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

Algoritmos computacionais para geração de reticulados algébricos via Método de Krüskemper

Otávio Benicio Mirandola

Orientador: Prof. Dr. Agnaldo José Ferrari

Programa: Matemática Aplicada e Computacional

Presidente Prudente, setembro de 2021.

UNIVERSIDADE ESTADUAL PAULISTA

Faculdade de Ciências e Tecnologia de Presidente Prudente

Programa de Pós-Graduação em Matemática Aplicada e Computacional

Algoritmos computacionais para geração de reticulados algébricos via Método de Krüskemper

Otávio Benicio Mirandola

Orientador: Prof. Dr. Agnaldo José Ferrari

Dissertação apresentada ao Programa de Pós-Graduação em Matemática Aplicada e Computacional - POSMAC, da Faculdade de Ciências e Tecnologia da UNESP, campus Presidente Prudente, para a obtenção do título de Mestre em Matemática Aplicada.

Presidente Prudente, setembro de 2021.

M672a

Mirandola, Otávio Benicio
Algoritmos computacionais para geração de reticulados algébricos via método de Krüskemper / Otávio Benicio Mirandola. -- Presidente Prudente, 2021
106 p. : tabs., fotos

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Faculdade de Ciências e Tecnologia, Presidente Prudente
Orientador: Agnaldo José Ferrari

1. Reticulados. 2. Reticulados algébricos. 3. Distância produto mínima. 4. Teoria algébrica dos números. 5. Corpos de números. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Faculdade de Ciências e Tecnologia, Presidente Prudente. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

unesp

UNIVERSIDADE ESTADUAL PAULISTA

Câmpus de Presidente Prudente

CERTIFICADO DE APROVAÇÃO

TÍTULO DA DISSERTAÇÃO: Algoritmos computacionais para geração de reticulados algébricos via Método de Kruskemper

AUTOR: OTÁVIO BENICIO MIRANDOLA
ORIENTADOR: AGNALDO JOSÉ FERRARI

Aprovado como parte das exigências para obtenção do Título de Mestre em Matemática Aplicada e Computacional, pela Comissão Examinadora:

Prof. Dr. AGNALDO JOSÉ FERRARI (Participaçao Virtual)
Departamento de Matemática / Faculdade de Ciências de Bauru

Tatiana Miguel Rodrigues de Souza

Profa. Dra. TATIANA MIGUEL RODRIGUES DE SOUZA (Participaçao Virtual)
Departamento de Matemática / Faculdade de Ciências de Bauru

João E Strapasson

Prof. Dr. JOÃO ELOIR STRAPASSON (Participaçao Virtual)
Faculdade de Ciências Aplicadas / Universidade Estadual de Campinas

Presidente Prudente, 28 de setembro de 2021

Agradecimentos

Ao concluir este trabalho, agradeço:

À Deus, que me deu saúde e condições para seguir este caminho.

Aos meus pais, Benvina e José, por todo apoio, suporte e incentivo que permitiram me dedicar aos estudos durante todo o período de graduação e pós-graduação.

Aos meus irmãos e sobrinhos.

Ao meu orientador, Prof. Dr. Agnaldo José Ferrari, por todo o conhecimento compartilhado e ajuda prestada durante os períodos de iniciação científica e pós-graduação.

À amiga Amanda e ao amigo Isaque, pela convivência durante os cursos e atividades do programa de mestrado, pelas conversas e apoio durante esse período e além dele.

Às amigas Leandra e Thaynara, e ao amigo Micael, pela amizade e por todas as conversas de incentivo, sempre presentes mesmo à distância, em nome de quem agradeço à todos os amigos.

À todos os meus professores e professoras, da Educação Básica ao Ensino Superior, por minha formação intelectual e cívica.

Aos colegas de graduação e pós-graduação, pela boa convivência.

Aos funcionários do Departamento de Matemática da Faculdade de Ciências, da Unesp de Bauru, e do Programa de Pós-graduação em Matemática Aplicada e Computacional, da Faculdade de Ciências e Tecnologia, da Unesp de Presidente Prudente.

À banca examinadora.

À todos que contribuíram de alguma forma para a realização deste trabalho, direta ou indiretamente.

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

Que mesmo em face do maior encanto
Dele se encante mais meu pensamento.
Vinicius De Moraes

Resumo

Neste trabalho apresentamos um método para a construção de reticulados algébricos com diversidade máxima, no sentido de serem gerados através de mergulhos em corpos de números totalmente reais, que possuem importante aplicação na Teoria de Códigos. Neste sentido, apresentamos uma abordagem computacional para a construção de reticulados no espaco n-dimensional pelo método, particularmente para a geração de versões rotacionadas de reticulados conhecidos até a sexta dimensão.

Palavras-Chave: *reticulados; reticulados algébricos; distância produto mínima; Teoria algébrica dos números; Corpos de números.*

Abstract

In this work we present a method for the construction of algebraic lattices with maximum diversity, in the sense that they are generated by the embedding in totally real number fields, which have an important application in Code Theory. In this sense, we present a computational approach for the construction of lattices by this method, particularly for the generation of rotated versions of known lattices up to the sixth dimension.

Keywords: *lattices; algebraic lattices; Minimum product distance; Algebraic Number Theory; number fields*.

Sumário

Introdução

Reticulados algébricos possuem importante aplicação na Teoria da Informação, em particular em estudos onde constelações de sinais com estrutura de reticulados são utilizadas para transmissão de sinais sobre os canais Gaussiano e com desvanecimento do tipo Reyleigh.

Um canal de comunicação é um meio físico por onde uma informação é transmitida de uma fonte até um destinatário, e está sujeito a interferências, que geram distorções ou erros. Pela Teoria dos Códigos Corretores de Erros, essas distorções podem causar informações recebidas diferentes daquelas enviadas. Com isso, surge a necessidade de detectar erros e recuperar a mensagem enviada ao receptor construindo, assim, códigos com pequena probabilidade de erros.

Os canais mais usados na transmissão de sinais são: o Canal gaussiano branco (AWGN), em que predominam atenuações e atrasos na propagação do sinal, e o Canal Rayleigh com desvanecimento, caracterizado pela propagação por múltiplos percursos formados pela reflexão e/ou difração do sinal transmitido.

Constelações de sinais podem ser projetadas representando cada sinal como um ponto no espaço euclidiano n-dimensional. Com isso, o processo de projetar um conjunto de palavras-código pode ser reduzido a um problema geométrico de alocação de pontos em uma região de um espaço. Nesse sentido, os códigos construídos a partir de reticulados algébricos constituem uma das técnicas de alocação de pontos.

O problema de encontrar boas constelações de sinais para a transmissão em um canal com desvanecimento do tipo Rayleigh, se associarmos as constelações de sinais a empacotamentos reticulados, é que estas constelações tenham diversidade máxima. Quanto maior a diversidade e a distância produto mínima, menor será a probabilidade de erro neste tipo de canal.

Uma maneira de obter constelações eficientes para ambos os canais é buscar reticulados densos com diversidade máxima e distância produto mínima grande. Um interesse prático nesse tipo de construção é que tais constelações podem ser usadas na transmissão de dados entre um móvel e uma base ou entre um móvel e um satélite, através do mesmo sistema de modulação/demodulação. Devido ao fato de que reticulados obtidos via corpos de números totalmente reais possuem diversidade máxima, boas constelações de reticulados associadas a canais com desvanecimento do tipo Rayleigh podem ser encontradas.

Neste trabalho apresentamos um método para construção de reticulados baseado nos trabalhos de Taussky, Krüskemper e Oggier, que computa a matriz geradora de um reticulado integral, dada a sua matriz de Gram. Isso produz um reticulado algébrico, no sentido de que o reticulado é construído através dos mergulhos em um corpo de números totalmente real, que possui diversidade máxima.

Pelo método, existe o controle do discriminante do corpo e da ordem no anel dos inteiros algébricos, que impactam na distância produto mínima dos reticulados construídos, sendo este um parâmetro importante quando associamos um reticulado a uma constelação de sinais para transmissão via o canal com desvanecimento do tipo Rayleigh.

O presente projeto consiste no estudo de algoritmos computacionais para encontrar corpos com melhores discriminante e ordem no anel dos inteiros algébricos com o intuito de construir reticulados que representem constelações de sinais com boas performances para o canal mencionado. Para isto, foram utilizados os softwares Wolfram Mathematica e PARI/GP.

No capítulo 1, a partir das referências [1], [2] e [3], apresentamos os conceitos básicos e principais propriedades de reticulados e empacotamentos esféricos, com o objetivo de introduzir estes conceitos para leitores não familiarizados. Além disso, apresentamos os principais reticulados conhecidos na literatura, com suas principais propriedades.

No capítulo 2, fazendo uso das referências [4], [5], [6], [8] e [11], apresentamos os conceitos da Álgebra que servem de base para situar o leitor acerca da fundamentação algébrica utilizada, bem como para introdução da Teoria Algébrica dos Números, conteúdo do próximo capítulo. Neste sentido, são apresentados conceitos básicos e propriedades relativos a Teoria de Anéis e Corpos, Ideais e um estudo sobre Extensões de Corpos.

No capítulo 3, com base nas referências [4], [7], [9], [10] e [11], apresentamos os principais conceitos e propriedades da Teoria Algébrica dos Números, importantes para o desenvolvimento dos trabalhos, sendo base para a construção de reticulados algébricos. Neste sentido, apresentamos conceitos e resultados da Teoria de Galois, além dos importantes conceitos de Corpos de Números, Anéis dos Inteiros, e Módulo, Norma e Traço.

No capítulo 4, utilizando das referências [12] a [18], apresentamos de forma detalhada o método de Krüskemper para a construção de reticulados, objeto de nosso trabalho. Inicialmente, tendo em base a Teoria Algébrica dos Números, apresentamos os conceitos de Reticulados Algébricos e Reticulados Ideais, bem como diversidade do reticulado e distância produto mínima. A partir disto, apresentamos os Teoremas de Taussky e Krüskemper, que fundamentam o método objeto deste trabalho. Por fim, apresentamos o algoritmo para a construção de reticulados algébricos, com base no trabalho de Oggier, a partir dos teoremas acima citados.

No capítulo 5 apresentamos os resultados obtidos a partir do método estudado, utilizando como ferramentas os softwares Wolfram Mathematica e PARI/GP. Após isso, finalizamos com uma discussão acerca destes resultados.

CAPÍTULO

1

Teoria dos Reticulados

Neste capítulo são apresentados principais conceitos e propriedades relativos ao estudo dos Reticulados e empacotamento reticulados, objeto de estudo do presente trabalho. Além disso, apresentamos os principais reticulados conhecidos na literatura e suas principais características.

1.1 Reticulados

Nesta seção são apresentados os conceitos básicos referentes aos reticulados, com suas principais propriedades.

Definição 1.1.1. *Seja $\{v_1, v_2, \cdots, v_m\}$ um conjunto de vetores linearmente independente do espaço vetorial $\mathbb{R}^n$, com $m \leq n$. O subconjunto do $\mathbb{R}^n$*

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

é chamado um reticulado de posto m, de modo que $\{v_1, v_2, \cdots, v_m\}$ é uma base do reticulado Λ.

Então, de acordo com a definição, ao variar os coeficientes α_i no conjunto dos inteiros, um reticulado no $\mathbb{R}^n$ é um conjunto infinito de pontos dispostos de maneira regular no espaço n-dimensional. Um reticulado $\Lambda \subset \mathbb{R}^n$ é um subgrupo do grupo abeliano $(\mathbb{R}^n, +)$. De fato, tomando vetores $u, w \in \Lambda$, temos que

$$u = \sum_{i=1}^{m} \alpha_i v_i;\ \alpha_i \in \mathbb{Z}$$

e

$$w = \sum_{i=1}^{m} \beta_i v_i;\ \beta_i \in \mathbb{Z}$$

Então temos

$$u + (-w) = \sum_{i=1}^{m} \alpha_i v_i + \sum_{i=1}^{m} -\beta_i v_i = \sum_{i=1}^{m} (\alpha_i - \beta_i) v_i$$

Como $(\alpha_i - \beta_i) \in \mathbb{Z}$, segue que $(u + (-w)) \in \Lambda$, o que mostra que Λ é subgrupo de $(\mathbb{R}^n, +)$.

Definição 1.1.2. *Seja $\Lambda \subset \mathbb{R}^n$ um reticulado com base $B = \{v_1, v_2, \cdots, v_m\}$. Definimos a região fundamental ou paralelotopo fundamental de Λ em relação à base B como o conjunto*

$$P_B = \left\{ x \in \mathbb{R}^n; x = \sum_{i=1}^{n} \alpha_i v_i; 0 \leq \alpha < 1 \right\}.$$

Geometricamente, a região fundamental é a região compreendida entre os vetores da base do reticulado, formando um paralelotopo com esses vetores. Desse modo, a região fundamental depende da base do reticulado escolhida. Bases diferentes determinam regiões diferentes.

Quando transladamos a região fundamental através de todos os pontos do reticulado, a união das cópias da região cobre todo o espaço euclidiano, de modo que cada cópia contem um único ponto do reticulado. Dessa forma, dizemos que a região fundamental "ladrilha"o espaço.

Definição 1.1.3. *Seja* $\{v_1, v_2, ..., v_m\}$ *uma base para o reticulado* Λ *tal que* $v_i = (v_{i1}, ..., v_{in})$, *para* $i = 1, ..., m$. *A matriz* $M = (v_{ij})$ *é chamada uma matriz geradora para o reticulado* Λ.

Desse modo, a matriz geradora é formada pelos vetores da base do reticulado, dispostos em linha ou coluna. Em nosso trabalho, convencionamos a disposição dos vetores em linhas na matriz. Se M é uma matriz geradora para o reticulado Λ, este pode ser escrito na forma matricial como

$$\Lambda = \{xM;\ x \in \mathbb{Z}^n\}.$$

A matriz geradora de um reticulado não é única. Isto decorre do fato da matriz geradora ter como entradas os elementos dos vetores da base do reticulado, dispostos em linha ou coluna. Como o reticulado não possui uma única base, segue que sua matriz geradora também não é única. A seguir, é apresentada a condição necessária e suficiente para que duas matrizes sejam geradoras de um mesmo reticulado.

Proposição 1.1.4. *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.*

Definição 1.1.5. *Seja M uma matriz geradora para o reticulado* Λ. *A matriz* $G = MM^t$, *em que t denota uma transposição, é chamada de matriz de Gram para o reticulado* Λ.

Como a matriz geradora M contém os vetores $v_1, v_2, ..., v_m$, vetores da base do reticulado, então a (i, j)-ésima entrada da matriz G é o produto interno $\langle v_i, v_j \rangle$. Então, as entradas da matriz de Gram G guardam informações métricas importantes, pois referem-se às posições relativas dos vetores da base do reticulado. Nessas informações podemos identificar, por exemplo, ortogonalidade entre vetores da base, bem como o comprimento desses vetores.

Definição 1.1.6. *O determinante de um reticulado* Λ *é definido como o determinante da matriz de Gram de* Λ, *ou seja, det(*Λ*) = det(G).*

O determinante de um reticulado independe da matriz geradora escolhida. De fato, pode ser provado que se M é uma matriz geradora de Λ com matriz de Gram $G = MM^t$ e M' outra geradora de Λ com matriz de Gram $G' = M'M'^t$, então $det(G) = det(G') = det(\Lambda)$. Como $G = MM^t$, se a matriz geradora M for quadrada, então $det(\Lambda) = det(G) = det(M)^2$. Nesse caso o reticulado é dito de posto completo.

Definição 1.1.7. *O volume do reticulado* Λ *é definido como* $Vol(\Lambda) = \sqrt{det(\Lambda)}$. *Esse é o volume da região fundamental do reticulado* Λ.

Bases diferentes do reticulado determinam o mesmo volume, pois duas matrizes geram o mesmo reticulado quando diferem por um produto de uma matriz inversível com entradas inteiras e determinante ± 1. Além disso, vimos que o determinante do reticulado independe da matriz geradora escolhida. Assim, o volume independe da base do reticulado em questão.

Se B é uma matriz de ordem n com entradas inteiras, um *sub-reticulado* de Λ é definido por

$$\Lambda' = \{\alpha BM;\ \alpha \in \mathbb{Z}^n\}$$

, em que M é a matriz geradora de Λ. Como um reticulado Λ é um grupo aditivo abeliano do $\mathbb{R}^n$, um sub-reticulado Λ' é subgrupo de Λ.

Definição 1.1.8. *Seja Λ um reticulado no $\mathbb{R}^n$. Definimos o reticulado dual de Λ, denotado por Λ^*, por*

$$\Lambda^* = \{x \in \mathbb{R}^n; \langle x, v\rangle \in \mathbb{Z}, \forall v \in \Lambda\}$$

Ou seja, o reticulado dual de um reticulado $\Lambda \subset \mathbb{R}^n$ é o reticulado composto pelo conjunto de todos os vetores do espaço n-dimensional tais que o produto interno desses vetores com todos os pontos de Λ resulta em um número inteiro. Um reticulado é denominado *isodual* quando ele é geometricamente congruente ao seu dual. Em outras palavras, um reticulado é isodual se ele difere de seu dual somente, possivelmente, por uma rotação ou reflexão.

Dois reticulados são *equivalentes* na métrica euclidiana se um deles pode ser obtido do outro através de uma composição de uma rotação ou reflexão com multiplicação por um fator de escala. Ou seja, os dois reticulados Λ_1 e Λ_2, com matrizes geradoras M_1 e M_2, respectivamente, são equivalentes se, e só se,

$$M_1 = \sqrt{c}AM_2R,$$

de modo que A é a matriz mudança de base, com entradas inteiras e determinante ± 1, R é uma matriz ortogonal e $\sqrt{c}$ é o fator de escala, com $c \in \mathbb{R}$.

1.2 Empacotamento esférico

Um *empacotamento esférico* é uma distribuição de esferas de mesmo raio no espaço $\mathbb{R}^n$ de modo que a intersecção de quaisquer duas dessas esferas tenha no máximo um ponto. Podemos nos referir ao empacotamento esférico simplesmente como empacotamento no $\mathbb{R}^n$. Dessa forma, um empacotamento no $\mathbb{R}^n$ é uma distribuição de esferas idênticas no espaço n-dimensional de modo que essas esferas não se sobreponham e tenham, no máximo, um ponto de intersecção tomando-se duas delas.

De acordo com Conway and Sloane [1], o problema clássico do empacotamento esférico consiste em encontrar um arranjo de esferas idênticas no $\mathbb{R}^n$ de modo que a fração do espaço coberta pelas esferas seja a maior possível.

Definição 1.2.1. *Um empacotamento reticulado é um empacotamento no $\mathbb{R}^n$ tal que o conjunto dos centros das esferas formam um reticulado $\Lambda \subset \mathbb{R}^n$. Dizemos também, nesse caso, que o empacotamento é associado ao reticulado Λ.*

Ao estudarmos os empacotamentos reticulados, o interesse está em determinar o empacotamento associado a um reticulado Λ em que as esferas tenham raio máximo. Esse raio é conhecido como raio de empacotamento e definido a seguir.

