sqrt{m}-1)(\sqrt{m}+\sqrt{n}) \\ 0 & m-n & m+n & -\frac{1}{4}(\sqrt{m}-1)(\sqrt{m}-\sqrt{n}) \\ \frac{1}{2}(\sqrt{m}+3) & -\frac{1}{4}(\sqrt{m}-1)(\sqrt{m}+\sqrt{n}) & -\frac{1}{4}(\sqrt{m}-1)(\sqrt{m}-\sqrt{n}) & \frac{l^2(m+3)+2l(\sqrt{m}-1)\sqrt{m}\sqrt{n}+4mn}{4l^2} \end{pmatrix}. \quad (4.18)$$

4.3 Testes computacionais

Apresentamos uma análise dos resultados obtidos utilizando o software Wolfram Mathematica 14.0 para calcular os valores de $\delta(\sigma(\mathcal{O}_{\mathbb{K}}))$. Um dos passos cruciais na construção de um reticulado é a obtenção da densidade de centro, uma medida que relaciona-se à densidade de empacotamento do reticulado.

Esquemmatizando o algoritmo para o cálculo da densidade de centro:

1. **Entrada:** Conjunto $\{m, n\}$ com $m \in \{2, 3, 4, \dots, 99\}$ e $n \in \{m+1, m+2, \dots, 100\}$.
2. **Inicialização:** Definir V como conjunto vazio e variáveis rm, rn, rm_1 , e rn_1 como 1.
3. **Iteração:** Para cada par (m, n) , calcular:
 - (a) O máximo divisor comum l de m e n .
 - (b) Divisões $m_1 = \frac{m}{l}$ e $n_1 = \frac{n}{l}$.

- (c) Resto de m , n , m_1 e n_1 quando divididos por 4, armazenados em t_1 , t_2 , t_3 e t_4 , respectivamente.
- (d) Raízes quadradas de m e n , verificando se são inteiras (u_1 e u_2).
- (e) Se m e n não têm raízes inteiras (u_1 e u_2 são **False**) e os restos t_1 , t_2 , t_3 , e t_4 coincidem com rm , rn , rm_1 e rn_1 , então:
- Armazenar o vetor $\mathbf{vet} = \{m, n, l\}$.
 - Calcular $V_1 = \frac{1}{lm_1n_1}$ e definir $\mathbf{vet} = \{V_1, m, n, l\}$.
 - Imprimir \mathbf{vet} .

4. **Saída:** Imprime o vetor $\{V_1, m, n, l\}$ sempre que as condições são satisfeitas.

A análise dos resultados obtidos revela um certo padrão no comportamento dos valores correspondentes de l entre m e n . Observou-se que, ao considerar diferentes valores e especialmente quando l é maior que 1, os resultados tendem a apresentar um desempenho superior. Com isso em mente, decidimos investigar o comportamento dos resultados ao desconsiderar os casos onde $l \neq 1$. A tabela a seguir apresenta os resultados obtidos sob essa condição, permitindo uma comparação mais direta entre os pares analisados.

| m | n | l | Densidade de centro |
|----|----|----|---------------------|
| 5 | 45 | 5 | 0.0222222 |
| 5 | 65 | 5 | 0.0153846 |
| 5 | 85 | 5 | 0.0117647 |
| 13 | 65 | 13 | 0.0153846 |
| 17 | 85 | 17 | 0.0117647 |
| 45 | 65 | 5 | 0.0017094 |
| 45 | 85 | 5 | 0.00130719 |
| 65 | 85 | 5 | 0.000904977 |

Tabela 4.1: Densidade de centro (i)

Os resultados apresentados a seguir seguem um padrão análogo ao anteriormente discutido, com a única diferença dos itens utilizados no Teorema [24](#). Assim como nas iterações anteriores, a expectativa é que, ao manter l diferente de 1, os resultados reflitam um comportamento consistente, com melhorias na estrutura e na eficiência dos valores obtidos. Essa abordagem não apenas confirma a regularidade observada nos resultados passados, mas também oferece uma perspectiva mais abrangente sobre a dinâmica que rege as relações entre m , n e l .

| m | n | l | Densidade de centro |
|----|----|----|---------------------|
| 5 | 10 | 5 | 0.025 |
| 5 | 30 | 5 | 0.00833333 |
| 5 | 50 | 5 | 0.005 |
| 5 | 70 | 5 | 0.00357143 |
| 5 | 90 | 5 | 0.00277778 |
| 13 | 26 | 13 | 0.00961538 |
| 13 | 78 | 13 | 0.00320513 |
| 17 | 34 | 17 | 0.00735294 |

Tabela 4.2: Densidade de centro (ii)

| m | n | l | Densidade de centro |
|----|----|----|---------------------|
| 10 | 15 | 5 | 0.00416667 |
| 10 | 35 | 5 | 0.00178571 |
| 10 | 55 | 5 | 0.00113636 |
| 10 | 75 | 5 | 0.000833333 |
| 18 | 27 | 9 | 0.00231481 |
| 26 | 39 | 13 | 0.00160256 |
| 34 | 51 | 17 | 0.00122549 |
| 42 | 63 | 21 | 0.000992063 |

Tabela 4.3: Densidade de centro (iii)

Observação 7. Nas tabelas anteriores os valores de densidade de centro apresentaram melhores resultados quando $l \neq 1$, indicando uma maior eficiência nesses casos. No

entanto, para o par específico do item (ii), $(m, n) \equiv (3, 3)$, os resultados com $l = 1$ mostraram-se mais efetivos, o que contrasta com os casos anteriores. Essa particularidade sugere uma dependência dos valores de m e n na otimização dos resultados.

| m | n | l | Densidade de centro |
|---|----|---|---------------------|
| 3 | 7 | 1 | 0.0119048 |
| 3 | 11 | 1 | 0.00757576 |
| 3 | 19 | 1 | 0.00438596 |
| 3 | 23 | 1 | 0.00362319 |
| 3 | 31 | 1 | 0.00268817 |
| 3 | 35 | 1 | 0.00238095 |
| 3 | 43 | 1 | 0.00193798 |
| 3 | 47 | 1 | 0.00177305 |

Tabela 4.4: Densidade de centro (ii')

A investigação computacional realizada forneceu resultados que, embora relevantes, revelam que ainda há um longo caminho para alcançar densidades mais próximas das ótimas. O melhor valor de densidade de centro encontrado, independente do intervalo escolhido, foi aproximadamente 0.025, um valor consideravelmente inferior quando comparado ao reticulado D_4 , cuja densidade de centro é a maior na dimensão 4, com um valor de 0.125. Essa disparidade indica que os reticulados construídos até o momento ainda não são ideais em termos de eficiência. Apesar dessa diferença, eles fornecem um entendimento inicial das propriedades dos reticulados gerados a partir do anel de inteiros algébricos $\mathcal{O}_{\mathbb{K}}$ de um corpo de números \mathbb{K} . Contudo, como observamos, essa abordagem inicial limita a densidade de centro obtida.