Definição 1.2.2. *O raio de empacotamento de um reticulado Λ é o maior raio ρ tal que $B_\rho(u) \cap B_\rho(v) = \emptyset$, $\forall u, v \in \Lambda$, com $u \neq v$.*

Ou seja, o raio de empacotamento é o maior raio tal que, para quaisquer dois pontos do reticulado Λ, as bolas abertas com raio ρ centradas nesses pontos não tenham elementos em comum. Podemos determinar o valor do raio de empacotamento através da norma mínima de um vetor não nulo do reticulado, que é definida a seguir.

Definição 1.2.3. *A norma mínima η de um reticulado Λ é definido por*

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

Dessa forma, a norma mínima tem o mesmo valor do quadrado da distância mínima entre dois pontos do reticulado. Assim, fica definido o valor do raio de empacotamento como metade do quadrado da distância mínima entre os pontos do reticulado, ou seja, $\rho = \sqrt{\eta}/2$. Outro conceito importante relacionado aos empacotamentos, em particular o empacotamento reticulado, é sua densidade, definida a seguir.

Definição 1.2.4. *Dado um empacotamento no $\mathbb{R}^n$ associado a um reticulado Λ, é definida sua densidade de empacotamento como sendo a proporção do espaço euclidiano n-dimensional coberta pela união das esferas do empacotamento.*

Dado um empacotamento no $\mathbb{R}^n$ associado ao reticulado Λ, com base $B = \{v_1, v_2, \cdots, v_n\}$ e raio de empacotamento ρ, a densidade de empacotamento de Λ é dada por

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

em que $B(\rho)$ denota a esfera de centro na origem e raio ρ na dimensão n. Assim, a densidade de empacotamento é definida como a razão entre o volume da esfera de raio ρ e o volume do reticulado Λ.

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

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

Deste modo, podemos reduzir o problema ao estudo de um outro parâmetro, chamado *densidade de centro*, dado por

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

e, portanto, a densidade de empacotamento de Λ é

$$\Delta(\Lambda) = Vol(B(1))\delta(\Lambda),$$

ou seja, o produto entre o volume da esfera unitária de dimensão n e a densidade de centro de Λ.

Ao aumentarmos o raio das esferas de um empacotamento no $\mathbb{R}^n$ associado a um reticulado Λ além do raio de empacotamento, as esferas se sobrepõem. Desse modo, podemos cobrir todo o espaço gerado pelo reticulado Λ, desde que esse novo raio seja suficientemente grande. O *raio de cobertura*, denotado por R, no $\mathbb{R}^n$ associado a um reticulado Λ é o menor raio associado às esferas que resulta em uma cobertura total do espaço gerado pelo reticulado Λ.

Em outras palavras, o raio de cobertura é o menor raio, aumentado além do raio de empacotamento, que faz com que as esferas sobrepostas "cubram" todo o espaço gerado pelo reticulado. Para mensurar qual seria essa melhor cobertura, utilizamos uma taxa análoga à densidade de empacotamento, definida a seguir.

Definição 1.2.5. *Considerando um arranjo de esferas de raio R centradas nos pontos do reticulado Λ que cobrem todo o $\mathbb{R}^n$, definimos a densidade de cobertura como*

$$\Theta = \frac{Vol(B(R))}{Vol(\Lambda)} = \frac{Vol(B(1))R^n}{Vol(\Lambda)}.$$

As densidades de empacotamento e cobertura satisfazem a seguinte relação:

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

ou seja, pelas definições dessas densidades, vemos que o volume de uma esfera com raio de empacotamento ρ é sempre menor ou igual ao volume do reticulado, enquanto que o volume da esfera com raio de cobertura R é sempre maior ou igual ao volume do reticulado.

Enquanto o problema do empacotamento esférico é determinar os empacotamentos mais densos, aqueles que cobrem a maior proporção do espaço, por esferas que se tangenciam, o problema da cobertura reside em determinar os empacotamentos menos densos por esferas que cobrem todo o espaço, de modo que a região de esferas sobrepostas seja a menor possível. Desse modo, vemos que quanto mais próximas de 1, melhor são as densidades, tanto de empacotamento quanto de cobertura.

O *"kissing number"* τ, ou *número de vizinhos*, de um empacotamento esférico é o número de esferas idênticas que tocam uma outra esfera idêntica central. Em outras palavras, fixada uma esfera do empacotamento, o kissing number é o número de esferas que tem um ponto de intersecção com essa esfera central.

O estudo desse parâmetro busca determinar qual o número máximo de esferas idênticas que tangenciam uma outra esfera idêntica central. Em um empacotamento reticulado, o kissing number é sempre o mesmo para todas as esferas, mas em um empacotamento qualquer isso não é necessariamente válido.

1.3 Principais reticulados conhecidos

Nesta seção apresentamos alguns dos principais reticulados conhecidos na literatura, bem como suas principais propriedades, já conhecidas.

1.3.1 Reticulado A_n

É conhecido como o reticulado no hiperplano. É definido por, para $n \geq 1$,

$$A_n = \left\{(x_0, x_1, ..., x_n) \in \mathbb{Z}^{n+1}; x_0 + x_1 + ... + x_n = 0\right\}$$

Desse modo, A_n é um reticulado n-dimensional no espaço euclidiano $\mathbb{R}^{n+1}$. Ou seja, A_n está contido no hiperplano $\sum_{i=0}^{n} x_i = 0$. Uma de suas matrizes geradoras é dada por:

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

Colocando as principais propriedades estudadas para o reticulado, temos $det(A_n) = n+1$, norma mínima $\eta = 2$, raio de empacotamento $\rho = \sqrt{2}/2$, com kissing number $\tau = n(n+1)$, densidade de centro $\delta = \frac{2^{-n/2}}{\sqrt{n+1}}$ e densidade de empacotamento

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

1.3.2 Reticulado D_n

O reticulado D_n, em que $n \geq 3$, é definido por

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

Uma matriz geradora é dada por

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

Além disso, temos $det(D_n) = 4$, $\eta = 2$, $\rho = \sqrt{2}/2$, $\tau = 2n(n-1)$, densidade de centro $\delta = 2^{-(n+2)/2}$ e densidade de empacotamento

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

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

1.3.3 Reticulado $\mathbb{Z}^n$

O reticulado $\mathbb{Z}^n$, para $n \geq 2$, é definido por

$$\mathbb{Z}_n = \{(x_1, x_2, ..., x_n); x_i \in \mathbb{Z}\}.$$

Possui uma matriz geradora $M = I_n$ (matriz identidade de ordem n). Além disso, $\eta = 1$, $\rho = 1/2$, $\tau = 2n$, densidade de centro $\delta = 2^{-n}$ e densidade de empacotamento

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

1.3.4 Reticulado E_8

O reticulado E_8 é um reticulado de dimensão 8, que é dado por

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

Assim, os elementos do reticulado E_8 são vetores de dimensão 8 tal que as coordenadas dos vetores são números inteiros ou inteiros acrescidos de 1/2, além de a soma das coordenadas dos vetores ser um número inteiro par.

Uma de suas matrizes geradoras é dada por

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

Além disso, temos $det(E_8) = 1$, $\eta = 2$, $\rho = \sqrt{2}/2$, $\tau = 240$, $\delta(E_8) = 1/16$ e $\Delta(E_8) = \pi^4/384$. Esse é o reticulado de maior densidade conhecida no espaço euclidiano $\mathbb{R}^8$.

1.3.5 Reticulado E_7

O reticulado E_7 é um reticulado 7-dimensional, definido por

$$E_7 = \{(x_1, x_2, ..., x_8) \in E_8; x_1 + x_2 + ... + x_8 = 0\},$$

ou seja, E_7 é um reticulado de dimensão 7 no espaço 8-dimensional e, além disso, é um sub-reticulado de E_8.

Uma das matrizes geradoras de E_7 é dada por

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

Além disso, temos $det(E_7) = 2$, $\eta = 2$, $\rho = \sqrt{2}/2$, $\tau = 126$, $\delta(E_7) = 1/16$ e $\Delta(E_7) = \pi^3/105$. Esse é o reticulado com maior densidade conhecida na dimensão 7.

1.3.6 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

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

Uma matriz geradora de E_6 é dada por

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

Para esse reticulado, temos $det(E_6) = 3$, $\eta = 2$, $\rho = \sqrt{2}/2$, $\tau = 72$, $\delta(E_6) = 1/8\sqrt{3}$ e $\Delta(E_6) = \pi^3/48\sqrt{3}$. Esse é o reticulado com maior densidade conhecida no espaço 6-dimensional.

1.3.7 Reticulado K_{12}

O reticulado K_{12}, também conhecido como reticulado de Coxeter-Todd, pois foi descrito por esses em 1954, é um reticulado 12-dimensional. Uma de suas matrizes geradoras é dada por

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

Temos que $det(K_{12}) = 729$, $\eta = 4$, $\rho = 1$, $\tau = 756$, $\delta(K_{12}) = 1/27$ e $\Delta(K_{12}) = \pi^6/19440$. O reticulado K_{12} é o reticulado com maior densidade conhecida na dimensão 12.

1.3.8 Reticulado Λ_{16}

O reticulado Λ_{16}, também conhecido como reticulado de Barnes-Wall, descrito por esses em 1959, é um reticulado no espaço 16-dimensional. Uma matriz geradora é dada por

$$M = \frac{1}{\sqrt{2}} \begin{pmatrix}
4 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 0 & 0 & 0 & 1 \\
0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}.$$

Além disso, temos $det(\Lambda_{16}) = 256$, $\eta = 4$, $\rho = 1$, $\tau = 4320$, $\delta(\Lambda_{16}) = 1/16$ e $\Delta(\Lambda_{16}) = \pi^8/16(8!)$. O reticulado Λ_{16} é o reticulado mais denso conhecido em dimensão 16.

1.3.9 Reticulado Λ_{24}

O reticulado Λ_{24} é um reticulado no espaço 24-dimensional e foi descrito por Leech em 1965. Uma de suas matrizes geradoras é dada por

$$M = \frac{1}{\sqrt{8}} \begin{pmatrix}
8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 2 & 0 & 2 & 0 & 0 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 2 & 2 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\
0 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 \\
-3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}.$$

Além disso, temos que $det(\Lambda_{24}) = 1$, $\eta = 4$, $\rho = 1$, $\tau = 196560$, $\delta(\Lambda_{24}) = 1$ e $\Delta(\Lambda_{24}) = \pi^{12}/12!$. O reticulado Λ_{24} é o reticulado de maior densidade conhecida em dimensão 24.

CAPÍTULO

2

Álgebra: conceitos básicos

Neste capítulo são apresentados os conteúdos algébricos estudados, em que foram explorados os conceitos da Teoria algébrica dos números. Os conteúdos abordados são de fundamental importância em nossa pesquisa, onde apresentaremos um método para a construção de reticulados algébricos, ou seja, reticulados construídos através de mergulhos em um corpo de números totalmente real, com diversidade máxima. Neste sentido, uma teoria algébrica sólida se faz extremamente necessária.

2.1 Grupos

Definição 2.1.1. *Dado um conjunto G, não vazio, munido de uma operação* $* : G \times G \to G$*, dizemos que G é um grupo, denotado por* $(G,*)$*, se são satisfeitas as seguintes condições, dados quaisquer* $a,b,c \in G$

1. *a operação* $*$ *é associativa, ou seja,* $(a*b)*c = a*(b*c)$*,*
2. *existe um* $e \in G$ *tal que* $a*e = e*a = a$*, para qualquer* $a \in G$*, onde e é denominado elemento neutro para a operação* $*$*,*
3. *para todo* $a \in G$*, exite* $a' \in G$ *tal que* $a*a' = a'*a = e$*, onde* a' *é denominado elemento simétrico de a.*

Se, além disso, valer que $a*b = b*a$, quaisquer que sejam $a,b \in G$, dizemos que G é um grupo comutativo ou abeliano. Por uma questão de simplificação, denotaremos um grupo apenas por seu conjunto, omitindo a operação, a menos que necessário. O número de elementos do grupo G é chamado de ordem de G, denotado por $o(G)$. Se esse número é finito, dizemos que G é um grupo finito. Quando um subconjunto $H \subseteq G$ é também um grupo em relação à $*$, dizemos que H é um *subgrupo* de G.

Definição 2.1.2. *Dado um grupo G e um elemento* $a \in G$*, a ordem (ou período) de a é dada pelo menor inteiro positivo m tal que* $a^m = e_G$*, onde* e_G *representa o elemento neutro de G em relação à sua operação. Se não existe tal inteiro m, dizemos que o elemento tem ordem infinita.*

Definição 2.1.3. *Dados um grupo* $(G,*)$*, H subgrupo de G e* $x \in G$*, o conjunto* $H*x = \{h*x;\ h \in H\}$ *é denominado classe lateral à direita de H em G.*

Da mesma forma, $x*H = \{x*h;\ h \in H\}$ é uma classe lateral à esquerda de H em G. O número de classes laterais à direita (ou esquerda) de H em G é chamado de índice de H em G, e

independe do elemento $x \in G$ tomado.

A seguir definimos uma classe especial de subgrupos, que, como veremos pelos resultados seguintes, se relacionam com a noção de classe lateral.

Definição 2.1.4. *Um subgrupo N de um grupo $(G,*)$ é dito subgrupo normal de G se, dados quaisquer $g \in G$ e $n \in N$, temos $g*n*g' \in N$.*

Podemos reescrever esta definição colocando $g*N*g' = \{g*n*g';\ n \in N\}$. Então N é um subgrupo normal de G se, e só se, $g*N*g' \subseteq N$, para todo $g \in G$. Com isso, chegamos ao seguinte resultado

Lema 2.1.5. *N é subgrupo normal do grupo $(G,*)$ se, e somente se, $g*N*g' = N$.*

Vimos pela definição que $g*N*g' \subseteq N$. Portanto basta verificar que $N \subseteq g*N*g'$. Omitiremos essa prova, que pode ser vista em [5]. Pelo resultado seguinte, temos a relação entre a igualdade de classes laterais à esquerda e à direita com a noção de subgrupo normal. A justificativa pode ser consultada em [5].

Lema 2.1.6. *Um subgrupo $N \in G$ é subgrupo normal de G se, e somente se, toda classe lateral à esquerda de N em G coincide com uma classe lateral à direita de N em G.*

Dados subconjuntos A e B de um grupo G, definimos $A*B$ como o conjunto $A*B = \{x \in G;\ x = a*b, a \in A, b \in B\}$. Com isso, é fácil verificar que, se $H \subseteq G$ é um subgrupo de G, então $H*H = H$. Então, suponha que $N \subseteq G$ é um subgrupo normal de G e que $a,b \in G$. Como N é normal em G, temos

$$N*aN*b = N*(a*N)*b = N*(N*a)*b = (N*N)*a*b = N*a*b,$$

ou seja, a operação entre duas classes laterais à direita resulta em uma classe lateral à direita. A partir disto, temos o seguinte resultado

Lema 2.1.7. *Um subgrupo $N \subseteq G$ é subgrupo normal de G se, e somente se, o produto de duas classes laterais à direita de N em G é também uma classe lateral à direita de N em G.*

Com a operação entre classes laterais bem definida, podemos definir o conjunto das classes à direita de um subgrupo N no grupo G. Denotamos por G/N este conjunto. por uma simples verificação das propriedades que definem um grupo, com a operação entre classes laterais dada acima, temos o seguinte resultado

Teorema 2.1.8. *Sejam G um grupo e N um subgrupo normal de G. Então G/N é também um grupo, denominado grupo quociente de G por N. Se G é finito, a ordem de G/N é dada por $o(G/N) = \frac{o(G)}{o(N)}$.*

A ordem do grupo G/N é também chamada *índice de H em G*, denotada por $(G:N)$, o número de classes laterais módulo N em G. O teorema acima pode ser reescrito como o Teorema de Lagrange, que nos diz que $o(G) = o(N) \cdot (G:N)$.

Definição 2.1.9. *Dizemos que um grupo multiplicativo G é cíclico se, para algum $a \in G$, temos $G = \{a^m;\ m \in \mathbb{Z}\}$. Se G é um grupo aditivo, então será cíclico se, dado $a \in G$, temos $G = \{m \cdot a;\ m \in \mathbb{Z}\}$. Em ambos os casos, o elemento a é chamado gerador do grupo G.*

Um conceito importante da Álgebra é o de homomorfismo, uma aplicação de uma estrutura algébrica em outra estrutura algébrica semelhante, que preserva as respectivas operações e, com isso, suas estruturas. Definimos então este conceito para grupos, como segue.

Definição 2.1.10. *Dados dois grupos $(G,*)$ e $(H,\circledast)$, uma aplicação $\varphi : G \longrightarrow H$ é dita um homomorfismo se, para quaisquer $a,b \in G$, tivermos $\varphi(a*b) = \varphi(a) \circledast \varphi(b)$.*

Se φ for um homomorfismo injetor, recebe o nome de monomorfismo de G em H. Quando φ é sobrejetor, recebe o nome de epimorfismo de G em H. Quando um homomorfismo é ao mesmo tempo injetor e sobrejetor, ou seja, uma bijeção, temos um importante caso de homomorfismo, definido a seguir.

Definição 2.1.11. *Dados dois grupos $(G,*)$ e $(H,\circledast)$ são chamados isomorfos se existe um homomorfismo bijetor entre eles, chamado isomorfismo de G em H. Neste caso, utilizamos a notação $G \approx H$.*

A principal característica dos isomorfismos é que, se dois grupos são isomorfos, então eles são "iguais", em certo aspecto. Dois grupos isomorfos só se diferem na natureza de seus elementos, mas a estrutura da operação em um grupo é idêntica à estrutura de seu grupo isomorfo. Com isso, conhecendo a operação em um grupo, podemos transpor esta de forma análoga ao outro grupo, o que justifica sua grande importância.

Cabe ressaltar que se existe um isomorfismo φ de um grupo G em um grupo H então, por sua característica bijetora, existe um isomorfismo de H em G, dado por φ^{-1}, a aplicação inversa de φ.

Antes de apresentar o próximo resultado, precisamos definir o núcleo de um homomorfismo.

Definição 2.1.12. *Dado um homomorfismo φ de G em H, o núcleo de φ, também chamado de Kernel de φ, é definido como o conjunto $Ker_\varphi = \{x \in G;\ \varphi(x) = e_H\}$, em que e_H denota o elemento neutro de H.*

O núcleo de um homomorfismo nunca é vazio, pois $\varphi(e_G) = e_H$, ou seja, $e_G \in Ker_\varphi$. Além disso, pode ser provado que se $\varphi : G \longrightarrow H$ é um homomorfismo com núcleo K, então K é um subgrupo normal de G. A prova pode ser encontrada em [5]. Com isso, podemos enunciar o seguinte teorema, cuja demonstração será omitida, podendo ser consultada em [5].

Teorema 2.1.13. *Dado um homomorfismo de grupos $\varphi : G \longrightarrow H$ sobrejetor com núcleo K, temos que $G/K \approx H$.*

Este resultado é importante, pois nos diz exatamente como são os grupos que são imagens de um certo grupo, via homomorfismo sobrejetor, ou seja, são dados na forma G/K, onde K é o núcleo do homomorfismo e subgrupo normal em G. Por outro lado, para todo subgrupo normal de G, G/N é uma imagem homeomorfa de G. Existe então uma correspondência biunívoca entre imagens homomorfas de G e subgrupos normais de G.

Apresentamos agora um caso especial de monomorfismos, aqueles aplicados de um grupo nele mesmo, muito importantes posteriormente quando tratarmos do grupo de Galois, tópico de importância central neste estudo. Nesse sentido, definimos

Definição 2.1.14. *Um monomorfismo sobrejetor de um grupo G em si mesmo é chamado de automorfismo de G.*

Dado esse caso particular de homomorfismo, faremos então uma construção de modo a obter um grupo formado por automorfismos de um grupo G. Para isso, sejam $A(G)$ o conjunto de todas as aplicações bijetoras de G nele próprio e $I : G \longrightarrow G$ uma aplicação que associa à cada elemento de G ele mesmo, ou seja, $Ix = x$, para todo $x \in G$. É fácil verificar que $A(G)$, com a operação de composição de aplicações, é um grupo e que a aplicação I definida acima é seu

elemento neutro.

Denotando então por $\mathscr{A}(G)$ o conjunto de todos os automorfismos de G, é evidente que este conjunto é não-vazio, pois $I \in \mathscr{A}(G)$. Pode ser mostrado que $\mathscr{A}(G)$ é um subgrupo de $A(G)$. Uma justificativa detalhada para isto pode ser encontrada em [5]. Desse modo, temos os seguinte resultado.

Proposição 2.1.15. *Se G é um grupo, então o conjunto $\mathscr{A}(G)$ dos automorfismos de G é também um grupo.*

2.2 Anéis e Corpos

Nesta seção apresentamos um outro tipo de estrutura algébrica, os anéis. Veremos que, apesar de certas semelhanças em conceitos e resultados, os anéis são estruturas diferentes dos grupos, a começar pela sua característica bioperacional. Agora definimos sobre duas operações, as quais chamamos adição e multiplicação.

Apesar dessa principal diferença, é possível fazer analogias aos conceitos vistos, como subgrupo normal, classes laterais, grupo quociente e homomorfismos, também para os anéis. Faremos essas analogias, trazendo os conceitos e resultados mais significativos para nosso estudo.

Veremos também um caso especial de anel, de grande relevância para este estudo. Começamos, então, definindo

Definição 2.2.1. *Seja A um conjunto não vazio munido de duas operações $\cdot : A \times A \to A$ e $+ : A \times A \to A$, chamadas multiplicação e adição, respectivamente. A é dito um anel, denotado por $(A, +, \cdot)$ se são satisfeitas as seguintes condições:*

1. *$(A, +)$ é um grupo abeliano,*
2. *a multiplicação é associativa, ou seja, para quaisquer $a, b, c \in A$ vale que $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,*
3. *a multiplicação é distributiva em relação a adição, ou seja, para quaisquer $a, b, c \in A$, vale $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(b + c) \cdot a = b \cdot a + c \cdot a$.*

Denotaremos, salvo quando necessário, um anel por A, omitindo as operações que o definem, deixando subentendido sua adição e multiplicação. Além disso, escreveremos, para simplificar a notação, a multiplicação $a \cdot b$ como ab.

Se, além das propriedades acima, valer que $ab = ba$, para todo a e b, dizemos que A é um anel comutativo. Se existe o elemento neutro para a multiplicação, ou seja, se existe $1 \in A$ tal que $1 \cdot a = a \cdot 1 = a, \forall a \in A$, dizemos que A é um anel com unidade 1. Se $1_A = 0_A$, então este é o único elemento de A, que recebe o nome de anel trivial. Trabalharemos, em geral, com anéis comutativos com unidade.

Um subconjunto $S \subseteq A$ de um anel A é um *subanel* de A se S é fechado para as operações que definem A e é também um anel em relação a estas operações. Um subconjunto $S \neq \emptyset$ será um subanel de A se, e somente se, dados $x, y \in S$, valer que $x - y \in S$ e $xy \in S$.

É simples verificar que qualquer intersecção de subanéis de um anel A é também um subanel de A. Com isso, podemos definir

Definição 2.2.2. *Dado um subconjunto M de um anel A, definimos o subanel de A gerado por M como a intersecção*

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

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 A que contêm 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*.

Um elemento $x \in A$ é dito invertível no anel A se existe $y \in A$ tal que $xy = 1$. O conjunto dos elementos invertíveis de um anel A, denotado por U_A, é um grupo comutativo em relação à multiplicação. Um caso especial de anel, objeto de importância central em nosso estudo, é definido a seguir.

Definição 2.2.3. *Se K é um anel comutativo com unidade, dizemos que K é um corpo se para todo $0 \neq x \in K$, existe $y \in K$ tal que $xy = 1$, ou seja, K é um corpo se $U_K = K \setminus \{0\}$.*

Um subconjunto de um corpo é um *subcorpo* se ele é também um corpo. Veremos ao longo desta seção resultados importantes relativos aos corpos.

De mesmo modo que definimos para os subanéis, a intersecção de subcorpos de um corpo K é também um subcorpo de K. Assim, dado um subconjunto $P \subseteq K$, o *subcorpo de K gerado por P* é definido pela intersecção $\cap K'$, com $K' \in J_P$, tal que J_P representa o conjunto dos subcorpos de K que contém 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*.

Definição 2.2.4. *Se A é um anel comutativo, então $0 \neq a \in A$ é um divisor de zero se existe $0 \neq b \in A$ tal que $ab = 0$. Um anel A que não possui divisores de zero é chamado de domínio, ou anel de integridade. Ou seja, A é um domínio se, para todos $x, y \in A$ vale que se $xy = 0$, então $x = 0$ ou $y = 0$.*

Quando A é um anel não-trivial, nenhum elemento invertível de A é um divisor de zero em A. Portanto todo corpo é um domínio.

O motivo desta distinção é que nem todo anel é um domínio. De fato, tomando o conjunto dos inteiros mod 6, ou seja, o conjunto das classes de resto módulo 6, dado por $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. Nesse conjunto, temos $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$. Ou seja, $\mathbb{Z}_6$ não é um domínio. Na verdade, o anel $\mathbb{Z}_m$ só será um domínio se, e só se, m for um número primo, fato simples de ser verificado.

Podemos definir para anéis, assim como fizemos para grupos, o conceito de homomorfismo. Relembramos que um homomorfismo entre grupos é definido como uma aplicação que preserva suas operações, ou seja, $\varphi(a * b) = \varphi(a) * \varphi(b)$. Então, para o caso de anéis, é natural definirmos da seguinte forma análoga.

Definição 2.2.5. *Uma aplicação ϕ de um anel A em um anel R será um homomorfismo de anéis se forem satisfeitas, para quaisquer $a, b \in A$,*

1. $\phi(a+b) = \phi(a) + \phi(b)$,
2. $\phi(ab) = \phi(a)\phi(b)$.

Cabe ressaltar que, apesar de utilizadas as mesmas notações, as operações referentes aos dois anéis podem ser diferentes. Desse modo, as operações presentes no lado esquerdo das igualdades acima se referem ao anel A, enquanto as operações do lado esquerdo se referem ao anel R.

Do mesmo modo que definimos para grupos, se um homomorfismo de anéis é uma aplicação injetora, recebe o nome de monomorfismo, caso seja sobrejetora, recebe o nome de epimorfismo. No caso de uma bijeção, temos o caso especial, definido a seguir.

Definição 2.2.6. *Dois anéis A e B são isomorfos se existe um homomorfismo bijetor entre eles, ou seja, um isomorfismo de anéis.*

As mesmas considerações feitas para grupos isomorfos podem ser transpostas de forma integral para anéis. Ou seja, dois grupos isomorfos são considerados idênticos em suas estruturas, salvo a natureza de seus elementos. Portanto, isomorfismos são importantes objetos de relação entre anéis.

Definimos o núcleo de um homomorfismo de grupos como o conjunto dos elementos do grupo domínio da aplicação que são levados ao elemento neutro do segundo grupo. Como não podemos garantir a existência da unidade 1, a definição mais natural de um núcleo para o caso de um homomorfismo $\phi : A \longrightarrow B$ de anéis é dada pelo conjunto $Ker_\phi = \{x \in A | \phi(x) = 0_B\}$. Como mencionamos anteriormente, Ker_ϕ é um subgrupo de A em relação à adição e, além disso, vale que se $a \in Ker_\phi$ e $b \in B$, então $ab, ba \in Ker_\phi$ [5].

Uma propriedade importante dos anéis é sua característica. Para defini-la, utilizamos a ordem de um elemento do anel, considerada sobre seu grupo aditivo. Então, relembrando, 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. A justificativa pode ser consultada em [4]. Isto posto, definimos

Definição 2.2.7. *A característica de um anel A é dada por*

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

chamadas característica zero e característica positiva, respectivamente.

Todo subanel de A tem a mesma característica de A. Além disso, se A for um domínio, então $car(A) = 0$ ou $car(A) = p$, 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 $car(A) = 0$ então $S = \{m \cdot 1 | m \in \mathbb{Z}\}$ é isomorfo a $\mathbb{Z}$ e, se $car(A) = n \neq 0$, então $S = \{m \cdot 1; m = 0, 1, ..., n-1\}$ é isomorfo a $\mathbb{Z}/n\mathbb{Z}$ [4].

De forma análoga, pela característica de um corpo K, necessariamente igual à zero ou um primo p ([4]), podemos determinar o subcorpo primo de K. Denotando este último por K_0, se $car(K) = 0$, então K_0 é isomorfo à $\mathbb{Q}$. Se $car(K) = p$, então o K_0 coincide com o subanel primo de K, pois este é um corpo isomorfo à $\mathbb{Z}/p\mathbb{Z}$ [4].

Assim como o corpo $\mathbb{Q}$ pode ser obtido do domínio $\mathbb{Z}$, faremos agora uma construção semelhante de modo que um corpo K seja obtido de um domínio A. Definiremos a seguir este corpo obtido. Para isto, dado um domínio A, definimos sobre $A \times (A \setminus \{0\})$ a seguinte relação, com $a,c \in A$ e $b,d \in A \setminus \{0\}$

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc.$$

É simples verificar que esta é uma relação de equivalência. As classes (a,b) são chamadas frações, denotadas por $\frac{a}{b}$. Considere K como o quociente do conjunto $A \times (A \setminus \{0\})$ pela relação de equivalência acima, ou seja, $K = A \times (A \setminus \{0\})/\sim$, munido da adição e multiplicação bem-definidas

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad e \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

É fácil verificar que $(K,+,\cdot)$ é um corpo, definido como

Definição 2.2.8. *Dado um domínio A, o corpo obtido pela construção acima é chamado de corpo de frações de A. Denotamos por $cf(A)$.*

O domínio A pode ser visto como um subanel de $cf(A)$, tomando $x = x/1$, para $x \in A$. Por outro lado, temos que $A = cf(A)$ se, e somente se, A é um corpo. Além disso, quando A é um subanel de um corpo K, o corpo de frações $cf(A)$ se relaciona com o subcorpo dos quocientes de A em K, dado por $x \cdot y^{-1}$; $x \in A, y \in A \setminus \{0\}$, no sentido que este último é o menor subcorpo de K que contém A e é isomorfo ao $cf(A)$ [4].

2.3 Ideais

Podemos definir, para anéis, um conceito análogo ao de subgrupo normal, visto anteriormente. Com isso, podemos fazer uma construção em anéis, utilizando analogias adequadas, semelhante aos grupos quocientes de grupos por subgrupos normais. Desse modo, apresentamos o conceito de ideal de um anel, o que nos fornece resultados importantes para o estudo de anéis e corpos.

Definição 2.3.1. *Sejam A um anel e $I \subseteq A$, não vazio. Dizemos que I é um Ideal de A se $(I,+)$ é subgrupo de $(A,+)$ e se, dado qualquer $a \in A$ e $r \in I$, temos $a \cdot r \in I$.*

Lembramos que consideramos o anel A comutativo. Caso não seja, a definição exige que ar e ra estejam em I. Uma condição necessária e suficiente para I ser um ideal de A é, dados quaisquer $a,b \in I$ e $r \in A$, então $r \cdot a + b \in I$.

Definição 2.3.2. *Dado um anel A, para todo $x \in A$ o conjunto $A \cdot x = \{a \cdot x;\ a \in A\}$, denotado por $\langle x \rangle$ ou (x), é um ideal de A, denominado o ideal principal gerado por x.*

Um domínio R é chamado *domínio principal* se todos os seus ideais são principais. Os chamados ideais triviais de um anel A são dados por $\langle 0 \rangle = \{0\}$ e $\langle 1 \rangle = A$. Além disso, A é o único ideal de A que contêm elementos invertíveis, ou seja, para todo $x \in A$, temos $\langle x \rangle = A$ se, e só se, $x \in U_A$ [4]. Uma consequência disto é dada pelo resultado a seguir.

Proposição 2.3.3. *Se A é um anel comutativo com unidade, cujos únicos ideias são os triviais $\langle 0 \rangle$ e o próprio A, então A é um corpo.*

Ou seja, todo corpo K possui apenas os ideais triviais $\langle 0\rangle$ e $\langle 1\rangle = K$. A prova deste resultado pode ser consultada em [5]. Pode ser mostrado que a intersecção de ideias em um anel A é também ideal em A. Então definimos, para qualquer subconjunto $R \subseteq A$, o ideal gerado por R como a intersecção $(R) = \cap U$, com $U \in \mathscr{I}_R$, no qual $\mathscr{I}(R)$ representa o conjunto de ideais que contêm R. De modo análogo ao visto para anéis e corpos, temos que (R) é o menor ideal de A que contêm R. Um ideal U de A é dito *finitamente gerado* quando $U = (R)$, para algum subconjunto $R \subseteq A$ finito.

Faremos agora a construção de modo à obter um conjunto quociente que seja um anel, conceito análogo aos grupos quocientes vistos anteriormente. Para isto, dado um ideal I de um anel A, denotemos por A/I o conjunto de todas as classes laterais distintas de I em A. Podemos considerar este conjunto, pois vimos que $(I,+)$ é subgrupo de $(A,+)$. Ou seja, A/I é o conjunto das classes laterais do tipo $a+I$, com $a \in A$.

Como vimos, A/I é um grupo quociente, com relação à adição dada por $(a+I)+(b+I) = (a+b)+I$. Então, para que A/I tenha uma estrutura de anel, devemos definir uma multiplicação sobre este conjunto de modo que sejam satisfeitas as propriedades que definem um anel. O mais natural é definir $(a+I)\cdot(b+I) = ab+I$. Pode ser provado que esta multiplicação é bem definida e que as propriedades multiplicativas que definem um anel são satisfeitas, o que pode ser visto em detalhes em [5]. Segue então o seguinte resultado.

Proposição 2.3.4. *Se A é um anel e I é um ideal de A, então o conjunto A/I adquirido na construção acima é um anel, chamado anel quociente de A sobre I.*

Se A é um anel comutativo, então A/I também o é, 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 trazer para anéis quocientes um resultado visto em grupos. Existe um homomorfismo sobrejetor ϕ de A em A/I dado por $\phi(a) = a+I$, para todo $a \in A$, que tem núcleo igual à I. Isto nos leva ao seguinte lema.

Lema 2.3.5. *[5] 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 nos diz como é a imagem de um certo anel por um homomorfismo sobrejetor. Esse resultado é dado pelo teorema a seguir.

Teorema 2.3.6. *[5] Seja $\phi : A \longrightarrow R$ um homomorfismo sobrejetor de anéis, com núcleo I. Então R é isomorfo à 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 um ideal U de R com o ideal W de A dado por $W = \{x \in A;\ \phi(x) \in U\}$. Neste caso, A/W é isomorfo à R/U.*

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

Definição 2.3.7. *Um ideal U de um anel A é um ideal primo de A se $U \neq A$ e, dados quaisquer $x,y \in A$, então $xy \in U$ implica em $x \in U$ ou $y \in U$.*

Definição 2.3.8. *Um ideal $M \neq A$ de A é chamado um ideal maximal de A se, dado um ideal U de A tal que $M \subset U \subset A$, então $M = U$ ou $A = U$.*

Ou seja, um ideal de A é maximal se não existe nenhum ideal entre ele e o anel A. Ou, ainda, é maximal quando é o elemento maximal do conjunto $\mathscr{I}_A \setminus \{A\}$ dos ideais de A, exceto claro o próprio A.

Proposição 2.3.9. *O ideal U de A é primo se, e somente se, A/U é um domínio.*

Demonstração. Suponha que A/U é um domínio. Então $A \neq U$, pois A/U é não trivial. Dados $x, y \in A$ tais que $xy \in U$, então $(x+U)(y+U) = xy+U = U$, o zero de A/U. Logo $x \in U$ ou $y \in U$, ou seja, U é primo. Reciprocamente, se U é ideal primo de A, então $A \neq U$ e portanto A/U é não trivial. Dados $x, y \in A$ tais que $(x+U)(y+U) = U$, o zero de A/U, então $xy \in U$. Logo $x \in U$ ou $y \in U$. Portanto A/U não possui divisores de zero, de onde segue que A/U é um domínio. ■

Proposição 2.3.10. *O ideal M de um anel A é maximal se, e somente se, A/M é um corpo.*

Demonstração. Suponha que A/M é um corpo. Então seus únicos ideais são $\langle 0 \rangle$ e $\langle 1 \rangle$. Como vimos, existe uma correspondência biunívoca entre o conjunto dos ideais de A/M e o conjunto dos ideais de A que contêm M, onde o ideal M de A corresponde ao ideal $\langle 0 \rangle$, enquanto que o ideal A corresponde ao ideal A/M. Portanto não existe nenhum ideal entre M e A, de onde segue que M é maximal. Reciprocamente, supondo M maximal de A, segue pela correspondência mencionada acima que A/M possui apenas os ideais $\langle 0 \rangle$ e o próprio A/M. Além disso, como consideramos A comutativo com unidade, segue que A/M também satisfaz essas propriedades. Portanto A/M é um corpo. ■

Um resultado imediato destes últimos é que, vistos sobre o ideal $\langle 0 \rangle$, temos

Corolário 2.3.11. *O ideal $\langle 0 \rangle$ de A é primo (respectivamente maximal) se, e só se, o anel A é um domínio (respectivamente corpo).*

Além disso, como todo corpo é um domínio, é imediato que

Corolário 2.3.12. *Todo ideal maximal é um ideal primo.*

2.4 Anel dos polinômios sobre um corpo

Antes de avançarmos para o próximo tópico, trataremos de um importante anel necessário para definir noções e enunciar resultados posteriores, o anel dos polinômios sobre um certo corpo. Apresentaremos, então, conceitos e propriedades importantes sobre este anel, o que nos dará algumas ferramentas para nosso estudo. Inicialmente, definimos quem são seus elementos e suas operações aditiva e multiplicativa.