Com base nos dados, a próxima fase desse estudo será focada no refinamento da construção desses reticulados. Um dos caminhos promissores é substituir o uso direto de $\mathcal{O}_{\mathbb{K}}$ por ideais não nulos desse anel. A utilização de ideais não nulos oferece um potencial para obter reticulados com densidades de centro mais altas, aproximando-nos de configurações mais eficientes.

4.4 Reticulados bem arredondados

Na teoria da informação e codificação, os reticulados bem arredondados desempenham um papel fundamental na construção de esquemas eficientes para transmissão de dados em canais ruidosos. Dois dos modelos mais relevantes são o canal gaussiano, que modela perturbações aditivas com ruído branco, e o canal Rayleigh com desvanecimento, que incorpora variações aleatórias na amplitude do sinal devido a efeitos de multipropagação. Neste contexto, reticulados bem arredondados são essenciais pois proporcionam estruturas geométricas que maximizam a eficiência energética e a capacidade de correção de erros. Esta seção explora a conexão entre teoria de reticulados e teoria da informação e como códigos baseados em reticulados podem ser otimizados para esses cenários de comunicação.

Definição 76. [5] Um reticulado Λ é dito bem arredondado quando seus vetores mínimos geram todo o espaço \mathbb{R}^n .

Em \mathbb{R}^2 , essa propriedade apresenta um comportamento particular: os reticulados podem ter 2, 4 ou 6 vetores mínimos, mas são bem arredondados apenas nos casos com 4

ou 6 vetores. No que se refere a reticulados bidimensionais, observa-se que apenas configurações com quatro ou seis vetores mínimos satisfazem essa condição, enquanto arranjos com dois vetores mínimos não a alcançam.

Ao analisarmos reticulados algébricos da forma $\sigma(\mathcal{O}_{\mathbb{K}})$, onde \mathbb{K} é um corpo quadrático e σ o mergulho canônico, encontramos apenas dois exemplos bem arredondados: o reticulado inteiro \mathbb{Z}^2 , associado ao corpo $\mathbb{Q}(\sqrt{-1})$, e o reticulado hexagonal, associado ao corpo $\mathbb{Q}(\sqrt{-3})$. Contudo, embora esses sejam os únicos casos em que $\sigma(\mathcal{O}_{\mathbb{K}})$ é bem arredondado, existem infinitos corpos quadráticos \mathbb{K} para os quais $\mathcal{O}_{\mathbb{K}}$ contém um ideal I tal que $\sigma(I)$ forma um reticulado bem arredondado.

A seguir apresentamos um algoritmo para verificar se o reticulado $\sigma(\mathcal{O}_{\mathbb{K}})$ ou um subreticulado dele é bem arredondado.

- (i) Dado \mathbb{K} um corpo biquadrático, listamos possíveis normas dos vetores do reticulado $\sigma(\mathcal{O}_{\mathbb{K}})$ e colocamos os valores encontrados num conjunto L_1 .
- (ii) Para cada norma da lista L_1 , verificamos se no reticulado existem 4 vetores linearmente independentes com a referida norma. Conhecemos a norma mínima do reticulado $\sigma(\mathcal{O}_{\mathbb{K}})$, caso o algoritmo não retorne 4 vetores linearmente independentes de norma mínima concluímos que o reticulado não é bem arredondado. Daí, podemos analisar para os subreticulados. Cada norma M (que satisfaz a condição inicial) é colocada num conjunto L_2 .
- (iii) Entrada: M (da Lista L_2).
 A : matriz geradora do reticulado $\sigma(\mathcal{O}_{\mathbb{K}})$.
 $v_j \in \sigma(\mathcal{O}_{\mathbb{K}})$ tal que $\|v_j\|^2 = M$, para $j = 1, 2, 3, 4$ (Passo anterior).
- (iv) Para cada $j = 1, 2, 3, 4$ encontrar $t_j = (t_{j1}, t_{j2}, t_{j3}, t_{j4}) \in \mathbb{Z}^4$ tal que $v_j = t_j A$ (o vetor t_j representa as coordenadas de v_j na base implícita na matriz geradora A).
- (v) Determinar a matriz $Q = T A$ (matriz geradora do reticulado $\Lambda = \text{span}\{v_1, v_2, v_3, v_4\}$), onde $T = (t_{ij})_{i,j=1}^4$.
- (vi) Aplicar a redução de Minkowski na matriz Q obtendo a matriz geradora reduzida Q_1 .
- (vii) Tomar $G = Q_1 Q_1^t$ (Gram reduzida do subreticulado Λ). Se $g_{11} = M$ então Λ é bem arredondado.
- (viii) As normas que estão relacionadas a subreticulados bem arredondados são listadas num conjunto L_3 .

Apresentamos agora um método para justificar que todo subreticulado bem arredondado obtido pelo algoritmo anterior pode ser realizado geometricamente através de um submódulo contido em $\mathcal{O}_{\mathbb{K}}$.