Definição 2.4.1. *Se K é um corpo, um polinômio com variável x e coeficientes sobre K é dado por uma expressão $p(x) = a_n x^n + \cdots + a_1 x + a_0$, com $a_0, \cdots, a_n \in K$ e n um inteiro positivo. Denotamos o conjunto destes polinômios por $K[x]$*

As operações sobre o conjunto dos polinômios são as usuais, dadas pela adição e multiplicação definidas a seguir, dados $p(x) = a_n x^n + \cdots + a_0$ e $q(x) = b_m x^m + \cdots + b_0$ ambos em $K[x]$, considerando $m \geq n$. Então

$$p(x) + q(x) = c_m x^m + \cdots c_0, \quad onde \;\; c_i = a_i + b_i, \quad 0 \leq i \leq m$$

e

$$p(x)q(x) = c_{m+n} x^{m+n} + \cdots + c_0, \quad onde \;\; c_i = \sum_{j=0}^{i} a_j b_{i-j}, \quad 0 \leq i \leq m+n.$$

Então $K[x]$, munido destas operações, é um anel, denominado *anel dos polinômios sobre um corpo K*. O zero deste anel é dado pelo polinômio constante $p(x) = 0$.

Dado um corpo K, denotamos por $K(x)$ o corpo quociente do anel dos polinômios $K[x]$ e chamamos este de *corpo de funções racionais*. Desse modo, $K(x)$ é formado por todos os quocientes $f(x)/g(x)$, com $g(x) \neq 0$. Podemos pensar nas frações $f(x)/g(x)$ como funções de K em si mesmo, por isso recebem o nome de *funções racionais* ou *expressões racionais*.

Proposição 2.4.2. *Todo ideal do anel $K[x]$ é principal, ou seja, se F é um ideal de $K[x]$, existe $f \in F$ tal que $F = \langle f \rangle$.*

Definição 2.4.3. *Se p é um polinômio sobre um corpo K, $p \neq 0$, então definimos o grau de p pela maior potência da variável x, com coeficiente não-nulo, que ocorre em p.*

Ou seja, o grau de um polinômio é definido pela função

$$gr : K[x] \setminus \{0\} \longrightarrow \mathbb{N} \quad dada\ por \quad \sum_{i=0}^{n} a_i x^i \longmapsto n,$$

onde n é o maior inteiro positivo tal que $a_n \neq 0$. Denotaremos o grau de um polinômio p por $gr(p)$. Segue das definições de adição e multiplicação do anel que $gr(p+q) \leq max(gr(p), gr(q))$ e $gr(pq) = gr(p) + gr(q)$. O grau do polinômio zero é, por convenção, igual à $-\infty$.

Um importante conceito envolvendo polinômios é o e divisibilidade. Na Teoria dos números vemos que, se $a, b \in \mathbb{Z}$, então a é divisível por b (ou que b divide a) se existe $c \in \mathbb{Z}$ tal que $a = bc$. Com esta noção, podemos estudar conceitos como irredutibilidade de um inteiro e introduzir números primos e a ideia de máximo divisor comum. Então, buscaremos fazer o mesmo para polinômios com coeficientes em um corpo, trazendo ideias similares. Nesse sentido, começamos introduzindo o conceito de divisibilidade, que pode ser dado pelo algoritmo da divisão euclidiana, dado pelo teorema a seguir, cuja demonstração será omitida e pode ser encontrada em [8].

Teorema 2.4.4. *(Algoritmo da divisão euclidiana) Sejam $f, p \in K[x]$ polinômios, com $f \neq 0$. Então existem polinômios únicos $q, r \in K[x]$ tais que $p = fq + r$, tal que $gr(r) < gr(f)$.*

Neste caso, o polinômio q é chamado *quociente* e r é dito *resto* da divisão. O processo para determinar p e q é o chamado algoritmo da divisão. Com isso, podemos definir a divisibilidade entre polinômios.

Definição 2.4.5. *Dados $f, g \in K[x]$, dizemos que f divide g, ou que g é múltiplo de f, se existe um polinômio $h \in K[x]$ tal que $g = fh$.*

Quando f divide g, denotamos por $f|g$. Caso contrário, denotamos como $f \nmid g$ para dizer que f não divide g. Note que, pelo algoritmo da divisão, f divide g se temos o polinômio resto $r = 0$. Com isto, podemos definir o conceito de máximo divisor comum para polinômios.

Definição 2.4.6. *Um polinômio $m \in K[x]$ é definido como o máximo divisor comum (mdc) de polinômios $p, q \in K[x]$ se $m|p$, $m|q$ e, além disso, sempre que $f|p$ e $f|q$, tivermos $f|m$.*

Quando $m \in K[x]$ é o máximo divisor comum dos polinômios p e q sobre K, então existem polinômios $a, b \in K[x]$ tais que $m = ap + bq$. Este é um resultado semelhante à divisão nos inteiros. Uma demonstração deste fato pode ser encontrada em [8].

Definição 2.4.7. *Se p e q são polinômios sobre um corpo K com $mdc(p,q) = 1$, então p e q são ditos coprimos.*

Colocados estes conceitos de divisibilidade entre polinômios, podemos encontrar para estes uma noção análoga a de números primos. O conceito em questão é o de irredutibilidade, de grande importância para este estudo, como veremos em tópicos posteriores. Relembrando, um inteiro é primo se não pode ser expresso como produto de dois primos menores. De forma, semelhante, diremos que um polinômio é irredutível quando não pode ser expresso pelo produto de dois polinômios, agora de menor grau. Desse modo, temos a seguinte definição.

Definição 2.4.8. *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.*

Ou seja, $p \in K[x]$ é irredutível se não existem $f, g \in K[x]$ tais que $0 < gr(f), gr(g) < gr(p)$ e $p = fg$. Pela definição acima, qualquer polinômio redutível pode ser escrito como produto de dois polinômios de menor grau. Se estes forem redutíveis podem ser, cada um, reescritos como um produto de polinômios de menor grau, e assim por diante. Por indução, este processo continua até certo ponto, ou seja, o ponto em que os polinômios fatores deste produto são todos irredutíveis. Desse modo, podemos enunciar o seguinte teorema.

Teorema 2.4.9. *[8] Qualquer polinômio sobre um corpo K é produto de polinômios irredutíveis sobre K.*

A seguir, apresentamos um critério para determinar se um polinômio é irredutível, o critério de Eisenstein. Antes, no entanto, precisamos enunciar o lema de Gauss, que provou que a irredutibilidade sobre $\mathbb{Z}$ equivale à irredutibilidade sobre $\mathbb{Q}$.

Lema 2.4.10. *(Lema de Gauss) Seja f um polinômio sobre $\mathbb{Z}$ irredutível sobre $\mathbb{Z}$. Então f, visto como um polinômio sobre $\mathbb{Q}$, é irredutível sobre $\mathbb{Q}$.*

Demonstração. Suponha que f é irredutível sobre $\mathbb{Z}$ mas redutível sobre $\mathbb{Q}$, ou seja, existem g, h de menor grau tais que $f = gh$. Multiplicando esta igualdade pelo produto dos denominadores dos coeficientes de g e h, podemos reescrever a equação como $nf = g'h'$, com $n \in \mathbb{Z}$ e g' e h' polinômios sobre $\mathbb{Z}$.

Queremos mostrar que podemos cancelar, um por um, os fatores primos de n, continuando em $\mathbb{Z}[x]$. Para isto, suponha que p é um fator primo de n. Afirmamos que se

$$g' = g_0 + g_1x + \cdots + g_rx^r \quad e \quad h' = h_0 + h_1x + \cdots + h_sx^s$$

então p divide todos os coeficientes g_i ou p divide todos h_i. De fato, se isso não vale, devem existir i e j tais que $p \nmid g_i$ e $p \nmid h_j$. Mas p divide os coeficientes de x^{i+j} do produto $g'h'$, dado por

$$h_0g_{i+j} + h_1g_{i+j-1} + \cdots + h_jg_i + \cdots h_{i+j}g_0$$

e pela escolha de i e j, temos que p divide todos os termos desta expressão, exceto talvez h_jg_i. Mas p deve dividir toda a expressão, inclusive $p|h_jg_i$, o que contradiz o estabelecido de que $p \nmid g_i$ e $p \nmid h_j$. Desse modo, mostramos o que foi afirmado.

Agora, sem perda de generalidade, podemos assumir que p divide todos os coeficientes g_i. Então $g' = pg''$,em que g'' é um polinômio sobre $\mathbb{Z}$ de mesmo grau que g' e g. Colocando $n = pn_1$, temos $pn_1f = pg''h'$, ou seja, $n_1f = g''h'$. Procedendo da mesma forma, podemos cancelar todos os fatores primos de n, chegando em uma equação da forma $f = \bar{g}\bar{h}$, tal que $\bar{g}$ e $\bar{h}$ são polinômios sobre $\mathbb{Z}$ múltiplos racionais de g e h, respectivamente. Logo $gr(\bar{g}) = gr(g)$ e $gr(\bar{h}) = gr(h)$, o

que contradiz a irredutibilidade de f sobre $\mathbb{Z}$. Portanto f é irredutível também sobre $\mathbb{Q}$. ■

A partir deste Lema, Eisenstein, um estudante de Gauss, formulou e provou um critério de irredutibilidade, dado pelo teorema a seguir.

Teorema 2.4.11. *(Critério de Eisenstein) Seja $f(x) = a_n x^n + \cdots + a_1 x + a_0$ um polinômio sobre $\mathbb{Z}$. Se existe um número primo p tal que*

1. $p \nmid a_n$,
2. $p|a_i, \;\; i = 0, \cdots, n-1$,
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

$$g = b_0 + b_1 x + \cdots + b_r x^r \quad e \quad h = c_0 + c_1 x + \cdots + c_s x^s$$

são polinômios de menor grau sobre $\mathbb{Z}$, com $r + s = n$. Temos que $a_0 = b_0 c_0$ e, pelo segundo item, $p|b_0$ ou $p|c_0$. Pelo terceiro item, p não pode dividir b_0 e c_0 ao mesmo tempo. Então, sem perda de generalidade, podemos supor que $p|b_0$ e $p \nmid c_0$. Se todos os coeficientes b_j são divisíveis por p, então $p|a_n$, o que contradiz o primeiro item. Então, seja b_j o primeiro coeficiente de g não divisível por p. Então $a_j = b_j c_0 + \cdots + b_0 c_j$, com $j < n$. Isto implica que $p|c_0$, pois p divide $a_0, b_1, \cdots, b_{j-1}$, mas não b_j, o que é uma contradição. Portanto f é irredutível sobre $\mathbb{Z}$ e, por consequência, sobre $\mathbb{Q}$. ■

Trazemos agora o conceito de *zero* de um polinômio, elemento que o anula quando aplicado sobre ele. Veremos um importante resultado, que nos garante a existência de zeros em qualquer polinômio sobre o corpo dos complexos, resultados de tamanha importância que recebe o nome de Teorema fundamental da Álgebra.

Definição 2.4.12. *Dado um polinômio p sobre o corpo K e um elemento $\alpha \in K$ tal que $p(\alpha) = 0$, então o número α recebe o nome de zero do polinômio, ou raiz da equação $p(x) = 0$.*

De mesmo modo, dado um subanel $R \subseteq \mathbb{C}$ e um polinômio f sobre R, então dizemos que $\alpha \in R$ é um zero de f em R se $f(\alpha) = 0$. Fazemos esta distinção para deixar claro onde se encontram os zeros de um polinômio. Utilizaremos a partir daqui o termo raiz, quando nos referirmos ao zero de um polinômio. Temos a seguir um resultado que nos diz quando um elemento $\alpha \in K$ é raiz de um polinômio sobre um corpo K. A demonstração pode ser encontrada em [8].

Lema 2.4.13. *Dados um polinômio $p \in K[x]$ e $\alpha \in K$, então $p(\alpha) = 0$ se, e somente se, $(x - \alpha)|p(x)$ em $K[x]$.*

Desse modo, se α é raiz de p em K, então $(x - \alpha)|p$. Portanto podemos escrever $p(x) = (x - \alpha)q(x)$ para algum polinômio $q \in K[x]$. Se, além disso, tivermos que $(x - \alpha)|q$ em $K[x]$, então α é raiz de q e portanto novamente uma raiz de p, pois teremos $(x - \alpha)(x - \alpha)|p$. Nesse caso, dizemos que α é uma raiz múltipla de p em $K[x]$. Definimos melhor este conceito de multiplicidade, como segue.

Definição 2.4.14. *Dado um $p \in K[x]$, dizemos que $\alpha \in K$ é uma raiz simples se $(x-\alpha)|p$ mas $(x-\alpha)^2 \nmid p$. Por outro lado, dizemos que α é raiz de p de multiplicidade m se $(x-\alpha)^m|p$ mas $(x-\alpha)^{m+1} \nmid p$.*

Pelas mesmas considerações feitas acima, temos o seguinte resultado, cuja prova pode ser consultada em [8].

Lema 2.4.15. *Seja $f \in K[x]$ um polinômio não-nulo. Então f possui raízes $\alpha_1, \cdots, \alpha_r$ com multiplicidades $m_1, m_2, \cdots, m_r$, respectivamente, se e somente se,*

$$f(x) = (x-\alpha_1)^{m_1} \cdots (x-\alpha_r)^{m_r} g(x),$$

onde g é um polinômio que não possui raízes em K.

Uma consequência deste lema é dada pelo seguinte teorema, muito conhecido no estudo de polinômios.

Teorema 2.4.16. *O número de raízes de um polinômio sobre um corpo K, contando com suas multiplicidades, é menor ou igual ao grau do polinômio.*

Isto nos traz ao Teorema fundamental da Álgebra, que nos diz o número de raízes de qualquer polinômio $p \in \mathbb{C}[x]$.

Teorema 2.4.17. *(Fundamental da Álgebra) Todo polinômio p sobre os $\mathbb{C}$ possui todas as suas raízes em $\mathbb{C}$.*

Ou seja, o teorema nos garante que qualquer polinômio de grau n em $\mathbb{C}$ possui exatamente n raízes nos complexos. Por isso, $\mathbb{C}$ é chamado de corpo *algebricamente fechado.*

2.5 Extensões de Corpos

Um dos estudos originais de Galois era encontrar raízes de polinômios em um determinado corpo $\mathbb{K}$. Mas nem sempre isto é possível, tendo em vista que em muitos casos estas raízes não existem. Então em alguns casos se faz necessário passar de um corpo menor $\mathbb{K}$ para um corpo maior $\mathbb{L}$ que contêm $\mathbb{K}$. Com isso, temos formada a ideia de extensão de um corpo à outro. Dizemos, neste caso, que $\mathbb{L}$ é um extensão do corpo $\mathbb{K}$. Esse conceito é de importância central neste estudo, e na Teoria de Galois. Veremos posteriormente que o grupo de Galois se associa a determinada extensão de corpo. Veremos então, nesta seção, os principais conceitos e resultados referentes a este importante objeto.

2.5.1 Extensões finitas

Definição 2.5.1. *Se $\mathbb{K} \subset \mathbb{L}$ são corpos, então dizemos que $\mathbb{L}$ é uma extensão do corpo $\mathbb{K}$ se $\mathbb{L}$ contém $\mathbb{K}$ como seu subcorpo. Neste caso, denotamos a extensão por $\mathbb{L}|\mathbb{K}$.*

Uma extensão $\mathbb{L}$ de $\mathbb{K}$ pode ser vista como um $\mathbb{K}$-espaço vetorial com as operações definidas no corpo $\mathbb{L}$, ou seja, $\mathbb{L}$ é um espaço vetorial sobre o corpo $\mathbb{K}$. Desse modo, através da dimensão desse espaço, é possível definirmos um grau para a extensão, como segue.

Definição 2.5.2. *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 $\mathbb{K}$, ou seja, $[\mathbb{L}:\mathbb{K}] = dim_{\mathbb{K}}\mathbb{L}$.*

Dizemos que a extensão é finita se $[\mathbb{L}:\mathbb{K}]$ é finito, caso contrário a extensão é dita infinita. Quando um conjunto $\{\beta_1,\beta_2,\cdots,\beta_n\}\subset\mathbb{L}$ 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 2.5.3. *Dada uma extensão* $\mathbb{L}|\mathbb{K}$, *temos que* $[\mathbb{L}:\mathbb{K}]=1$ *se, e somente se,* $\mathbb{L}=\mathbb{K}$.

Demonstração. Suponha $[\mathbb{L}:\mathbb{K}]=1$. O conjunto $\{1\}$ é linearmente independente e, portanto, é uma base de $\mathbb{L}|\mathbb{K}$. Logo, se $\alpha\in\mathbb{L}$, então é da forma $\alpha=a\cdot 1$, com $a\in\mathbb{K}$, ou seja, $\alpha\in\mathbb{K}$. 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 traz uma importante propriedade de extensões finitas, no que diz respeito à multiplicidade dos graus de uma extensão contidas em outra.

Teorema 2.5.4. *(Multiplicidade dos graus) Dados corpos* $\mathbb{K}\subset\mathbb{M}\subset\mathbb{L}$ *tais que* $[\mathbb{L}:\mathbb{K}]<\infty$, *ou seja,* $\mathbb{L}|\mathbb{K}$ *finita, então* $[\mathbb{L}:\mathbb{M}]<\infty$ *e* $[\mathbb{M}:\mathbb{K}]<\infty$. *Além disso, temos*

$$[\mathbb{L}:\mathbb{K}]=[\mathbb{L}:\mathbb{M}]\cdot[\mathbb{M}:\mathbb{K}].$$

Demonstração. Como $\mathbb{M}$ e $\mathbb{L}$ são ambos $\mathbb{K}$-espaços vetoriais e $\mathbb{M}\subset\mathbb{L}$, então $\mathbb{M}$ é subespaço de $\mathbb{L}$, portanto $[\mathbb{M}:\mathbb{K}]\leq[\mathbb{L}:\mathbb{K}]<\infty$. Para mostrar que $[\mathbb{L}:\mathbb{M}]<\infty$, considere $B=\{u_1,u_2,\cdots,u_n\}$ uma base de $\mathbb{L}$ como $\mathbb{K}$-espaço vetorial. Dado $x\in\mathbb{L}$, então existem $\alpha_1,\alpha_2,\cdots,\alpha_n\in\mathbb{K}\subset\mathbb{M}$ tais que $x=\alpha_1u_1+\cdots+\alpha_nu_n$. Logo B é um conjunto gerador de $\mathbb{L}$ como $\mathbb{M}$-espaço vetorial. Então existe $B'\subset B$ base de $\mathbb{L}$ como $\mathbb{M}$-espaço vetorial. Portanto $[\mathbb{L}:\mathbb{M}]\leq[\mathbb{L}:\mathbb{K}]<\infty$.

Por fim, mostremos que $[\mathbb{L}:\mathbb{K}]=[\mathbb{L}:\mathbb{M}]\cdot[\mathbb{M}:\mathbb{K}]$. Sejam $(v_i)_{1\leq i\leq m}$ uma base de $\mathbb{L}$ como $\mathbb{M}$-espaço vetorial e $(w_j)_{1\leq j\leq n}$ uma base de $\mathbb{M}$ como $\mathbb{K}$-espaço vetorial. Queremos mostrar que $\{v_iw_j,\ 1\leq i\leq m,\ 1\leq j\leq n\}$ é uma base de $\mathbb{L}$ como $\mathbb{K}$-espaço vetorial. Então:

(i) Dado $x\in\mathbb{L}$, então

$$x=\sum_{i=1}^{m}\alpha_iv_i,\quad \alpha_i\in\mathbb{M}.$$

Por outro lado, para todo $i=1,\cdots,m$, temos

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

Assim, temos

$$x=\sum_{i=1}^{m}\sum_{j=1}^{n}\beta_{ij}w_jv_i,\quad \beta_{ij}\in\mathbb{K}.$$

Portanto $\{v_iw_j\}$ gera $\mathbb{L}$ como $\mathbb{K}$-espaço vetorial.

(ii) Agora, suponha para $\beta_{ij}\in\mathbb{K}$ que

$$\sum_{i=1}^{m}\sum_{j=1}^{n}\beta_{ij}v_iw_j=0.$$

Então

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

Como $(v_i)_{1\leq i\leq m}$ é linearmente independente, então, para todo $i = 1, \cdots, m$,

$$\sum_{j=1}^{n} \beta_{ij} w_j.$$

Logo, como $(w_j)_{1\leq j\leq n}$ é linearmente independente, segue que $\beta_{ij} = 0$, ou seja, $\{v_i w_j\}$ é linearmente independente.

Portanto $\{v_i w_j,\ 1 \leq i \leq m,\ 1 \leq j \leq n\}$ é uma base de $\mathbb{L}$ como $\mathbb{K}$-espaço vetorial. Segue então que $[\mathbb{L} : \mathbb{K}] = m \cdot n = [\mathbb{L} : \mathbb{M}] \cdot [\mathbb{M} : \mathbb{K}]$. ■

Corolário 2.5.5. *Dados os corpos $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$, se $[\mathbb{L} : \mathbb{K}]$ é um número primo, então $\mathbb{M} = \mathbb{K}$ ou $\mathbb{M} = \mathbb{L}$.*

Ou seja, quando o grau de uma extensão $\mathbb{L}|\mathbb{K}$ é um número primo, então não existe nenhum corpo entre $\mathbb{K}$ e $\mathbb{L}$. Isto segue diretamente do teorema anterior.

Proposição 2.5.6. *Todo subcorpo de $\mathbb{C}$ contêm $\mathbb{Q}$.*

Demonstração. Dado um subcorpo $\mathbb{K} \subseteq \mathbb{C}$, então por definição $0, 1 \in \mathbb{K}$ e, por indução, temos $1 + 1 + \cdots 1 = n \in \mathbb{K}$, para todo inteiro $n > 0$. Mas $\mathbb{K}$ é fechado para inversos aditivos, portanto $-n \in K$, ou seja, $\mathbb{Z} \subseteq \mathbb{K}$. Além disso, se $p, q \in \mathbb{Z}$, com $q \neq 0$, como $\mathbb{K}$ é fechado para o produto e inversos multiplicativos, então $pq^{-1} \in \mathbb{K}$, ou seja, $\mathbb{Q} \subseteq \mathbb{K}$. ■

Se $\mathbb{L}|\mathbb{K}$ é uma extensão finita, definimos para cada elemento $\alpha \in \mathbb{L}$ seu polinômio característico, construído a partir de uma base de $\mathbb{L}|\mathbb{K}$. Se $\{\beta_1, \cdots, \beta_n\}$ é uma base de $\mathbb{L}|\mathbb{K}$, para todo $\alpha \in \mathbb{L}$ existem $a_{ij} \in \mathbb{K}$ tais que $\alpha \cdot \beta_i = \sum_{j=1}^{n} a_{ij}\beta_j$, com $i = 1, \cdots, n$.

Definição 2.5.7. *O polinômio característico de $\alpha \in \mathbb{L}$ em relação a $\mathbb{L}|\mathbb{K}$, denotado por $car_{\alpha,\mathbb{L}|\mathbb{K}}$, é definido como o determinante*

$$car_{\alpha,\mathbb{L}|\mathbb{K}} = det\left(x \cdot \delta_{ij} - a_{ij}\right)_{i,j=1,\cdots,n} \in \mathbb{K}[x],$$

de modo que

$$\begin{cases} \delta_{ij} = 1, & \text{se } i = j \\ \delta_{ij} = 0, & \text{se } i \neq j. \end{cases}$$

Pode ser mostrado que $car_{\alpha,\mathbb{L}|\mathbb{K}}$ independe da escolha da base e que α é uma raiz de suas raízes sobre $\mathbb{K}$. A prova pode ser consultada em [4]. Além disso, vemos que o polinômio característico $car_{\alpha,\mathbb{L}|\mathbb{K}}$ tem grau igual à $[\mathbb{L}|\mathbb{K}] = n$ e, desse modo, depende da extensão $\mathbb{L}|\mathbb{K}$, além de α. Para extensões finitas, temos o seguinte resultado.

Proposição 2.5.8. *Considere a extensão finita $\mathbb{L}|\mathbb{K}$ e $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$. Então, para todo $\alpha \in \mathbb{L}$, temos*

$$car_{\alpha,\mathbb{L}|\mathbb{K}} = (car_{\alpha,\mathbb{M}|\mathbb{K}})^{[\mathbb{L}:\mathbb{M}]}.$$

Desse modo, dizemos que $car_{\alpha,\mathbb{L}|\mathbb{K}}$ é a potência $[\mathbb{L} : \mathbb{M}]$-ésima de $car_{\alpha,\mathbb{M}|\mathbb{K}}$. Ocultamos a prova, que pode ser encontrada em [4]. Veremos no próximo tópico que $car_{\alpha,\mathbb{L}|\mathbb{K}}$ é igual ao polinômio minimal de α sobre $\mathbb{K}$, quando α é um elemento algébrico, conceitos que definiremos adiante. Com isso, veremos que $car_{\alpha,\mathbb{L}|\mathbb{K}}$ é irredutível. Esses conceitos serão de grande importância em nosso estudo, daí a relevância do polinômio característico.

Dada uma extensão $\mathbb{L}|\mathbb{K}$, se $Y \subset \mathbb{K}$, então definimos o anel $\mathbb{K}[Y]$ gerado por $\mathbb{K}$ e Y como a intersecção de todos os subanéis de $\mathbb{L}$ que contêm $\mathbb{K}$ e Y. Dizemos também que $\mathbb{K}[Y]$ é o *subanel*

de $\mathbb{L}$ *obtido de* $\mathbb{K}$ *pela adjunção de* Y. De mesmo modo, definimos o corpo $\mathbb{K}(Y)$ gerado por $\mathbb{K}$ e Y como a intersecção de todos os subcorpos de $\mathbb{L}$ que contêm $\mathbb{K}$ e Y. Dizemos que $\mathbb{K}(Y)$ é o *subcorpo de* $\mathbb{L}$ *obtido de* $\mathbb{K}$ *pela adjunção de* Y. Se $Y = \{a_1, \cdots, a_n\}$ é finito, escrevemos $\mathbb{K}[Y] = [a_1, \cdots, a_n]$ e $\mathbb{K}(Y) = (a_1, \cdots, a_n)$, e dizemos que o corpo $\mathbb{K}(Y)$ é uma *extensão finitamente gerada de* $\mathbb{K}$. Quando $\mathbb{L}$ é gerado sobre $\mathbb{K}$ por um único elemento, temos o seguinte resultado, cuja demostração pode ser vista em [11].

Proposição 2.5.9. *Se* $\mathbb{L}$ *é uma extensão do corpo* $\mathbb{K}$ *e* $a \in \mathbb{L}$, *então*

$$\mathbb{K}[a] = \{f(a);\ f(x) \in \mathbb{K}[x]\}$$

e

$$\mathbb{K}(a) = \{f(a)/g(a);\ f, g \in \mathbb{K}[x], g(a) \neq 0\}.$$

Além disso, $\mathbb{K}(a)$ *é o corpo de frações de* $\mathbb{K}[a]$.

Utilizamos as notações $\mathbb{K}[a]$ e $\mathbb{K}(a)$ de acordo com as notações do anel dos polinômio $\mathbb{K}[x]$ e o corpo de funções racionais $\mathbb{K}(x)$, como nos mostra a descrição de $\mathbb{K}[a]$ e $\mathbb{K}(a)$. Adiante, veremos que $\mathbb{K}(\alpha) = \mathbb{K}[\alpha]$, quando α é um algébrico sobre $\mathbb{K}$, noção que definiremos a seguir e que nos traz ao nosso próximo tópico, um caso especial de extensões de corpos.

2.5.2 Extensões algébricas

Definição 2.5.10. *Se* $\mathbb{L}|\mathbb{K}$ *é uma extensão de corpos, dizemos que o elemento* $\alpha \in \mathbb{L}$ *é algébrico sobre* $\mathbb{K}$ *se for raiz de algum polinômio* $p \in \mathbb{K}[x] \setminus \{0\}$, *ou seja,* $p(\alpha) = 0$. *Caso este polinômio não exista, dizemos que* α *é transcendente sobre* $\mathbb{K}$.

Se $\mathbb{K} = \mathbb{Q}$, dizemos simplesmente que α é algébrico ou transcendente. Podemos garantir a existência de algébricos em qualquer extensão $\mathbb{L}|\mathbb{K}$, visto que todo $\alpha \in \mathbb{K}$ é algébrico sobre $\mathbb{K}$, pois é raiz do polinômio $p(x) = x - \alpha$. Além disso, se α é algébrico sobre $\mathbb{K}$, é também algébrico sobre qualquer corpo $\mathbb{M}$ entre $\mathbb{K}$ e $\mathbb{L}$.

Os exemplos mais clássicos de transcendentes sobre $\mathbb{Q}$ são os números irracionais π e e. Além disso, os corpos $\mathbb{R}$ e $\mathbb{C}$ possuem mais números transcendentes do que algébricos, pois o conjunto dos algébricos, reais ou complexos, é enumerável, enquanto que o conjunto dos transcendentes não.

Definição 2.5.11. *Um polinômio* $p(x) = a_n x^n + \cdots + a_1 x + a_0$ *sobre* $\mathbb{K}$ *é mônico se* $a_n = 1$.

Definição 2.5.12. *Dados uma extensão* $\mathbb{L}|\mathbb{K}$ *e* α *um algébrico sobre* $\mathbb{K}$, *definimos o polinômio minimal de* α *sobre* $\mathbb{K}$ *como o polinômio mônico* $f \in \mathbb{K}[x] \setminus \{0\}$ *de menor grau tal que* $f(a) = 0$. *Utilizamos a notação* $min_{\alpha,\mathbb{K}}$.

Podemos aprofundar o conceito de polinômio minimal da seguinte forma. Dado $\alpha \in \mathbb{L}$, seja $\phi_\alpha : \mathbb{K}[x] \longrightarrow \mathbb{L}$ um homomorfismo definido por $f \longmapsto f(\alpha)$, ou seja, substituindo x po α. Então $\mathbb{K}[\alpha]$ é a imagem deste homomorfismo. Denotemos por $I_{\alpha,\mathbb{K}}$ seu núcleo. Pode ser mostrado que $I_{\alpha,\mathbb{K}}$ é um ideal, necessariamente principal, de $\mathbb{K}[x]$ [4]. Além disso, $I_{\alpha,\mathbb{K}} \neq \langle 0 \rangle$ se, e só se, α é algébrico sobre $\mathbb{K}$. Neste caso, o único polinômio mônico gerador de $I_{\alpha,\mathbb{K}}$ é o polinômio minimal de α sobre $\mathbb{K}$, ou seja, $I_{\alpha,\mathbb{K}} = \langle min_{\alpha,\mathbb{K}} \rangle$.

Proposição 2.5.13. *Considere os corpos* $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$, $\alpha \in \mathbb{L}$ *algébrico sobre* $\mathbb{K}$, *com* $min_{\alpha,\mathbb{K}} = p$ *e* $min_{\alpha,\mathbb{M}} = q$. *Então vale que*

1. *o minimal* p *é irredutível em* $\mathbb{K}[x]$,

2. *se* $f \in \mathbb{K}[x]$ *é tal que* $f(a) = 0$, *então* $p|f$,

3. $q|p$.

Demonstração. Primeiro, suponha que p é redutível, ou seja, $p = gh$, com $g, h \in \mathbb{K}[x]$. Então, como $p(\alpha) = 0$, devemos ter $g(\alpha) = 0$ ou $f(\alpha) = 0$, o que contradiz a minimalidade de p. Portanto p é irredutível. Para o segundo item, pela divisão euclidiana existem $g, r \in \mathbb{K}[x]$ tais que $f = pg + r$, com $r = 0$ ou $gr(r) < gr(p)$. Por hipótese $p(\alpha) = f(\alpha) = 0$, então $r(\alpha) = 0$, o que só é válido se $r = 0$, pois p é minimal. Portanto $p|f$. O fato de que $q|p$ é consequência do segundo item, com $p \in \mathbb{M}[x]$. ■

Além disso, temos o seguinte resultado, complementar ao anterior, cuja prova é trivial e pode ser consultada em [4].

Proposição 2.5.14. *Sejam* $\mathbb{L}|\mathbb{K}$ *uma extensão,* $\alpha \in \mathbb{L}$ *algébrico sobre* $\mathbb{K}$ *e* $f \in \mathbb{K}[x]$ *um polinômio mônico pertencente ao ideal* $I_{\alpha,\mathbb{K}}$, *ou seja,* $f(\alpha) = 0$. *Então são equivalentes:*

(i) $f|min_{\alpha,\mathbb{K}}$,

(ii) $gr(f) \leq gr(min_{\alpha,\mathbb{K}})$,

(iii) f *é irredutível em* $\mathbb{K}[x]$,

(iv) $f = min_{\alpha,\mathbb{K}}$.

Com isso, podemos enunciar o seguinte resultado, que associa o polinômio minimal ao polinômio característico, quando α é algébrico.

Proposição 2.5.15. *Considere a extensão* $\mathbb{L}|\mathbb{K}$, *com* $\alpha \in \mathbb{L}$ *algébrico sobre* $\mathbb{K}$. *Então*

(i) $car_{\alpha,\mathbb{K}(\alpha)|\mathbb{K}} = min_{\alpha,\mathbb{K}}$,

(ii) se $\mathbb{L}|\mathbb{K}$ *é finta, então* $car_{\alpha,\mathbb{K}(\alpha)|\mathbb{K}} = (min_{\alpha,\mathbb{K}})^{[\mathbb{L}:\mathbb{K}(\alpha)]}$.

Demonstração. Para mostrar (i), basta ver que $car_{\alpha,\mathbb{K}(\alpha)}|\mathbb{K}$ é um polinômio no ideal $I_{\alpha,\mathbb{K}}$, mônico, de grau $[\mathbb{K}(\alpha) : \mathbb{K}] = gr(min_{\alpha,\mathbb{K}})$. Portanto satisfaz as condições da proposição anterior, de onde segue que $car_{\alpha,\mathbb{K}(\alpha)|\mathbb{K}} = min_{\alpha,\mathbb{K}}$. O item (ii) resulta diretamente do item (i) e da proposição 2.9. ■

Desse modo, o polinômio característico $car_{\alpha,\mathbb{K}(\alpha)}|\mathbb{K}$, nestas condições, é irredutível. Podemos utilizar esta proposição para determinar o polinômio minimal de qualquer elemento α algébrico sobre $\mathbb{K}$. Para isto, basta conhecer uma extensão finita $\mathbb{L}|\mathbb{K}$ tal que $\alpha \in \mathbb{L}$ e calcular seu polinômio característico $car_{\alpha,\mathbb{L}|\mathbb{K}}$. Pelo item (ii) acima, este é uma $[\mathbb{L} : \mathbb{K}(\alpha)]$-ésima potência do polinômio minimal $min_{\alpha,\mathbb{K}}$ [4].

Proposição 2.5.16. *Se* $\mathbb{K}$ *é um subcorpo de* $\mathbb{C}$ *e* $m \in \mathbb{K}[x]$ *é mônico irredutível, então existe* $\alpha \in \mathbb{C}$ *algébrico sobre* $\mathbb{K}$ *tal que* $min_{\alpha,\mathbb{K}} = m$.

Demonstração. Seja α uma raiz de m em $\mathbb{C}$. Então $m(\alpha) = 0$, então $min_{\alpha,\mathbb{K}}|m$. Mas m é irredutível sobre $\mathbb{K}$ e ambos os polinômios são mônicos, de onde segue que $m = min_{\alpha,\mathbb{K}}$. ■

Proposição 2.5.17. *Dada uma extensão* $\mathbb{L}|\mathbb{K}$, *se* $\alpha \in \mathbb{L}$ *é algébrico sobre* $\mathbb{K}$, *então* $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.

Demonstração. Lembramos que $\mathbb{K}[\alpha] = \{f(\alpha);\ f \in \mathbb{K}[x]\}$ e $\mathbb{K}(\alpha) = \left\{\frac{f_1(\alpha)}{f_2(\alpha)};\ f_1, f_2 \in \mathbb{K}[x]\right\}$, com $f_2 \neq 0$. Consideremos então um elemento genérico de $\mathbb{K}(\alpha)$ como $\frac{f_1(\alpha)}{f_2(\alpha)}$. É imediato que $\mathbb{K}[\alpha] \subseteq \mathbb{K}(\alpha)$. Por outro lado, se α é algébrico sobre $\mathbb{K}$ e $p = min_{\alpha,\mathbb{K}}$, então p e f_2 são coprimos em $\mathbb{K}[x]$ e, pelo Teorema de Bézout, existem $g, h \in \mathbb{K}[x]$ tais que $gf_2 + hp = 1$. Então, como $p(\alpha) = 0$, segue que $f_2(\alpha)g(\alpha) = 1$, ou seja, $f_2(\alpha)$ é invertível. Logo $\frac{f_1(\alpha)}{f_2(\alpha)} = f_1(\alpha)g(\alpha) \in \mathbb{K}[\alpha]$, de onde segue que $\mathbb{K}(\alpha) \subseteq \mathbb{K}[\alpha]$. Portanto $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$. ■

O próximo resultado, muito importante, nos garante que, quando α é algébrico, o quociente do anel $\mathbb{K}[x]$ pelo ideal principal $I_{\alpha,\mathbb{K}} = \langle min_{\alpha,\mathbb{K}} \rangle$ é isomorfo ao corpo $\mathbb{K}(\alpha)$ e que, além disso, $\mathbb{K}(\alpha)|\mathbb{K}$ é uma extensão finita.

Teorema 2.5.18. *Sejam $\mathbb{L}|\mathbb{K}$ uma extensão de corpos e $\alpha \in \mathbb{L}$ algébrico sobre $\mathbb{K}$ tal que $min_{\alpha,\mathbb{K}} = p$, com $gr(p) = n$. Então*

1. $\mathbb{K}[x]/\langle p \rangle \approx \mathbb{K}(\alpha)$;
2. $\left\{1, \alpha, \cdots, \alpha^{n-1}\right\}$ *é uma base de $\mathbb{K}(\alpha)$ sobre $\mathbb{K}$, ou seja, $[\mathbb{K}(\alpha) : \mathbb{K}] = gr(p) = n$.*

Demonstração. Pela irredutibilidade de p, o ideal $\langle p \rangle = I_{\alpha,\mathbb{K}}$ é maximal em $\mathbb{K}[x]$. Logo $\mathbb{K}[x]/\langle p \rangle$ é um corpo. Considerando o homomorfismo sobrejetor $\phi : \mathbb{K}[x] \longrightarrow \mathbb{K}$, dado por $f \longmapsto f(\alpha)$, vimos que $\langle p \rangle$ é seu núcleo. Portanto, pelo teorema de isomorfismo para anéis, temos que $\mathbb{K}[x]/\langle p \rangle \approx \mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.