Sejam $\{e_1, e_2, e_3, e_4\}$ uma base integral de \mathbb{K} e \mathcal{M} um \mathbb{Z} -módulo livre de posto 4 gerado por $\{\omega_1, \omega_2, \omega_3, \omega_4\}$, em que $\omega_i = t_{i1}e_1 + t_{i2}e_2 + t_{i3}e_3 + t_{i4}e_4$ (t_{ij} do algoritmo anterior), para

$i = 1, 2, 3, 4$. O reticulado $\sigma(\mathcal{M})$ possui matriz geradora

$$\begin{aligned}
 Q &= \begin{pmatrix} \sigma_1(\omega_1) & \sigma_2(\omega_1) & \sigma_3(\omega_1) & \sigma_4(\omega_1) \\ \sigma_1(\omega_2) & \sigma_2(\omega_2) & \sigma_3(\omega_2) & \sigma_4(\omega_2) \\ \sigma_1(\omega_3) & \sigma_2(\omega_3) & \sigma_3(\omega_3) & \sigma_4(\omega_3) \\ \sigma_1(\omega_4) & \sigma_2(\omega_4) & \sigma_3(\omega_4) & \sigma_4(\omega_4) \end{pmatrix} = \begin{pmatrix} \sigma_1\left(\sum_{j=1}^4 t_{1j}e_j\right) & \cdots & \sigma_4\left(\sum_{j=1}^4 t_{1j}e_j\right) \\ \vdots & \ddots & \vdots \\ \sigma_1\left(\sum_{j=1}^4 t_{4j}e_j\right) & \cdots & \sigma_4\left(\sum_{j=1}^4 t_{4j}e_j\right) \end{pmatrix} \\
 &= \begin{pmatrix} t_{11} & t_{12} & t_{13} & t_{14} \\ t_{21} & t_{22} & t_{23} & t_{24} \\ t_{31} & t_{32} & t_{33} & t_{34} \\ t_{41} & t_{42} & t_{43} & t_{44} \end{pmatrix} \cdot \begin{pmatrix} \sigma_1(e_1) & \sigma_2(e_1) & \sigma_3(e_1) & \sigma_4(e_1) \\ \sigma_1(e_2) & \sigma_2(e_2) & \sigma_3(e_2) & \sigma_4(e_2) \\ \sigma_1(e_3) & \sigma_2(e_3) & \sigma_3(e_3) & \sigma_4(e_3) \\ \sigma_1(e_4) & \sigma_2(e_4) & \sigma_3(e_4) & \sigma_4(e_4) \end{pmatrix} = TA,
 \end{aligned} \tag{4.19}$$

em que A é a matriz geradora do reticulado $\sigma(\mathcal{O}_{\mathbb{K}})$. Assim, pelo algoritmo anterior, Q é a matriz geradora do reticulado $\sigma(\mathcal{M}) = \text{span}\{v_1, v_2, v_3, v_4\}$. Podemos também inferir que

$$\text{Vol}(\sigma(\mathcal{M})) = |\det(Q)| = |\det(TA)| = |\det(T)||\det(A)| = |\det(T)|\sqrt{\mathcal{D}_{\mathbb{K}}},$$

e portanto

$$[\mathcal{O}_{\mathbb{K}} : \mathcal{M}] = |\det(T)|.$$

Exemplo 19. *Considere o corpo biquadrático $\mathbb{K} = \mathbb{Q}(\sqrt{5} + \sqrt{13})$, listamos possíveis normas dos vetores do reticulado $\sigma(\mathcal{O}_{\mathbb{K}})$, listadas no conjunto abaixo*

$L_1 = \{4, 6, 14, 16, 18, 20, 21, 22, 23, 24, 27, 30, 31, 33, 34, 36, 37, 38, 41, 42, 43, 46, 47, 49, 51, 52, 53, 54, 56, 57, 58, 59, 61, 62, 63, 64, 66, 67, 68, 69, 70, 71, 72, 73, 74, 76, 77, 78, 79, 80, 81, 82, 83, 84, 86, 87, 88, 89, 90, 92, 93, 94, 96, 97, 98, 99, 100, 101, 102, 103, 105, 106, 107, 108, 109, 110, 111, 113, 114, 115, 116, 118, 119, 120, 121, 122, 123, 124, 126, 127, 129, 131, 132, 133, 134, 135, 136, 137, 138, 139, 141, 142, 144, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 157, 158, 159, 161, 162, 163, 164, 165, 166, 167, 168, 170, 171, 172, 173, 174, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 193, 194, 196, 197, 198, 199\}$

Na verdade a lista inicial era bem maior, chegando até a norma 11000, mas para os propósitos que citaremos a seguir, limitamos até 200. O objetivo é mostrar que o reticulado $\sigma(\mathcal{O}_{\mathbb{K}})$ ou algum subreticulado dele é bem arredondado. Assim, para cada norma da lista, verificamos se no reticulado existem 4 vetores linearmente independentes com a referida norma, as que satisfazem essa condição são listadas no conjunto abaixo:

$L_2 = \{21, 23, 27, 31, 33, 37, 41, 43, 47, 49, 51, 53, 57, 59, 61, 63, 66, 67, 69, 71, 73, 74, 77, 79, 81, 82, 83, 84, 87, 89, 92, 93, 94, 97, 98, 99, 101, 102, 103, 105, 106, 107, 108, 109, 111, 113, 114, 115, 118, 119, 121, 122, 123, 124, 126, 127, 129, 131, 132, 133, 134, 135, 137, 138, 141, 142, 146, 148, 149, 151, 153, 157, 158, 159, 161, 162, 163, 164, 165, 166, 167, 171, 172, 173, 174, 177, 178, 179, 181, 183, 186, 187, 188, 189, 191, 193, 194, 196, 197, 198, 199\}$

Usando a redução de Minkowski, apresentada na Seção [4.2](#), verificamos que norma mínima do reticulado é 4, e esta norma não apareceu na lista anterior, então não existe a possibilidade do reticulado $\sigma(\mathcal{O}_{\mathbb{K}})$ ser bem arredondado, mas podemos procurar por subreticulados que sejam bem arredondados. Agora, existem 4 vetores $\{v_1, v_2, v_3, v_4\}$ linearmente independentes de norma M , para cada $M \in L_2$, resta saber se o reticulado

$\Lambda = \text{span}\{v_1, v_2, v_3, v_4\}$ possui norma mínima M , para cada $M \in L_2$. As normas que satisfazem essa condição são listadas no conjunto abaixo:

$$L_3 = \{37, 43, 69, 97\}$$

Portanto, podemos exibir 4 subreticulados gerados por vetores de norma mínima e esses reticulados podem ser realizados geometricamente via \mathbb{Z} -módulos. Façamos para $M = 37$.