Para mostrar o segundo item, sabemos que $\mathbb{K}(\alpha) = \mathbb{K}[\alpha] = \{f(\alpha) | f \in \mathbb{K}[x]\}$. Pela divisão euclidiana, existem $q, r \in \mathbb{K}[x]$ tais que $f = pq + r$, com $r = 0$ ou $gr(r) < gr(p) = n$. Ou seja,

$$r = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{K}[x].$$

Então

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

Portanto $\left\{1, \alpha, \cdots, \alpha^{n-1}\right\}$ gera $K(\alpha)$ sobre $\mathbb{K}$. Como $gr(p) = n$ e $p = min_{\alpha,\mathbb{K}}$, segue que o conjunto forma uma base de $\mathbb{K}(\alpha)|\mathbb{K}$. ■

Definição 2.5.19. *Dizemos que uma extensão $\mathbb{L}|\mathbb{K}$ é algébrica se todo $\alpha \in \mathbb{L}$ é algébrico sobre $\mathbb{K}$. Caso contrário, a extensão é dita transcendente.*

O teorema a seguir no garante que toda extensão finita é algébrica, ou seja, as extensões algébricas compõe uma classe maior de extensões. Mas a recíproca não é verdadeira.

Teorema 2.5.20. *Toda extensão finita é algébrica.*

Demonstração. Dada uma extensão finita $\mathbb{L}|\mathbb{K}$ e $\alpha \in \mathbb{L}$, então $\mathbb{K} \subseteq \mathbb{K}(\alpha) \subseteq \mathbb{L}$. Pelo último teorema, temos que $[\mathbb{K}(\alpha) : \mathbb{K}] < \infty$. Então suponha $[\mathbb{K}(\alpha) : \mathbb{K}] = n$. Logo $\left\{1, \alpha, \cdots, \alpha^{n-1}, \alpha^n\right\}$ é linearmente dependente sobre $\mathbb{K}$, ou seja, existem $a_0, a_1, \cdots, a_n \in \mathbb{K}$, não todos nulos, tais que $\sum_{i=0}^{n} a_i \alpha^i = 0$. Então α é raiz do polinômio $p = \sum_{i=0}^{n} a_i x^i \in \mathbb{K}[x]$ e portanto algébrico sobre $\mathbb{K}$. Isto mostra que a extensão é algébrica. ■

Proposição 2.5.21. *[11] Seja $\mathbb{L}|\mathbb{K}$ uma extensão tal que todo $\alpha_i \in \mathbb{L}$ é algébrico sobre $\mathbb{K}$. Então $\mathbb{K}(\alpha_1, \cdots, \alpha_n)|\mathbb{K}$ é uma extensão finita. Além disso,*

$$[\mathbb{K}(\alpha_1, \cdots, \alpha_n) : \mathbb{K}] \leq \prod_{i=1}^{n} [\mathbb{K}(\alpha_i) : \mathbb{K}].$$

Corolário 2.5.22. *[11] Dada uma extensão $\mathbb{L}|\mathbb{K}$, então $\alpha \in \mathbb{L}$ é algébrico sobre $\mathbb{K}$ se, e só se, $[\mathbb{L}:\mathbb{K}] < \infty$.*

Proposição 2.5.23. *Sejam $\mathbb{L}|\mathbb{K}$ uma extensão de corpos e $X \subset \mathbb{L}$ tal que todo elemento de X é algébrico sobre $\mathbb{K}$. Então a extensão $\mathbb{K}(X)|\mathbb{K}$ é algébrica. Além disso, se X é finito, então $[\mathbb{K}(X):\mathbb{K}] < \infty$.*

Demonstração. Dado $a \in \mathbb{K}(X)$, existem $\alpha_1, \cdots, \alpha_n \in X$ tais que $a \in \mathbb{K}(\alpha_1, \cdots, \alpha_n)$. Pela proposição anterior, $\mathbb{K}(\alpha_1, \cdots, \alpha_n)$ é algébrica, logo a é algébrico sobre $\mathbb{K}$ e, portanto, $\mathbb{K}(X)|\mathbb{K}$ é extensão algébrica. A finitude do grau segue diretamente da proposição anterior. ■

O resultado a seguir apresenta um critério de irredutibilidade de polinômios, quando trabalhamos com extensões de $\mathbb{Q}$ geradas por dois ou mais algébricos em $\mathbb{C}$. Com ele, é possível determinar o grau destas extensões.

Lema 2.5.24. *Se $\mathbb{K}$ é um corpo tal que $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{C}$, com $[\mathbb{K}:\mathbb{Q}] = m$ e se $f \in \mathbb{K}[x]$ é irredutível sobre $\mathbb{Q}$, com $gr(f) = n$, tal que $mdc(m,n) = 1$, então f é irredutível sobre $\mathbb{K}$.*

Demonstração. Se $\alpha \in \mathbb{C}$ é raiz de f, então $[\mathbb{Q}(\alpha):\mathbb{Q}] = gr(f) = n$, pois f é irredutível sobre $\mathbb{Q}$. Colocando $p = min_{\alpha,\mathbb{K}}$, então $[\mathbb{K}(\alpha):\mathbb{K}] = gr(p) := s$. Então $p|f$ e $s \leq n$. Considere $[\mathbb{K}(\alpha):\mathbb{Q}(\alpha)] = r$. Logo, pelo teorema de multiplicidade dos graus, temos $[\mathbb{K}(\alpha):\mathbb{Q}] = sm = rn$. Como $mdc(m,n) = 1$ e $n|sm$, então $n|s$, de onde segue que $n \leq s$. Portanto $n = s$, ou seja, $f = cp$, na qual $c \in \mathbb{K}^*$ é uma constante. Logo f é irredutível sobre $\mathbb{K}$. ■

O próximo resultado nos garante uma "transitividade"na propriedade de uma extensão ser algébrica.

Teorema 2.5.25. *Considere os corpos $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$. Então $\mathbb{L}|\mathbb{M}$ e $\mathbb{M}|\mathbb{K}$ são algébricas se, e somente se, $\mathbb{L}|\mathbb{K}$ é algébrica.*

Demonstração. Se $\mathbb{L}|\mathbb{K}$ é algébrica, qualquer elemento $\alpha \in \mathbb{L}$ é algébrico também sobre $\mathbb{M}$, ou seja, $\mathbb{L}|\mathbb{M}$ é algébrica. Além disso, todo $\beta \in \mathbb{M}$ é algébrico sobre $\mathbb{K}$, pois $\beta \in \mathbb{L}$, ou seja, $\mathbb{M}|\mathbb{K}$ é algébrica.

Reciprocamente, suponha que $\mathbb{L}|\mathbb{M}$ e $\mathbb{M}|\mathbb{K}$ são algébricas. Sejam $\alpha \in \mathbb{L}$ e $min_{\alpha,\mathbb{M}} = p(x) = a_0 + a_1x + \cdots + x^n$. Como $\mathbb{M}|\mathbb{K}$ é algébrica, o corpo $\mathbb{M}_0 = \mathbb{K}(a_0, \cdots, a_{n-1})$ é uma extensão finita. Então $p(x) \in \mathbb{M}_0[x]$ e portanto α é algébrico sobre $\mathbb{M}_0$. Logo

$$[\mathbb{M}_0(\alpha):\mathbb{K}] = [\mathbb{M}_0(\alpha):\mathbb{M}_0][\mathbb{M}_0:\mathbb{K}] < \infty.$$

Então $[\mathbb{K}(\alpha)] < \infty$, pois $\mathbb{K}(\alpha) \subset \mathbb{M}_0(\alpha)$. Logo α é algébrico sobre $\mathbb{K}$. Como isso vale para todo $\alpha \in \mathbb{L}$, temos que $\mathbb{L}|\mathbb{K}$ é uma extensão algébrica. ■

Podemos, com esta propriedade transitiva, definir a seguinte operação no conjunto $SC_{\mathbb{L}}$ dos subcorpos de um corpo $\mathbb{L}$. A aplicação $F_{\mathbb{L}} : SC_{\mathbb{L}} \longrightarrow SC_{\mathbb{L}}$ definida por $\mathbb{K} \longmapsto \{\alpha \in \mathbb{L} |\ \alpha \textit{ algebrico sobre } \mathbb{K}\}$ satisfaz, para quaisquer $\mathbb{K}, \mathbb{M} \in SC_{\mathbb{L}}$,

$$\mathbb{K} \subseteq F_{\mathbb{L}}(\mathbb{K}) \quad e \quad \mathbb{K} \subseteq \mathbb{M} \Rightarrow F_{\mathbb{L}}(\mathbb{K}) \subseteq F_{\mathbb{L}}(\mathbb{M}).$$

Uma justificativa que mostra que estas condições são satisfeitas pode ser consultada em [4]. Com isso, podemos definir a imagem de um corpo por esta aplicação, como segue.

Definição 2.5.26. *O corpo $F_{\mathbb{L}}(\mathbb{K}) = \{\alpha \in \mathbb{L};\ \alpha \textit{ algebrico sobre } \mathbb{K}\}$, obtido pela aplicação acima, recebe o nome de fecho algébrico de $\mathbb{K}$ em $\mathbb{L}$.*

Teremos que $F_{\mathbb{L}}(\mathbb{K}) = \mathbb{L}$ se, e somente se, a extensão $\mathbb{L}|\mathbb{K}$ for algébrica. Por outro lado, se $F_{\mathbb{L}}(\mathbb{K}) = \mathbb{K}$, dizemos que $\mathbb{K}$ é *algebricamente fechado* em $\mathbb{L}$. Pelas propriedades da aplicação $F_{\mathbb{L}}$ vale que, para toda extensão $\mathbb{L}|\mathbb{K}$, o corpo $F_{\mathbb{L}}(\mathbb{K})$ é algebricamente fechado em $\mathbb{L}$ [4]. Além disso, como $F_{\mathbb{L}}(\mathbb{K})$ é o conjunto de todo elemento de $\mathbb{L}$ que é algébrico sobre $\mathbb{K}$, então $F_{\mathbb{L}}(\mathbb{K})$ é a maior extensão algébrica de $\mathbb{K}$ contida em $\mathbb{L}$.

2.5.3 Corpo de raízes

Como mencionamos anteriormente, nem sempre um polinômio $p \in \mathbb{K}[x]$ possui necessariamente suas raízes no corpo $\mathbb{K}$. Se o objetivo é estudar as raízes de tal polinômio, é necessário considerar extensões de $\mathbb{K}$, de modo que essas raízes estejam em alguma extensão.

Sabemos, pelo Teorema fundamental da Álgebra, que o corpo $\mathbb{C}$ dos complexos é algebricamente fechado, ou seja, possui todas as raízes de qualquer polinômio. No entanto, estamos interessados na menor extensão de $\mathbb{K}$ que satisfaça esta condição. Veremos nesta seção a existência de tal extensão.

Teorema 2.5.27. *Se $f \in \mathbb{K}[x]$ é um polinômio irredutível, então existe uma extensão $\mathbb{L}|\mathbb{K}$ tal que f possui ao menos uma raiz em $\mathbb{L}$.*

Demonstração. Como f é irredutível, então $\mathbb{K}[x]/\langle f\rangle$ é um corpo. Então colocamos $\mathbb{L} = \mathbb{K}[x]/\langle f\rangle$. Considere o homomorfismo de anéis $\phi : \mathbb{K} \longrightarrow \mathbb{L}$ dado por $\phi(a) = \overline{a} = a + \langle f\rangle$. Temos que ϕ é injetor, pois dado $a \in \mathbb{K}$,

$$a \in Ker_{\phi} \Rightarrow \overline{a} = \overline{0} \Rightarrow f|a \Rightarrow a = 0.$$

Então, pela injetividade de ϕ, $\mathbb{K}$ pode ser visto como um subcorpo de $\mathbb{L}$, podendo assumir $\overline{a} = a$. Mostraremos que $\alpha = \overline{x} = x + \langle f\rangle$ é raiz de f. Considerando $f(x) = a_0 + a_1 + \cdots + a_n x^n$, temos

$$f(\alpha) = \overline{a_0} + \cdots + \overline{a_n x^n} = \overline{a_0 + a_1 + \cdots + a_n x^n} = \overline{0}.$$

Portanto $\mathbb{L}$ é uma extensão de $\mathbb{K}$ que contêm uma raiz α de f. ■

De modo equivalente, este teorema pode ser enunciado da seguinte forma: para todo polinômio $f \in \mathbb{K}[x]$, existem um corpo $\mathbb{L} \supseteq \mathbb{K}$ e $\alpha \in \mathbb{L}$ tais que $(x-\alpha)|f$ em $\mathbb{L}[x]$ pois, nestas condições, α é uma raiz de f em $\mathbb{L}$.

Dada $\mathbb{L}$ uma extensão do corpo $\mathbb{K}$, dizemos que $f \in \mathbb{K}[x]$ *fatora* sobre $\mathbb{L}$ se pode ser escrito como produto de polinômios lineares (de grau 1), ou seja, $f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \in \mathbb{L}[x]$, de modo que $c, \alpha_1, \cdots, \alpha_n \in \mathbb{L}$. Pela proposição abaixo, vemos que qualquer polinômio $f \in \mathbb{K}[x]$ pode ser fatorado em um produto de polinômios lineares sobre um determinado corpo $\mathbb{L} \supseteq \mathbb{K}$.

Proposição 2.5.28. *Para todo polinômio $f \in \mathbb{K}[x] \setminus \{0\}$, com $gr(f) = n$, existem um corpo $\mathbb{L}|\mathbb{K}$ e elementos $c \in \mathbb{K} \setminus \{0\}$ e $\alpha_1, \cdots, \alpha_n \in \mathbb{L}$ tais que $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$.*

Demonstração. Basta mostrar que existem $\alpha_1, \cdots, \alpha_n \in \mathbb{L}_n$ tais que $(x-\alpha_1)\cdots(x-\alpha_n)$ divide f em $\mathbb{L}_n[x]$. Faremos isto por indução sobre $n = gr(f)$. Pelo teorema anterior, vimos que isto vale se $n = 1$, pois se existe $\alpha \in \mathbb{L}$ raiz de f, então $(x-\alpha)|f$. Então suponha que vale para $n-1$, ou seja, existem $\alpha_1, \cdots, \alpha_{n-1} \in \mathbb{L}_{n-1}$ e $f_{n-1} \in \mathbb{L}_{n-1}[x]$ tais que $f(x) = (x-\alpha_1)\cdots(x-\alpha_{n-1})f_{n-1}(x)$. Pelo teorema anterior, existem $\mathbb{L}_n \supseteq \mathbb{L}_{n-1}$ e $\alpha_n \in \mathbb{L}_n$ tais que $f_{n-1} = (x-\alpha_n)f_n$. Portanto $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)f_n$. ■

Os elementos $\alpha_1, \cdots, \alpha_n$ são, evidente, as raízes de f em $\mathbb{L}$, não necessariamente distintas, ou seja, podem ser raízes de multiplicidade maior que 1. Então, pelo Teorema Fundamental da Álgebra, temos que f fatora sobre $\mathbb{K}$ se, e somente se, todas as suas raízes em $\mathbb{C}$ estão em $\mathbb{K}$. Se $\mathbb{L}$ cumpre essa condição, todo corpo $\mathbb{M} \supseteq \mathbb{L}$ também a satisfaz. Deste modo, estamos interessados no menor corpo com estas condições, que definimos a seguir.

Definição 2.5.29. *Dado um polinômio $f \in \mathbb{K}[x]$, dizemos que $\mathbb{L}|\mathbb{K}$ é o corpo de raízes de f, denotado por $\mathbb{L} = \mathbb{K}(R_f)$, se $\mathbb{L}$ é o menor corpo que contêm $\mathbb{K}$ e todas as raízes de f.*

O próximo resultado garante a existência de um corpo de raízes, para qualquer polinômio sobre um corpo.

Teorema 2.5.30. *(Existência do corpo de raízes) Todo polinômio $f \in \mathbb{K}[x] \setminus \{0\}$ possui um corpo de raízes.*

Demonstração. Faremos a prova por indução sobre $n = gr(f)$. Se $n = 1$, então f possui uma raiz única em $\mathbb{K}$, e portanto $\mathbb{K} = \mathbb{K}(R_f)$. Agora, suponha que seja válido para todo $g \in \mathbb{K}[x]$, com $gr(g) < n$. Pelo teorema acima, existe uma extensão $\mathbb{L}|\mathbb{K}$ que contêm ao menos uma raiz α de f. Então $f = (x-\alpha)g$ com $gr(g) < gr(f)$. Portanto, pela hipótese de indução, existe um corpo contendo todas as raízes de g. Se $\mathbb{M}$ é o menor corpo que satisfaz essas condições, temos que $\mathbb{M}(\alpha) = \mathbb{K}(R_f)$. ■

Podemos estender esta noção, de maneira equivalente, da seguinte forma: dado um corpo $\mathbb{K}$ um polinômio f sobre $\mathbb{K}$, podemos determinar uma extensão $\mathbb{F}$ de $\mathbb{K}$ tal que f fatora sobre $\mathbb{F}$ e, além disso, de modo que f não fatore sobre nenhum corpo menor que $\mathbb{F}$. Temos então a seguinte definição.

Definição 2.5.31. *Um corpo $\mathbb{F}$ é chamado de corpo de fatoração (splitting field) do polinômio f sobre o corpo $\mathbb{K}$ se $\mathbb{K} \subseteq \mathbb{F}$ e*

1. *f fatora sobre $\mathbb{F}$,*
2. *se $\mathbb{K} \subseteq \mathbb{F}' \subseteq \mathbb{F}$ e f fatora sobre $\mathbb{F}'$, então $\mathbb{F}' = \mathbb{F}$.*

Segue da segunda parte da definição que $\mathbb{F} = \mathbb{K}(\alpha_1, \alpha_2, \cdots, \alpha_n)$, nas quais $\alpha_1, \alpha_2, \cdots, \alpha_n$ são as raízes de f em $\mathbb{L}$, ou seja, $\mathbb{F}$ é uma extensão finitamente gerada de $\mathbb{K}$. Todo polinômio sobre um corpo $\mathbb{K}$ possui um corpo de fatoração, como garante o teorema a seguir, que também trata de sua unicidade, cuja justificativa pode ser encontrada em [8].

Teorema 2.5.32. *Seja $f \in \mathbb{K}[x]$. Existe um único corpo de fatoração $\mathbb{F}$ de f sobre $\mathbb{K}$. Além disso, $[\mathbb{F} : \mathbb{K}] = n$.*

A finitude da extensão segue do fato de $\mathbb{F} = \mathbb{K}(\alpha_1, \cdots, \alpha_n)$ ser finitamente gerada e algébrica. Os corpos de fatoração possuem uma conexão com um caso particular de extensões, denominada extensão normal, que definimos a seguir. Esta conexão é dada no teorema seguinte, cuja demonstração pode ser consultada em [8].

Definição 2.5.33. *Uma extensão de corpos $\mathbb{L}|\mathbb{K}$ é dita normal se todo polinômio irredutível $f \in \mathbb{K}[x]$ que possui ao menos uma raiz em $\mathbb{L}$ fatora em $\mathbb{L}$.*

Teorema 2.5.34. *[8] Uma extensão $\mathbb{L}|\mathbb{K}$ é normal e finita se, e somente se, $\mathbb{L}$ é um corpo de fatoração para algum polinômio sobre $\mathbb{K}$.*

Anteriormente, definimos que um corpo $\mathbb{K}$ é algebricamente fechado sobre um corpo $\mathbb{L} \supseteq \mathbb{K}$ se o fecho algébrico de $\mathbb{K}$ em $\mathbb{L}$ é tal que $F_{\mathbb{L}}(\mathbb{K}) = \mathbb{L}$. Podemos estender esta noção da seguinte forma.

Definição 2.5.35. *Um corpo $\mathbb{K}$ é dito algebricamente fechado se é algebricamente fechado em $\mathbb{L}$, para toda extensão $\mathbb{L}$ de $\mathbb{K}$.*

Podemos caracterizar corpos algebricamente fechados de acordo com o seguinte resultado.

Proposição 2.5.36. *[4] Dado um corpo $\mathbb{K}$, as seguintes condições são equivalentes:*

(i) $\mathbb{K}$ é algebricamente fechado;

(ii) todo polinômio $f \in \mathbb{K}[x] \setminus \mathbb{K}$ tem uma raiz em $\mathbb{K}$;

(iii) todo polinômio irredutível $p \in \mathbb{K}[x]$ tem grau 1;

(iv) todo $f \in \mathbb{K}[x] \setminus \{0\}$ fatora-se em $\mathbb{K}[x]$ em polinômios lineares;

(v) $\mathbb{K}$ não possui nenhuma extensão algébrica $\mathbb{L}|\mathbb{K}$.

Demonstração. $(i) \Rightarrow (ii)$: Sabemos que existem $\mathbb{L} \supseteq \mathbb{K}$ e $\alpha \in \mathbb{L}$ tais que $x-\alpha|f$. Como $\mathbb{K}$ é algebricamente fechado, então α é algébrico sobre $\mathbb{K}$. Logo $\alpha \in F_{\mathbb{L}}(\mathbb{K}) = \mathbb{K}$, ou seja, α é uma raiz de f em $\mathbb{K}$.

$(ii) \Rightarrow (iii)$: Por hipótese, p possui uma raiz $\beta \in \mathbb{K}$, portanto $x-\beta|p$ em $\mathbb{K}[x]$. Como p é irredutível, associado à $x-\beta$, então $gr(p) = 1$.

$(iii) \Rightarrow (iv)$: Denotamos a fatoração de $f = a \cdot p_1 \cdots p_r$ em polinômios irredutíveis $p_1, \cdots, p_r \in \mathbb{K}[x]$, com $a \in \mathbb{K} \setminus \{0\}$. Então $gr(p_1) = \cdots = gr(p_r) = 1$.

$(iv) \Rightarrow (v)$: Supondo que $\mathbb{K}$ possui uma extensão algébrica $\mathbb{L} \supseteq \mathbb{K}$, então existe $\alpha \in \mathbb{L}$ tal que $gr(min_{\alpha,\mathbb{K}}) > 1$. Como $min_{\alpha,\mathbb{K}}$ é irredutível em $\mathbb{K}$, isto contradiz a hipótese de (iv).

$(v) \Rightarrow (i)$: Supondo que $\mathbb{K}$ não é algebricamente fechado, então $\mathbb{K} \subset F_{\mathbb{L}}(\mathbb{K})$ para alguma extensão $\mathbb{L}$ de $\mathbb{K}$, o que contradiz a hipótese de (v). ■

2.5.4 Extensões Separáveis

Nesta seção, estudaremos um caso especial de extensões de corpos tomando como base a multiplicidade das raízes de um polinômio minimal. Focaremos nos elementos $\alpha \in \mathbb{L}$ que são algébricos sobre $\mathbb{K}$ e, além disso, são raízes simples do polinômio minimal $min_{\alpha,\mathbb{K}}$.

Lembramos que uma raiz α de um polinômio $f \in \mathbb{K}[x]$ tem multiplicidade igual à $max\{m \in \mathbb{N} \mid (x-\alpha)^m | f\}$. 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.

Para determinar a multiplicidade de uma raiz α do polinômio $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{K}[x]$, utilizamos a derivada $D : \mathbb{K}[x] \longrightarrow \mathbb{K}[x]$ definida por

$$\sum_{i=0}^{n} a_i x^i \longmapsto \sum_{i=1}^{n} i \cdot a_i x^{i-1}.$$

Denotamos a derivada de f por Df ou f'. Quando $\mathbb{K}$ é um domínio, temos que $Df = 0$ se, e só se, $\begin{cases} f \in \mathbb{K} \ \ quando \ \ car(\mathbb{K}) = 0 \\ f \in \mathbb{K}[x^p] \ \ quando \ \ car(\mathbb{K}) = p \ (p \ primo). \end{cases}$

Uma condição necessária e suficiente para que uma raiz α de um polinômio $f \in \mathbb{K}[x]$ seja simples é que $Df(\alpha) \neq 0$ [4].

Colocados estes conceitos iniciais, estamos interessados nos polinômios cujas raízes são todas simples, como definimos a seguir.

Definição 2.5.37. *Um polinômio $f \in \mathbb{K}[x]$ é dito separável se todas as suas raízes são simples no seu corpo de raízes. Caso contrário, f é dito inseparável.*

De maneira equivalente podemos dizer que $f \in \mathbb{K}[x]$ é separável sobre $\mathbb{K}$ se possui raízes simples no seu corpo de fatoração. Ou seja, f tem a seguinte forma sobre seu corpo de fatoração:

$$f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),$$

de modo que os elementos α_i são todos diferentes.

A proposição a seguir nos garante que todo polinômio irredutível é separável. Antes, enunciamos o seguinte lema, cuja demonstração, que pode ser consultada em [8], omitiremos.

Lema 2.5.38. *Se $0 \neq f \in \mathbb{K}[x]$ é um polinômio e $\mathbb{F}$ é seu corpo de fatoração, então f possui uma raiz múltipla se, e só se, f e Df possuem um fator comum de grau ≥ 1 em $\mathbb{F}[x]$.*

Proposição 2.5.39. *Seja $\mathbb{K}$ um subcorpo de $\mathbb{C}$. Todo polinômio irredutível sobre $\mathbb{K}$ é separável.*

Demonstração. Pelo lema acima, um polinômio $f \in \mathbb{K}[x]$ é inseparável se, e só se, f e Df possuem um fator comum de grau ≥ 1. Desse modo, como f é irredutível o fator comum deve ser f. Mas Df possui grau menor que f, e o único múltiplo de f de menor grau é $p = 0$, portanto $Df = 0$. Logo, se $f(x) = a_0 + a_1x + \cdots + a_mx^m$, isto equivale a $na_n = 0$ para todo inteiro $n > 0$. Para subcorpos de $\mathbb{C}$, isto equivale a $a_n = 0$, para todo n. Logo todo polinômio irredutível $f \neq 0$ é separável. ■

Além disso, temos o seguinte resultado para a separabilidade de um polinômio irredutível f, que envolve a condição $Df \neq 0$. A justificativa é simples, e pode ser encontrada em [4].

Proposição 2.5.40. *Para todo polinômio irredutível $f \in \mathbb{K}[x]$ são equivalentes as seguintes condições:*

1. *f é separável,*
2. *existem um corpo $\mathbb{L} \supseteq \mathbb{K}$ e $\alpha \in \mathbb{L}$ tais que α é raiz simples de f,*
3. *$Df \neq 0$.*

Estas condições são satisfeitas quando $car(\mathbb{K}) = 0$ ou $car(\mathbb{K}) = p \neq 0$ e $f \notin \mathbb{K}[x^p]$.

Como mencionado no início da seção, estamos interessados no conjunto de elementos $\alpha \in \mathbb{L}$ que são, ao mesmo tempo, algébricos sobre $\mathbb{K}$ e raízes simples do polinômio minimal $min_{\alpha,\mathbb{K}}$. Nesse sentido, estendemos a noção de separabilidade para elementos de um corpo e para extensões de corpos, como segue.

Definição 2.5.41. *Seja $\mathbb{L}|\mathbb{K}$ uma extensão de corpos e $\alpha \in \mathbb{L}$. Dizemos que α é um elemento separável sobre $\mathbb{K}$ se o polinômio minimal $p = min_{\alpha,\mathbb{K}}$ é separável. Se todo elemento $\alpha \in \mathbb{L}$ é separável sobre $\mathbb{K}$, então $\mathbb{L}|\mathbb{K}$ é dita uma extensão separável. Caso contrário, $\mathbb{L}|\mathbb{K}$ é inseparável.*

O resultado a seguir nos garante uma condição suficiente para que uma extensão algébrica seja separável.

Proposição 2.5.42. *Se $\mathbb{L}|\mathbb{K}$ é uma extensão algébrica e $car(\mathbb{K}) = 0$, então $\mathbb{L}|\mathbb{K}$ é separável.*

Demonstração. Considere o elemento $\alpha \in \mathbb{L}$ e seu polinômio minimal $p = min_{\alpha,\mathbb{K}}$. Como $car(\mathbb{K}) = 0$, temos que $gr(Dp) = gr(p) - 1$. Como p é minimal de α sobre $\mathbb{K}$, então $Dp(\alpha) \neq 0$, ou seja, α é uma raiz simples de p. Portanto p é separável, de onde segue que α é separável. Como supomos isto válido para qualquer $\alpha \in \mathbb{L}$, segue que $\mathbb{L}|\mathbb{K}$ é separável. ■

O corolário a seguir é consequência direta da última proposição.

Corolário 2.5.43. *Seja $\mathbb{L}|\mathbb{K}$ uma extensão algébrica com $car(\mathbb{K}) = 0$. Se f é irredutível sobre $\mathbb{K}$ e $gr(f) = n$, então f possui n raízes distintas no seu corpo de raízes.*

A proposição a seguir nos garante a "transitividade"da propriedade de ser separável.

Proposição 2.5.44. *Sejam $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ corpos tal que $\mathbb{L}|\mathbb{K}$ é uma extensão separável. Então $\mathbb{M}|\mathbb{K}$ e $\mathbb{L}|\mathbb{M}$ são separáveis.*

Demonstração. A separabilidade de $\mathbb{M}|\mathbb{K}$ decorre direto de $\mathbb{L}|\mathbb{K}$. Para mostrar para $\mathbb{L}|\mathbb{M}$, considere $\alpha \in \mathbb{L}$ e $p = min_{\alpha,\mathbb{K}}$ e $q = min_{\alpha,\mathbb{M}}$. Temos então que q divide p em $\mathbb{M}[x]$ e que todas as raízes de q em $\mathbb{M}$ são também raízes de p. Como α é separável sobre $\mathbb{K}$, então p é separável sobre $\mathbb{K}$, de onde segue que q é separável sobre $\mathbb{M}$. Portanto α é separável sobre $\mathbb{M}$, ou seja, $\mathbb{L}|\mathbb{M}$ é separável. ■

A seguir, definimos um caso particular de corpo $\mathbb{K}$ tal que todo polinômio irredutível em $\mathbb{K}[x]$ é separável. Além disso, veremos que este corpo se relaciona com o conceito de extensão separável.

Definição 2.5.45. *Um corpo $\mathbb{K}$ é dito perfeito quando $car(\mathbb{K}) = 0$ ou $car(\mathbb{K}) = p \neq 0$ e $\mathbb{K}^p = \mathbb{K}$, com p primo.*

Além disso, se $car(\mathbb{K}) = p$, então a aplicação $\pi : \mathbb{K} \longrightarrow \mathbb{K}$ definida por $a \longmapsto a^p$ é um monomorfismo com imagem $Im(\pi) = \mathbb{K}^p = \mathbb{K}$ [4]. Portanto $\mathbb{K}$ será perfeito se, e somente se, π for bijetiva, ou seja, um automorfismo de $\mathbb{K}$. O seguinte resultado nos garante uma condição necessária e suficiente para que um corpo seja perfeito.

Proposição 2.5.46. *Um corpo $\mathbb{K}$ é perfeito se, e somente se, todo polinômio irredutível $f \in \mathbb{K}[x]$ é separável.*

Demonstração. Se $car(\mathbb{K}) = 0$, vimos pelo corolário anterior que f é separável. Então considere $\mathbb{K}$ um corpo perfeito com $car(\mathbb{K}) = p > 0$. Suponha que $f \in \mathbb{K}[x]$ é irredutível e $f \in \mathbb{K}[x^p]$, ou seja, f não é separável, da forma $f(x) = \sum_{j=0}^{n} a_j x^{p \cdot j}$. Como $\mathbb{K}$ é prefeito, existem $b_j \in \mathbb{K}$ tais que $a_j = b_j^p$, par $j = 0, 1, \cdots, n$. Logo $f(x) = (\sum_{j=0}^{n} b_j x_j)^p$, o que contradiz a irredutibilidade de f. Portanto f é separável.

Reciprocamente, seja $a \in \mathbb{K}$ e $f(x) = x^p - a$ separável. Sabemos que existem $\mathbb{L} \supseteq \mathbb{K}$ e $\alpha \in \text{Ł}$ tais que $f(\alpha) = 0$ em $\mathbb{L}$. Logo $\alpha^p = a$, ou seja, $f(x) = (x - \alpha)^p$. Como $min_{\alpha,\mathbb{K}}$ divide f, temos

que $min_{\alpha,\mathbb{K}} = (x-\alpha)^r$ para $1 \leq r \leq p$ e, supondo $min_{\alpha,\mathbb{K}}$ separável, temos $r = 1$. Disto resulta que $x - \alpha \in \mathbb{K}[x]$, logo $\alpha \in \mathbb{K}$ e $a \in \mathbb{K}^p$. Isto mostra que $\mathbb{K} \subseteq \mathbb{K}^p$, ou seja, $\mathbb{K}$ é perfeito. ■

Com isso, temos a seguinte proposição, que nos permite caracterizar um corpo perfeito de acordo com extensões separáveis.

Teorema 2.5.47. *Um corpo $\mathbb{K}$ é perfeito se, e somente se, toda extensão algébrica de $\mathbb{K}$ é separável.*

Demonstração. Primeiro, suponha que $\mathbb{K}$ é perfeito e que $\mathbb{L}|\mathbb{K}$ é uma extensão algébrica. Dado qualquer $\alpha \in \mathbb{L}$, temos que $min_{\alpha,\mathbb{K}}$ é separável, pois é irredutível. Portanto α é separável sobre $\mathbb{K}$, e como supomos isto para todo $\alpha \in \mathbb{L}$, segue que $\mathbb{L}|\mathbb{K}$ é uma extensão separável.

Reciprocamente, suponha que toda extensão de $\mathbb{K}$ é separável e que $\mathbb{K}$ não é perfeito. Então deve existir um polinômio irredutível $p \in \mathbb{K}[x]$ que é inseparável. Deste modo, existem $\mathbb{L} \supseteq \mathbb{K}$ e $\alpha \in \mathbb{L}$ tais que $p = min_{\alpha,\mathbb{K}}$. Então α é inseparável sobre $\mathbb{K}$ e, portanto, $\mathbb{K}(\alpha)|\mathbb{K}$ é inseparável, uma contradição. Logo $\mathbb{K}$ é perfeito. ■

2.5.5 Teorema do Elemento Primitivo

A seguir, apresentamos um importante conceito que está estritamente ligado à noção de separabilidade. Mostraremos, deste modo, a existência do chamado elemento primitivo e da extensão de corpos ligada a ele. Veremos, na sequência, o importante Teorema do elemento primitivo, que nos traz uma condição necessária e suficiente para caracterizar esta extensão associada ao elemento em questão.

Definição 2.5.48. *Dizemos que $\alpha \in \mathbb{L}$ é um elemento primitivo da extensão $\mathbb{L}|\mathbb{K}$ se $\mathbb{L} = \mathbb{K}(\alpha)$ e se α é algébrico sobre $\mathbb{K}$. Neste caso, dizemos que $\mathbb{L}|\mathbb{K}$ é uma extensão simples.*

Ou seja, $\mathbb{L}|\mathbb{K}$ é simples quando é finitamente gerada pela adjunção do elemento primitivo α. Então $\mathbb{L}|\mathbb{K}$ é obviamente uma extensão finita. No entanto, nem toda extensão finita possui elemento primitivo. O teorema a seguir nos garante uma condição necessária e suficiente para que uma extensão seja simples.

Teorema 2.5.49. *(do Elemento Primitivo) Uma extensão finita $\mathbb{L}|\mathbb{K}$ é simples se, e somente se, existe um número finito de corpos $\mathbb{M}$ tais que $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$.*

Demonstração. Faremos a prova para o caso em que o corpo $\mathbb{K}$ possui infinitos elementos. Primeiro, suponha que exista apenas um número finito de corpos entre $\mathbb{K}$ e $\mathbb{L}$. Como $\mathbb{L}|\mathbb{K}$ é finito, podemos reescrever como $\mathbb{L} = \mathbb{K}(\alpha_1, \cdots, \alpha_n)$, com $\alpha_1, \cdots, \alpha_n \in \mathbb{L}$. Faremos a prova por indução sobre n. Se $n = 1$, é trivial que a extensão é simples, pois $\mathbb{L} = \mathbb{K}(\alpha)$. Supondo $\mathbb{L} = \mathbb{K}(\alpha_1, \cdots, \alpha_{n-1})$, então como todo corpo entre $\mathbb{K}$ e $\mathbb{M}$ é intermediário em $\mathbb{L}|\mathbb{K}$, por indução temos que $\mathbb{M} = \mathbb{K}(\beta)$. Então temos $\mathbb{L} = \mathbb{K}(\alpha_n, \beta)$. Dado $a \in \mathbb{L}$, considere o corpo $\mathbb{F}_a = \mathbb{K}(\alpha_n + a\beta)$ intermediário em $\mathbb{L}|\mathbb{K}$. Como, por hipótese, existe apenas um número finito de tais corpos intermediários, com $\mathbb{K}$ tendo infinitos elementos, existem $a, b \in \mathbb{K}$ tais que $a \neq b$ e $\mathbb{F}_a = \mathbb{F}_b$. Então temos que

$$\beta = \frac{(\alpha_n + b\beta) - (\alpha_n + a\beta)}{b - a} \in \mathbb{F}_b.$$

Segue então que $\alpha_n = (\alpha_n + b\beta) - b\beta \in \mathbb{F}_b$, ou seja, $\mathbb{L} = \mathbb{K}(\alpha_n, \beta) = \mathbb{F}_b$. Portanto $\mathbb{L}|\mathbb{K}$ é uma extensão simples.