Seja \mathbb{K} um corpo de números tal que $\mathbb{K} = \mathbb{Q}(\sqrt{5} + \sqrt{13})$. Nesse caso, $[\mathbb{K} : \mathbb{Q}] = 4$ e, como $(5, 13) \equiv (1, 1) \pmod{4}$, tomando $e_1 = 1$, $e_2 = \frac{1+\sqrt{5}}{2}$, $e_3 = \frac{1+\sqrt{13}}{2}$ e $e_4 = \frac{1+\sqrt{5}+\sqrt{13}+\sqrt{65}}{4}$, temos que $\{e_1, e_2, e_3, e_4\}$ é uma \mathbb{Z} -base de $\mathcal{O}_{\mathbb{K}}$. Seja \mathcal{M} um submódulo de $\mathcal{O}_{\mathbb{K}}$ gerado pelos vetores linearmente independentes $\{w_1, w_2, w_3, w_4\}$, em que $w_1 = -2 + e_2 + e_4$, $w_2 = -2 + 2e_2 - e_4$, $w_3 = -1 - e_2 + e_3 - e_4$ e $w_4 = -2e_2 - e_3 + e_4$

$$\{-2 + e_1 + e_3, -2 + 2e_1 - e_3, -1 - e_1 + e_2 - e_3, -2e_1 - e_2 + e_3\}.$$

Nesse caso, $\sigma(\mathcal{M})$ é um reticulado de posto 4 em \mathbb{R}^4 . De fato, se $x \in \mathcal{M}$, então existem $a_1, a_2, a_3, a_4 \in \mathbb{Z}$ tais que

$$x = a_1(-2 + e_1 + e_3) + a_2(-2 + 2e_1 - e_3) + a_3(-1 - e_1 + e_2 - e_3) + a_4(-2e_1 - e_2 + e_3),$$

e conseqüentemente $\sigma(x) = \gamma TA$, onde $\gamma = (a_1, a_2, a_3, a_4)$,

$$T = \begin{pmatrix} -2 & 1 & 0 & 1 \\ -2 & 2 & 0 & -1 \\ -1 & -1 & 1 & -1 \\ 0 & -2 & -1 & 1 \end{pmatrix} \quad e \quad A = \begin{pmatrix} \sigma_1(e_1) & \sigma_2(e_1) & \sigma_3(e_1) & \sigma_4(e_1) \\ \sigma_1(e_2) & \sigma_2(e_2) & \sigma_3(e_2) & \sigma_4(e_2) \\ \sigma_1(e_3) & \sigma_2(e_3) & \sigma_3(e_3) & \sigma_4(e_3) \\ \sigma_1(e_4) & \sigma_2(e_4) & \sigma_3(e_4) & \sigma_4(e_4) \end{pmatrix},$$

onde A é uma matriz geradora do reticulado $\sigma(\mathcal{O}_{\mathbb{K}})$, já que $\{e_1, e_2, e_3, e_4\}$ é uma \mathbb{Z} -base para $\mathcal{O}_{\mathbb{K}}$. Temos que $Q = TA$ é uma matriz geradora para $\sigma(\mathcal{M})$, e como Q tem posto 4, segue que o reticulado $\sigma(\mathcal{M})$ possui posto 4. Uma matriz de Gram para o reticulado $\sigma(\mathcal{M})$ é $G = TG_1T^t$, onde $G_1 = (\text{Tr}_{\mathbb{K}|\mathbb{Q}}(e_i e_j))_{i,j=1}^4$ é uma matriz de Gram para o reticulado $\sigma(\mathcal{O}_{\mathbb{K}})$ tal que

$$G_1 = \begin{pmatrix} 4 & 2 & 2 & 1 \\ 2 & 6 & 1 & 3 \\ 2 & 1 & 14 & 7 \\ 1 & 3 & 7 & 21 \end{pmatrix},$$

então uma matriz de Gram para o reticulado $\sigma(\mathcal{M})$ é dada por

$$G = TG_1T^t = \begin{pmatrix} 37 & -2 & -18 & 8 \\ -2 & 37 & 8 & -18 \\ -18 & 8 & 37 & -2 \\ 8 & -18 & -2 & 37 \end{pmatrix}.$$

Nesse caso, usando o algoritmo de redução de base de Minkowski, nota-se que a matriz Q já está reduzida. Assim, o reticulado $\sigma(\mathcal{M})$ é gerado por quatro vetores de norma mínima 37, sendo, portanto, um reticulado bem arredondado.

Apresentamos agora uma tabela com as normas mínimas dos subreticulados bem arredondados via corpos biquadráticos.

| Base (i) do Teorema 23 | | | | Base (ii) do Teorema 23 | | | |
|------------------------|-----|-----|--|-------------------------|-----|-----|--|
| m | n | l | $\min\{\ \sigma(x)\ ^2; x \in \mathcal{M}\}$ | m | n | l | $\min\{\ \sigma(x)\ ^2; x \in \mathcal{M}\}$ |
| 5 | 13 | 1 | {37, 43, 69, 97} | 21 | 33 | 3 | {45, 53, 95} |
| 5 | 17 | 1 | {43, 49, 97, 101} | 21 | 45 | 3 | {55, 63, 105} |
| 5 | 21 | 1 | {55, 83, 125, 275} | 21 | 57 | 3 | {65, 73, 115} |
| 5 | 29 | 1 | {67, 95, 143} | 21 | 69 | 3 | {83, 117, 125} |
| 5 | 33 | 1 | {77, 101} | 21 | 77 | 7 | {39, 45, 153} |

| Base (iii) do Teorema 23 | | | |
|--------------------------|-----|-----|--|
| m | n | l | $\min\{\ \sigma(x)\ ^2 \mid x \in \mathcal{M}\}$ |
| 5 | 6 | 1 | {84, 166, 216} |
| 5 | 10 | 1 | {64, 280} |
| 5 | 14 | 1 | {376} |

Os resultados evidenciam que o método é eficaz para as bases (i), (ii) e (iii), fornecendo valores mínimos de $\|\sigma(x)\|^2$ dentro do intervalo considerado. Entretanto, para as bases (iv) e (v), observa-se uma divergência nos resultados, sugerindo que o intervalo de busca adotado não é suficiente nesses casos. Portanto, embora o método apresente consistência em contextos restritos, sua generalização requer ajustes para garantir sua efetividade.

4.5 Família de reticulados \mathbb{Z}^4 rotacionados

Nesta seção faremos a construção de uma família de reticulados \mathbb{Z}^4 rotacionados via subcorpos biquadráticos, e diferentemente da construção da seção anterior, aqui escolheremos \mathbb{Z} -módulos contidos em $\mathbb{Z}[\theta]$ ao invés de contidos no anel dos inteiros algébricos. As referências utilizadas nessa seção foram [1], [2].

Seja α um elemento totalmente real e positivo de \mathbb{K} , ou seja, $\alpha_i = \sigma_i(\alpha) \in \mathbb{R}$ e $\alpha_i = \sigma_i(\alpha) > 0$ para todo $i = 1, 2, \dots, n$.

O mergulho torcido $\sigma : \mathbb{K} \rightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ é definido por

$$\sigma_\alpha(x) = \left(\sqrt{\alpha_1} \sigma_1(x), \dots, \sqrt{\alpha_{r_1}} \sigma_{r_1}(x), \sqrt{2\alpha_{r_1+1}} \sigma_{r_1+1}(x), \dots, \sqrt{2\alpha_{r_1+r_2}} \sigma_{r_1+r_2}(x) \right),$$

onde $x \in \mathbb{K}$. Frequentemente, identificamos $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ com \mathbb{R}^n . Se $\alpha = 1$, então o mergulho torcido é chamado de mergulho canônico.

Reticulados algébricos são aqueles obtidos a partir de módulos no anel de inteiros de corpos de números algébricos por meio de mergulhos canônicos ou torcidos. Se \mathcal{M} é um \mathbb{Z} -módulo livre de $\mathbb{Z}[\theta]$ de posto completo n , então $\sigma_\alpha(\mathcal{M})$ é um reticulado n -dimensional cuja norma mínima é dada por

$$t = \min\{\|\sigma_\alpha(x)\|^2 : x \in \mathcal{M}, x \neq 0\}.$$

O volume de $\sigma_\alpha(\mathcal{M})$ é dado por

$$\text{Vol}(\sigma_\alpha(\mathcal{M})) = 2^{-r_2} [\mathbb{Z}[\theta] : \mathcal{M}] \sqrt{\Delta(\mathbb{Z}[\theta]) \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha)},$$

em que r_2 é a metade da quantidade de homomorfismos imaginários, $[\mathbb{Z}[\theta] : \mathcal{M}]$ é o índice do \mathbb{Z} -módulo \mathcal{M} sobre $\mathbb{Z}[\theta]$, $\Delta(\mathbb{Z}[\theta])$ é o discriminante de $\mathbb{Z}[\theta]$ e $\mathcal{N}(\alpha)$ é a norma do elemento α . A densidade de centro de $\sigma_\alpha(\mathcal{M})$ é dada por

$$\delta(\sigma_\alpha(\mathcal{M})) = \frac{t^{n/2}}{2^n \text{Vol}(\sigma_\alpha(\mathcal{M}))},$$

Se o corpo \mathbb{K} é abeliano, então para todo $i = 1, 2, \dots, n$, então

$$\|\sigma_\alpha(x)\|^2 = \begin{cases} \text{Tr}_{\mathbb{K}}(\alpha x^2), & \text{se } \mathbb{K} \text{ é totalmente real,} \\ \frac{1}{2} \text{Tr}_{\mathbb{K}}(\alpha x \bar{x}), & \text{se } \mathbb{K} \text{ é totalmente complexo.} \end{cases} \quad (4.20)$$

Neste caso, da Equação (4.20), segue que

$$\delta(\sigma_\alpha(\mathcal{M})) = \frac{t^{n/2}}{2^n [\mathbb{Z}[\theta] : \mathcal{M}] \sqrt{\Delta(\mathbb{Z}[\theta]) \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha)}}. \quad (4.21)$$

Seja $\mathbb{K} = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ um corpo biquadrático sobre \mathbb{Q} , onde m, n ($m < n$) são inteiros racionais, livres de quadrados e de paridades distintas, com $m = 2^t p_1 p_2 \cdots p_r$, $t = 0, 1$, $r \geq 0$, p_i é um número primo e $p_i \equiv 1 \pmod{4}$, para $i = 1, 2, \dots, r$. Sob estas condições, $4m$ pode ser escrito como a soma dos quadrados de dois inteiros, ou seja, $4m = a^2 + b^2$, onde $a, b \in \mathbb{Z}$. Escolhemos $n = a + (m + 1)$. Obviamente, dado $m = 2^t p_1 p_2 \cdots p_r$, o n escolhido nem sempre é livre de quadrados; por exemplo, se $m = 13$ então $n = 18$ ou $n = 20$. Portanto, estamos interessados apenas em m e n livre de quadrados. Neste caso, considere o inteiro $k = \sqrt{4m - (n - m - 1)^2}$.

Proposição 22. *Existem infinitos m e n livres de quadrados tais que $4m = a^2 + b^2$ e $n = a + (m + 1)$.*

Demonstração. Seja $a \in \mathbb{Z}$, $a > 0$. Como $(1 - a, 1) = 1$ pelo teorema de Dirichlet, a sequência $(1 - a) + n$, onde $n \in \mathbb{Z}$, contém infinitos números primos p tais que $p \equiv 1 \pmod{4}$. Em particular, o teorema vale para n livre de quadrados, ou seja, existem infinitos n livres de quadrados tais que $p = (1 - a) + n$, ou equivalentemente, $n = a + (p + 1)$. Como $a \in \mathbb{Z}$ é arbitrário, e tomando $m = p$, concluímos que m é livre de quadrados, e o resultado segue. ■

Proposição 23. *Seja \mathcal{M} um \mathbb{Z} -módulo livre de $\mathbb{Z}[\theta]$ de posto completo 4 gerado por $\{\omega_1, \omega_2, \omega_3, \omega_4\}$, onde*

$$\begin{cases} \omega_1 = (1 + k^2)\theta - \theta^3, \\ \omega_2 = (n - m) + (m - n)\theta^2, \\ \omega_3 = (mk - nk)\theta, \\ \omega_4 = mk - nk. \end{cases}$$

Então

$$[\mathbb{Z}[\theta] : \mathcal{M}] = (4m - (n - m - 1)^2)(n - m)^3.$$

Demonstração. Pela Equação (4.19), temos que

$$T = \begin{pmatrix} 0 & 1 + k^2 & 0 & -1 \\ n - m & 0 & m - n & 0 \\ 0 & mk - nk & 0 & 0 \\ mk - nk & 0 & 0 & 0 \end{pmatrix},$$

e conseqüentemente, o índice de \mathcal{M} sobre $\mathbb{Z}[\theta]$ é calculado de forma análoga ao índice de \mathcal{M} sobre $\mathcal{O}_{\mathbb{K}}$, isto é,

$$[\mathbb{Z}[\theta] : \mathcal{M}] = |\det(T)| = |k^2(n - m)^3| = k^2(n - m)^3 = (4m - (n - m - 1)^2)(n - m)^3,$$

pois $k > 0$ e $n > m$. ■

Proposição 24. *O elemento $\alpha = (m^2 + n^2 + 6mn - m - n) + (-m - n + 1)\theta^2$ é totalmente real e positivo.*

Demonstração. Temos que $\theta_1 = -\theta_4 = \sqrt{m} + \sqrt{n}$ e $\theta_2 = -\theta_3 = \sqrt{m} - \sqrt{n}$. O polinômio minimal $p(x) = x^4 - 2(m+n)x^2 + (m-n)^2$ satisfaz $p(x) \leq 0$ se $\theta_4 \leq x \leq \theta_2 < 0$ ou $0 < \theta_3 \leq x \leq \theta_1$. Por outro lado, $p(x) \geq 0$ se $\theta_2 \leq x \leq \theta_3$. Também temos que $4m = (n - m - 1)^2 + k^2$, então

$$\begin{aligned}(n - m - 1)^2 &< 4m \\ (n - m)^2 - 2(n - m) + 1 &< 4m \\ (m - n)^2 - 2(m + n) + 1 &< 0 \\ p(1) &< 0.\end{aligned}$$

Como $0 < 1 < \theta_1$ e $p(1) < 0$, segue que $\theta_3 < 1$, ou seja, $-\sqrt{m} + \sqrt{n} < 1$, então

$$\begin{aligned}(-\sqrt{m} + \sqrt{n})^2 &< 1 \\ m + n - 2\sqrt{mn} &< 1 \\ m + n - 1 &< 2\sqrt{mn}.\end{aligned}$$

Portanto,

$$-2\sqrt{mn}(m + n - 1) > -4mn. \quad (4.22)$$

Agora, como $\theta_1 = -\theta_4$ e $\theta_2 = -\theta_3$, pela Equação (4.22), segue que

$$\begin{aligned}\sigma_1(\alpha) &= \sigma_4(\alpha) = (m^2 + n^2 + 6mn - m - n) + (-m - n + 1)\theta_1^2 \\ &= (m^2 + n^2 + 6mn - m - n) + (-m - n + 1)(\sqrt{m} + \sqrt{n})^2 \\ &= (m^2 + n^2 + 6mn - m - n) + (-m - n + 1)(m + 2\sqrt{mn} + n) \\ &= 4mn - 2\sqrt{mn}(m + n - 1) > 4mn - 4mn = 0.\end{aligned}$$

$$\begin{aligned}\sigma_2(\alpha) &= \sigma_3(\alpha) = (m^2 + n^2 + 6mn - m - n) + (-m - n + 1)\theta_2^2 \\ &= (m^2 + n^2 + 6mn - m - n) + (-m - n + 1)(\sqrt{m} - \sqrt{n})^2 \\ &= (m^2 + n^2 + 6mn - m - n) + (-m - n + 1)(m - 2\sqrt{mn} + n) \\ &= 4mn + 2\sqrt{mn}(m + n - 1) > 0,\end{aligned}$$

pois $m, n \geq 2$. Portanto, $\sigma_i(\alpha) > 0$ para $i = 1, 2, 3, 4$, ou seja, α é totalmente real e positivo. ■

Proposição 25. *A norma de α é dada por*

$$N_{K/\mathbb{Q}}(\alpha) = [4mn(m^2 + n^2 - 2mn - 2m - 2n + 1)]^2.$$

Demonstração. Como $\alpha = a_1 + a_2\theta^2$, com $a_1 = m^2 + n^2 + 6mn - m - n$ e $a_2 = -m - n + 1$, pela Equação (2.1) temos que

$$\begin{aligned}
N_{K/\mathbb{Q}}(\alpha) &= \prod_{i=1}^4 \sigma_i(\alpha) = \prod_{i=1}^4 (a_1 + a_2\sigma_i(\theta)^2) = \prod_{i=1}^4 (a_1 + a_2\theta_i^2) \\
&= a_1^4 + a_1^3a_2 \sum_{i=1}^4 \theta_i^2 + a_1^2a_2^2 \sum_{1 \leq i < j \leq 4} \theta_i^2\theta_j^2 \\
&\quad + a_1a_2^3 \sum_{1 \leq i < j < k \leq 4} \theta_i^2\theta_j^2\theta_k^2 + a_2^4 \prod_{i=1}^4 \theta_i^2 \\
&= a_1^4 + (4m + 4n)a_1^3a_2 + (6m^2 + 4mn + 6n^2)a_1^2a_2^2 + a_1(m - n)^4a_2^3 \\
&= [4mn(m^2 + n^2 - 2mn - 2m - 2n + 1)]^2.
\end{aligned}$$

■

Proposição 26. *O raio de empacotamento do reticulado $\Lambda = \sigma_\alpha(\mathcal{M})$ é dado por*

$$\rho(\Lambda) = 16mn(n - m)(m - n)(n^2 + m^2 - 2nm - 2n - 2m + 1).$$

Demonstração. Seja $x \in M$, então existem $b_1, b_2, b_3, b_4 \in \mathbb{Z}$ tais que

$$\begin{aligned}
x &= b_1\omega_1 + b_2\omega_2 + b_3\omega_3 + b_4\omega_4 \\
&= b_1[(1 + k^2)\theta - \theta^3] + b_2[(n - m) + (m - n)\theta^2] + b_3[(mk - nk)\theta] + b_4(mk - nk) \\
&= (-b_2m + b_4mk + b_2n - b_4nk) + (b_1 + b_1k^2 + b_3mk - b_3nk)\theta \\
&\quad + (b_2m - b_2n)\theta^2 + (-b_1)\theta^3.
\end{aligned}$$

Tomando

$$\begin{cases} a_0 = -b_2m + b_4mk + b_2n - b_4nk, \\ a_1 = b_1 + b_1k^2 + b_3mk - b_3nk, \\ a_2 = b_2m - b_2n, \\ a_3 = -b_1, \end{cases}$$

sabendo que $k = \sqrt{4m - (n - m - 1)^2}$, $\alpha_j = \sigma_j(\alpha)$, para $j = 1, 2, 3, 4$, e $\alpha = (m^2 + n^2 + 6mn - m - n) + (-m - n + 1)\theta^2$, segue que

$$\begin{aligned}
\|\sigma(x)\|^2 &= (-b_2m + b_4mk + b_2n - b_4nk)^2 \sum_{j=1}^4 \alpha_j \\
&\quad + (b_1 + b_1k^2 + b_3mk - b_3nk)^2 \sum_{j=1}^4 \alpha_j \theta_j^2 \\
&\quad + (b_2m - b_2n)^2 \sum_{j=1}^4 \alpha_j \theta_j^4 + (-b_1)^2 \sum_{j=1}^4 \alpha_j \theta_j^6 \\
&\quad + 2[(-b_2m + b_4mk + b_2n - b_4nk)(b_1 + b_1k^2 + b_3mk - b_3nk)] \sum_{j=1}^4 \alpha_j \theta_j \\
&\quad + (-b_2m + b_4mk + b_2n - b_4nk)(b_2m - b_2n) \sum_{j=1}^4 \alpha_j \theta_j^2 \\
&\quad + [(-b_2m + b_4mk + b_2n - b_4nk)(-b_1) \\
&\quad + (b_1 + b_1k^2 + b_3mk - b_3nk)(b_2m - b_2n)] \sum_{j=1}^4 \alpha_j \theta_j^3 \\
&\quad + (b_1 + b_1k^2 + b_3mk - b_3nk)(-b_1) \sum_{j=1}^4 \alpha_j \theta_j^4 \\
&\quad + (b_2m - b_2n)(-b_1) \sum_{j=1}^4 \alpha_j \theta_j^5 \\
&= 16mn(n - m)(m - n)(n^2 + m^2 - 2nm - 2n - 2m + 1)(b_1^2 + b_2^2 + b_3^2 + b_4^2).
\end{aligned}$$

Portanto,

$$\min\{\|\sigma(x)\|^2 : x \in M, x \neq 0\} = 16mn(n - m)(m - n)(n^2 + m^2 - 2nm - 2n - 2m + 1),$$

basta escolher, por exemplo, $b_1 = 1$ e $b_2 = b_3 = b_4 = 0$. ■

Proposição 27. *O reticulado $\Lambda = \sigma_\alpha(\mathcal{M})$ é uma versão rotacionada do reticulado \mathbb{Z}_4 .*

Demonstração. Pela Equação (4.21), a densidade central do reticulado $\Lambda = \sigma_\alpha(\mathcal{M})$ é dada por

$$\begin{aligned}
\delta(\sigma_\alpha(\mathcal{M})) &= \frac{t^{n/2}}{2^n [\mathbb{Z}[\theta] : M] \sqrt{\Delta(\mathbb{Z}[\theta])} N_{K/\mathbb{Q}}(\alpha)} \\
&= \frac{[16mn(n-m)(m-n)(n^2+m^2-2nm-2n-2m+1)]^2}{2^4(4m-(n-m-1)^2)(n-m)^3} \\
&\quad \frac{1}{\sqrt{2^{12}(mn(m-n))^2[4mn(m^2+n^2-2mn-2m-2n+1)]^2}} \\
&= \frac{2^8 m^2 n^2 (m-n)^4 (n^2+m^2-2nm-2n-2m+1)^2}{2^4 (n^2+m^2-2nm-2n-2m+1) (m-n)^3 2^6 (mn(m-n))} \\
&\quad \frac{1}{(4mn(m^2+n^2-2mn-2m-2n+1))} \\
&= \frac{2^8 m^2 n^2 (m-n)^4 (n^2+m^2-2nm-2n-2m+1)^2}{2^4 (2^8 m^2 n^2 (m-n)^4 (n^2+m^2-2nm-2n-2m+1)^2)} \\
&= \frac{1}{2^4}.
\end{aligned}$$

Portanto, como o reticulado \mathbb{Z}_4 é o único reticulado na dimensão 4 que, a menos de isomorfismo, tem densidade central igual a $\frac{1}{2^4}$, segue o resultado. Mostremos que é uma versão rotacionada e escalonada do \mathbb{Z}^4 . Uma matriz geradora para o reticulado $\sigma_\alpha(\mathcal{M})$ é dada por $M_1 = TMA$, onde

$$T = \begin{pmatrix} 0 & 1+k^2 & 0 & -1 \\ n-m & 0 & m-n & 0 \\ 0 & mk-nk & 0 & 0 \\ mk-nk & 0 & 0 & 0 \end{pmatrix},$$

$$M = \begin{pmatrix} \sigma_1(1) & \sigma_2(1) & \sigma_3(1) & \sigma_4(1) \\ \sigma_1(\theta) & \sigma_2(\theta) & \sigma_3(\theta) & \sigma_4(\theta) \\ \sigma_1(\theta^2) & \sigma_2(\theta^2) & \sigma_3(\theta^2) & \sigma_4(\theta^2) \\ \sigma_1(\theta^3) & \sigma_2(\theta^3) & \sigma_3(\theta^3) & \sigma_4(\theta^3) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ \frac{1}{\sqrt{m}+\sqrt{n}} & \frac{1}{\sqrt{m}-\sqrt{n}} & \frac{1}{-\sqrt{m}+\sqrt{n}} & \frac{1}{-\sqrt{m}-\sqrt{n}} \\ \frac{1}{(\sqrt{m}+\sqrt{n})^2} & \frac{1}{(\sqrt{m}-\sqrt{n})^2} & \frac{1}{(-\sqrt{m}+\sqrt{n})^2} & \frac{1}{(-\sqrt{m}-\sqrt{n})^2} \\ \frac{1}{(\sqrt{m}+\sqrt{n})^3} & \frac{1}{(\sqrt{m}-\sqrt{n})^3} & \frac{1}{(-\sqrt{m}+\sqrt{n})^3} & \frac{1}{(-\sqrt{m}-\sqrt{n})^3} \end{pmatrix}, \text{ e}$$

$$A = \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & 0 & 0 & 0 \\ 0 & \sqrt{\sigma_2(\alpha)} & 0 & 0 \\ 0 & 0 & \sqrt{\sigma_3(\alpha)} & 0 \\ 0 & 0 & 0 & \sqrt{\sigma_4(\alpha)} \end{pmatrix},$$

com

$$\sigma_1(\alpha) = \sigma_4(\alpha) = \alpha = (m^2 + n^2 + 6mn - m - n) + (-m - n + 1)(\sqrt{m} + \sqrt{n})^2$$

$$\sigma_2(\alpha) = \sigma_3(\alpha) = (m^2 + n^2 + 6mn - m - n) + (-m - n + 1)(-\sqrt{m} + \sqrt{n})^2.$$

Assim, uma matriz de Gram associada é dada por

$$G = M_1 M_1^t = \begin{pmatrix} \rho(\Lambda) & 0 & 0 & 0 \\ 0 & \rho(\Lambda) & 0 & 0 \\ 0 & 0 & \rho(\Lambda) & 0 \\ 0 & 0 & 0 & \rho(\Lambda) \end{pmatrix}.$$

Portanto, o reticulado $\sigma_\alpha(\mathcal{M})$ é uma versão rotacionada e escalonado do reticulado \mathbb{Z}^4 .

■

Conclusão

Ao longo desta dissertação, investigamos a construção de reticulados em \mathbb{R}^n a partir de \mathbb{Z} -módulos e ideais do anel de inteiros de corpos biquadráticos, contribuindo para o desenvolvimento teórico e para aplicações práticas em matemática aplicada. O estudo foi conduzido em três eixos principais: a caracterização algébrica dos reticulados, sua análise computacional e a exploração de propriedades geométrica para problemas de empacotamento esférico e teoria da informação.

Inicialmente, desenvolvemos um método completo para a construção de reticulados baseado no anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de corpos biquadráticos. Nesse método é utilizado cinco bases integrais via homomorfismos canônicos, conforme estabelecido pelo Teorema 23, seguida pela aplicação da redução de Minkowski para otimização dessas bases. A implementação computacional desse processo, realizada em Wolfram Mathematica 14.0, permitiu uma análise das densidades de centro obtidas. Os resultados, embora relevantes, revelaram uma discrepância significativa em relação aos reticulados conhecidos por sua eficiência. Enquanto o reticulado D_4 , reconhecido como ótimo na dimensão 4, apresenta uma densidade de centro de 0.125, as construções aqui realizadas alcançaram valores máximos próximos de 0.025, correspondendo a menos de 20% da densidade ideal. Essa diferença destacou a necessidade de refinamentos metodológicos para aproximar-nos de configurações mais eficientes.

Na segunda etapa da pesquisa, direcionamos esforços para o aprimoramento dessas construções, explorando alternativas que pudessem levar a reticulados com melhores propriedades de empacotamento. Uma abordagem promissora consistiu na substituição do anel total $\mathcal{O}_{\mathbb{K}}$ por ideais, por preservarem a estrutura de módulo, mas com maior flexibilidade, mostraram potencial para gerar reticulados com densidades mais elevadas. Em seguida, investigamos reticulados bem arredondados, cuja relevância se estende à teoria da informação. Para essa classe de reticulados, desenvolvemos um algoritmo específico capaz de encontrar possíveis subreticulados bem arredondados de $\sigma(\mathcal{O}_{\mathbb{K}})$, gerando assim uma tabela completa com as normas mínimas associadas. Além disso, propusemos uma construção alternativa baseada em \mathbb{Z} -módulos contidos em $\mathbb{Z}[\theta]$, em vez do anel de inteiros completo, o que permitiu a obtenção de uma família de reticulados \mathbb{Z}^4 rotacionados com propriedades distintas das estudadas anteriormente.

Como perspectivas futuras, este trabalho abre caminho para investigações em três direções principais. A primeira diz respeito ao aprofundamento da análise computacional, com foco em reticulados construídos a partir de corpos totalmente imaginários, onde parâmetros como vetores de norma mínima, densidades de centro e realização geométrica comparativa com D_4 serão estudados. A segunda linha de pesquisa envolve a exploração de construções baseadas em ideais próprios de $\mathcal{O}_{\mathbb{K}}$, buscando reticulados que superem em

eficiência aqueles gerados pelo anel completo. Por fim, a terceira direção visa ampliar o entendimento sobre reticulados bem arredondados, não apenas classificando famílias genéricas desses objetos, mas também estabelecendo critérios algébricos para sua construção.

Em síntese, os resultados aqui apresentados fornecem um avanço teórico e computacional para o estudo de reticulados em dimensões superiores. As limitações identificadas ao longo do trabalho não apenas evidenciam a complexidade inerente ao problema, mas também delimitam fronteiras claras para investigações futuras, as quais têm o potencial de avançar a teoria e aplicação de reticulados.

Referências

- [1] A. J. Ferrari. Reticulados algébricos via corpos abelianos. Dissertação (mestrado), Universidade Estadual Paulista, Instituto de Biociências, Letras e Ciências Exatas, São José do Rio Preto, 2008. 105 f.
- [2] G. C. Jorge. *Reticulados q -ários e algébricos*. Tese (doutorado), Universidade Estadual de Campinas, Campinas, SP, 2012. Orientador: Sueli Irene Rodrigues Costa.
- [3] N. Kakuta; P. Salehyan. *Introdução à Teoria de Galois*. Cultura Acadêmica Editora, São Paulo, 2013.
- [4] O. B. Mirandola. Algoritmos computacionais para geração de reticulados algébricos via método de krüskemper. Dissertação (mestrado), Universidade Estadual Paulista, Faculdade de Ciências, 2021.
- [5] W. L. S. Pinto; C. Alves. Reticulados bem arredondados em \mathbb{R}^2 . *Proceedings Series of the Brazilian Society of Computational and Applied Mathematics*, 6(2), 2018.
- [6] V. C. Silva. Extensões algébricas dos racionais. In *31^o Colóquio Brasileiro de Matemática*, Rio de Janeiro, July 30 - August 5 2017. IMPA.
- [7] I. N. Stewart; D. O. Tall. *Algebraic Number Theory*. Chapman and Hall, London, 1987.
- [8] J. E. Strapasson. *Geometria discreta e codigos*. Tese (doutorado), Universidade Estadual de Campinas, 2007.
- [9] K. S. Williams. Integers of biquadratic fields. *Transactions of the American Mathematical Society*, 149:345–364, March 1970. Received by the editors March 16, 1970. Supported by National Research Council of Canada, Grant A-7233.