Reciprocamente, suponha que $\mathbb{L}|\mathbb{K}$ é simples, ou seja, $\mathbb{L} = \mathbb{K}(\alpha)$, para algum $\alpha \in \mathbb{K}$. Se $\mathbb{M}$ é um corpo entre $\mathbb{L}$ e $\mathbb{K}$, então $\mathbb{L} = \mathbb{M}(\alpha)$. Agora, considere os polinômios minimais $p = min_{\alpha}, \mathbb{K}$ e $q = min_{\alpha,\mathbb{M}} \in \mathbb{M}[x]$. Então q divide p em $\mathbb{M}[x]$. Supondo $q(x) = a_0 + a_1 x + \cdots + x^r$, considere $\mathbb{M}_0 = \mathbb{K}(a_0, \cdots, a_{r-1}) \in \mathbb{M}$. Então $q \in \mathbb{M}_0[x]$, de onde segue que $min_{\alpha,\mathbb{M}_0}$ divide q. Logo, temos

$$[\mathbb{L} : \mathbb{M}] = gr(q) \geq gr(min_{\alpha,\mathbb{M}_0}) = [\mathbb{L} : \mathbb{M}_0] = [\mathbb{L} : \mathbb{M}] \cdot [\mathbb{M} : \mathbb{M}_0].$$

Isto implica que $[\mathbb{M} : \mathbb{M}_0] = 1$, ou seja, $\mathbb{M}_0 = \mathbb{M}$. Isto significa que $\mathbb{M}$ é determinado pelo minimal q. Mas existem apenas um número finito de polinômios mônicos divisores de p em $\mathbb{L}[x]$. Portanto existe apenas um número finito de corpos tais como $\mathbb{M}$, ou seja, intermediários entre $\mathbb{K}$ e $\mathbb{L}$. ■

Podemos generalizar o Teorema do Elemento Primitivo para um número finito de elementos geradores da extensão, considerando um corpo $\mathbb{K}$ de cardinalidade infinita.

Teorema 2.5.50. *[4] Considere a extensão $\mathbb{L} = \mathbb{K}(\alpha, \beta_1, \cdots, \beta_r)|\mathbb{K}$, na qual α é algébrico e $\beta_1, \cdots, \beta_r$ são separáveis sobre $\mathbb{K}$, com $n_j = [\mathbb{K}(\beta_j) : \mathbb{K}]$, $j = 0, 1, \cdots, r$ com $\beta_0 = \alpha$. Então em todo subconjunto $C \subseteq \mathbb{K}$ com cardinalidade maior que $n_0 \cdot n_1 \cdots n_{r-1} \cdot (n_r - 1)$ exstem $\lambda_1, \cdots, \lambda_r$ tais que $\mathbb{L} = \mathbb{K}(\alpha + \lambda_1\beta_1 + \cdots + \lambda_r\beta_r)$.*

A demonstração é feita de forma semelhante ao teorema anterior, construindo sucessivamente elementos $\lambda_1, \cdots, \lambda_r \in C$ tais que $\mathbb{K}(\alpha, \beta_1, \cdots, \beta_j) = \mathbb{K}(\alpha_{j-1}, \beta_j) = \mathbb{K}(\alpha_j)$, tal que $\alpha_j = \alpha + \lambda_1\beta_1 + \cdots + \lambda_j\beta_j$.

O seguinte corolário garante a existência do elemento primitivo, e da extensão simples, quando uma extensão é separável, consequência do teorema anterior. A prova pode ser consultada em [4].

Corolário 2.5.51. *Dada uma extensão $\mathbb{L} = \mathbb{K}(\alpha, \beta_1, \cdots, \beta_r)|\mathbb{K}$, onde α é algébrico e $\beta_1, \cdots, \beta_r$ são separáveis sobre $\mathbb{K}$, então $\mathbb{L}|\mathbb{K}$ possui um elemento primitivo, ou seja, $\mathbb{L} = \mathbb{K}(\alpha)$. Em particular, toda extensão finita separável possui elemento primitivo.*

O resultado a seguir traz um caso particular, considerando extensões sobre o corpo dos racionais.

Teorema 2.5.52. *Sejam $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{C}$ corpos tais que $\mathbb{L}|\mathbb{K}$ é uma extensão finita. Então existe $\gamma \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\alpha)$.*

Demonstração. Como $\mathbb{L}|\mathbb{K}$ é finita, existe uma base de elementos algébricos $\{\alpha_1, \cdots, \alpha_n\}$ de $\mathbb{L}$ vista como $\mathbb{K}$-espaço vetorial tal que $\mathbb{L} = \mathbb{K}(\alpha_1, \cdots, \alpha_n)$. Faremos a prova por indução sobre n, bastando mostrar para o caso $n = 2$, ou seja, se $\mathbb{L} = \mathbb{K}(\alpha, \beta)$ então existe $\gamma \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\gamma)$. Considere os polinômios minimais $p = min_{\alpha,\mathbb{K}}$ e $q = min_{\beta,\mathbb{K}}$ tais que $gr(p) = r$ e $gr(q) = s$. Então p e q possuem r e s raízes distintas em $\mathbb{C}$, respectivamente, pois são irredutíveis e $car(\mathbb{Q}) = 0$. Então suponha $R_p = \{\alpha_1 = \alpha, \cdots, \alpha_r\}$ e $R_q = \{\beta_1 = \beta, \cdots, \beta_s\}$. Considere $\lambda_{ij} = \frac{\alpha_i - \alpha}{\beta - \beta_j} \in \mathbb{C}$, com $i = 1, \cdots, r$ e $j = 2, \cdots, s$. Como $\mathbb{K}$ tem cardinalidade infinita, existe $\lambda \in \mathbb{K} \setminus \{\lambda_{ij}; 1 \leq i \leq r, 2 \leq j \leq s\}$.

Considere $\gamma := \alpha + \lambda\beta$ e $f(x) := p(\gamma - \lambda x)$. Então temos $f \in \mathbb{K}(\gamma)[x]$ e que $f(\beta) = p(\gamma - \lambda\beta) = p(\alpha) = 0$. Afirmamos que $\forall j$, $f(\beta_j) \neq 0$. Se não fosse, ou seja, se existe $j \neq 1$ tal que $f(\beta_j) = 0$, então $p(\gamma - \lambda\beta_j) = 0$, ou seja, $\gamma - \lambda\beta_j = \alpha_i$, para algum i. Teríamos então $\alpha + \lambda\beta - \lambda\beta_j = \alpha_i - \alpha$, ou seja, $\lambda = \frac{\alpha_i - \alpha}{\beta - \beta_j}$, o que contradiz a escolha de λ. Então temos $f(\beta_j) \neq 0$, o que garante que $mdc_{\mathbb{C}[x]}(f, q) = (x - \beta)$.

Como $\mathbb{K}(\gamma)[x] \subseteq \mathbb{C}[x]$, temos que $mdc_{\mathbb{K}(\gamma)[x]}(f,q) | mdc_{\mathbb{C}[x]}(f,q)$, ou seja, $mdc_{\mathbb{K}(\gamma)[x]}(f,q) = 1$ ou $mdc_{\mathbb{K}(\gamma)[x]}(f,q) = x - \beta$. Se $mdc_{\mathbb{K}(\gamma)[x]}(f,q) = 1$, então teríamos $mdc_{\mathbb{C}[x]}(f,q) = 1$, pois $\mathbb{K}(\gamma)[x] \subseteq \mathbb{C}[x]$. Então $mdc_{\mathbb{K}(\gamma)[x]}(f,q) = x - \beta$, o que implica em $\beta \in \mathbb{K}[\gamma]$. Como $\alpha = \gamma - \lambda\beta$, segue que $\alpha, \beta \in \mathbb{K}(\gamma)$ e portanto $\mathbb{L} = \mathbb{K}(\alpha,\beta) \subseteq \mathbb{K}(\gamma)$. Além disso, $\gamma \in \mathbb{L}$ e $\mathbb{K} \subseteq \mathbb{L}$ implicam em $\mathbb{K}(\gamma) \in \mathbb{L}$. Portanto $\mathbb{L} = \mathbb{K}(\gamma)$, como queríamos mostrar. ■

Para finalizar esta seção, apresentamos o seguinte teorema, que estende a ideia de extensão para isomorfismos de corpos. Omitiremos a prova, que pode ser consultada em [11].

Teorema 2.5.53. *(Extensão de Isomorfismos) Sejam $\sigma : \mathbb{K} \longrightarrow \mathbb{K}'$ um isomorfismo de corpos, $S = \{f_i(x)\}$ um conjunto de polinômios sobre $\mathbb{K}$ e $S' = \{\sigma(f_i(x))\}$ o conjunto correspondente em $\mathbb{K}'$. Seja $\mathbb{L}$ um corpo de fatoração para S sobre $\mathbb{K}$ e $\mathbb{L}'$ um corpo de fatoração para S' sobre $\mathbb{K}'$. então existe um isomorfismo $\tau : \mathbb{L} \longrightarrow \mathbb{L}'$ tal que $\tau_{|\mathbb{K}} = \sigma$. Além disso, se $\alpha \in \mathbb{L}$ e β é uma raiz de $\sigma(min_{\alpha,\mathbb{K}})$ em $\mathbb{L}'$, então τ pode ser escolhido de forma que $\tau(\alpha) = \beta$.*

CAPÍTULO

3

Teoria algébrica dos números

Neste capítulo são apresentados os principais conceitos e propriedades da teoria algébrica dos números, essenciais para nosso trabalho, com foco inicial à Teoria de Galois. Sua ideia principal foi associar a cada polinômio f um grupo de permutações das raízes de f e, de modo correspondente, associar a cada extensão de corpos um grupo, conhecido como grupo de Galois, que estudaremos a seguir.

Antes disso, definimos um caso especial de extensões de corpos, presentes no trabalho de Galois ao estudar as raízes de equações polinomiais. Uma extensão finita $\mathbb{L}|\mathbb{K}$ é chamada Galoiseana ou de Galois se $\mathbb{L}$ é o corpo de raízes de f sobre $\mathbb{K}$, para algum polinômio separável $f \in \mathbb{K}[x]$.

Uma condição necessária e suficiente para que uma extensão finita $\mathbb{L}|\mathbb{K}$ seja de Galois é que $\mathbb{L}|\mathbb{K}$ seja normal e separável. Uma justificativa detalhada pode ser vista em [10]. Além disso, se $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{L}$ são corpos tal que $\mathbb{L}|\mathbb{K}$ é de Galois, então $\mathbb{L}|\mathbb{F}$ é de Galois [10].

3.1 Grupo de Galois

Lembramos que um automorfismo em um corpo $\mathbb{L}$ é um isomorfismo de anéis de $\mathbb{L}$ em $\mathbb{L}$. Denotamos o conjunto de todos os automorfismos de $\mathbb{L}$ por $Aut(\mathbb{L})$. É fácil verificar que $(Aut(\mathbb{L}), \circ)$ é um grupo, no qual $\circ$ representa a composição entre funções e a aplicação identidade $Id \in Aut(\mathbb{L})$ é seu elemento neutro.

Se $\mathbb{L}$ e $\mathbb{F}$ são extensões do corpo $\mathbb{K}$, definimos o $\mathbb{K}$-*homomorfismo* $\tau : \mathbb{L} \longrightarrow \mathbb{F}$ como o homomorfismo de anéis tal que $\tau(a) = a$, para todo $a \in \mathbb{K}$, ou seja, $\tau_{|\mathbb{K}} = Id$. Se τ é injetiva, é chamada de $\mathbb{K}$-monomorfismo, e se for bijetiva recebe o nome de $\mathbb{K}$-isomorfismo. Se τ é um $\mathbb{K}$-isomorfismo de $\mathbb{L}$ em $\mathbb{L}$, recebe o nome de $\mathbb{K}$-automorfismo.

Além disso, se $\tau : \mathbb{L} \longrightarrow \mathbb{F}$ é um $\mathbb{K}$-homomorfismo entre extensões de $\mathbb{K}$, então τ é também uma transformação linear de $\mathbb{K}$-espaços vetoriais, pois $\tau(\alpha a) = \tau(\alpha)\tau(a) = \alpha\tau(a)$, dados $\alpha \in \mathbb{K}$ e $a \in \mathbb{L}$. Então, como $\tau \neq 0$ e $\mathbb{L}$ é um corpo, temos τ injetiva. Por outro lado, se $[\mathbb{L} : \mathbb{K}] = [\mathbb{F} : \mathbb{K}] < \infty$, então τ é sobrejetiva por propriedade da dimensão. Em particular, temos que se $[\mathbb{L} : \mathbb{K}] < \infty$ então todo $\mathbb{K}$-homomorfismo de $\mathbb{L}$ em $\mathbb{L}$ é uma bijeção, ou seja, um $\mathbb{K}$-automorfismo. Dados estes conceitos preliminares, podemos definir o grupo de Galois de uma extensão, como segue.

Definição 3.1.1. *Seja $\mathbb{L}$ uma extensão do corpo $\mathbb{K}$. O grupo de Galois de $\mathbb{L}|\mathbb{K}$, denotado por $Gal(\mathbb{L}|\mathbb{K})$, é definido pelo conjunto de todos os $\mathbb{K}$-automorfismos de $\mathbb{L}$, ou seja,*

$$Gal(\mathbb{L}|\mathbb{K}) = \left\{p \in Aut(\mathbb{L});\ p_{|\mathbb{K}} = Id\right\}.$$

Se $\mathbb{L}|\mathbb{K}$ é extensão Galoisiana, ou seja, $\mathbb{L}$ é o corpo de raízes de $f \in \mathbb{K}[x]$, então $Gal(\mathbb{L}|\mathbb{K})$ recebe o nome de grupo de Galois de f sobre $\mathbb{K}$. Além disso, vemos que $Gal(\mathbb{L}|\mathbb{K})$ é um subgrupo do grupo dos automorfismos $Aut(\mathbb{L})$ com relação a composição entre funções.

O grupo de Galois de uma extensão galoisiana $\mathbb{L}|\mathbb{K}$ foi introduzido desta forma, como subgrupo de $Aut(\mathbb{L})$, por Dedekind posteriormente ao trabalho de Galois, que por sua vez havia estudado um grupo de permutações das raízes de um polinômio. Deste modo, traremos este grupo de permutações, também chamado grupo da equação $f(x) = 0$, através da proposição abaixo.

Proposição 3.1.2. *[4] Seja $\mathbb{L} = \mathbb{K}(R_f)$ o corpo das raízes de $f \in \mathbb{K}[x]$, mônico e separável. Então:*

1. *Dado $\sigma \in Aut(\mathbb{L})$, a restrição $\sigma_{|R_f}$ é uma permutação de R_f, em que $R_f = \{a \in \mathbb{L};\ f(a) = 0\}$ é o conjunto das raízes de f no corpo $\mathbb{L}$ algebricamente fechado.*
2. *Dado $\sigma \in Aut(\mathbb{L})$, é definido por $\sigma \longmapsto \sigma|_{R_f}$ um homomorfismo necessariamente injetivo de $Aut(\mathbb{L})$ no grupo S_{R_f} de todas as permutações de R_f.*

O subgrupo $\left\{\sigma_{|R_f};\ \sigma \in Aut(\mathbb{L})\right\}$ do grupo S_{R_f}, imagem deste homomorfismo, é chamado de *grupo de f* ou grupo da equação $f = 0$ sobre $\mathbb{K}$.

Se $\mathbb{L}$ é uma extensão do corpo $\mathbb{K}$ gerado pela adjunção do conjunto das raízes de um polinômio $f \in \mathbb{K}[x]$, os próximos dois lemas mostram que podemos interpretar o grupo de Galois $Gal(\mathbb{L}|\mathbb{K})$ como um grupo de permutações das raízes de f. Começamos com o caso geral onde $\mathbb{L} = \mathbb{K}(X)$ é gerado sobre $\mathbb{K}$ pela adjunção de um subconjunto X, no qual podemos determinar $\mathbb{K}$-automorfismos de $\mathbb{L}$ em termos de sua ação sobre X. A prova pode ser consultada em [11].

Lema 3.1.3. *Seja $\mathbb{L} = \mathbb{K}(X)$ uma extensão de $\mathbb{K}$ gerada por $X \subset \mathbb{L}$. Se $\tau, \varphi \in Gal(\mathbb{L}|\mathbb{K})$ são tais que $\tau_{|X} = \varphi_{|X}$, então $\tau = \varphi$. Portanto $\mathbb{K}$-automorfismos de $\mathbb{L}$ são determinados por sua ação sobre o conjunto gerador X.*

Lema 3.1.4. *Sejam $\tau : \mathbb{L} \longrightarrow \mathbb{F}$ um $\mathbb{K}$-homomorfismo e $\alpha \in \mathbb{L}$ algébrico sobre $\mathbb{K}$. Se $f(x) \in \mathbb{K}[x]$ é tal que $f(\alpha) = 0$, então $f(\tau(\alpha)) = 0$. Deste modo, τ permuta as raízes do polinômio minimal $min_{\alpha,\mathbb{K}}$. Além disso, $min_{\alpha,\mathbb{K}} = min_{\tau(\alpha),\mathbb{K}}$.*

Demonstração. Considere $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Então, como τ é transformação linear, temos

$$0 = \tau(0) = \tau(f(\alpha)) = \sum_i \tau(a_i)\tau(\alpha)^i.$$

Como cada $a_i \in \mathbb{K}$, temos que $\tau(a_i) = a_i$. Logo $\sum_i a_i\tau(\alpha)^i = 0$, portanto $f(\tau(\alpha)) = 0$. Em particular, se $p = min_{\alpha,\mathbb{K}}$, então $p(\tau(\alpha)) = 0$, de onde segue que $min_{\tau(\alpha),\mathbb{K}}$ divide p. Mas p é irredutível, portanto $min_{\tau(\alpha),\mathbb{K}} = p = min_{\alpha,\mathbb{K}}$. ■

Corolário 3.1.5. *Se $\mathbb{L}|\mathbb{K}$ é uma extensão finita, então $Gal(\mathbb{L}|\mathbb{K})$ é um grupo finito.*

Demonstração. Como $\mathbb{L}|\mathbb{K}$ é finita, podemos escrever $\mathbb{L} = \mathbb{K}(\alpha_1, \cdots, \alpha_n)$, com $\alpha_i \in \mathbb{L}$ algébricos sobre $\mathbb{K}$. Pelo lema anterior, existe apenas um número finito de possibilidades para a imagem de qualquer α_i, portanto um número finito de automorfismos de $\mathbb{L}|\mathbb{K}$. ■

O teorema a seguir associa o grupo de Galois de um polinômio f a um subgrupo do grupo de permutações S_n.

Teorema 3.1.6. *Seja $\mathbb{L} = \mathbb{K}(R_f)$, com $f \in \mathbb{K}[x]$ tal que suas n raízes são distintas em $\mathbb{L}$. Então $Gal(\mathbb{L}|\mathbb{K})$ é isomorfo a um subgrupo de S_n.*

Demonstração. Pelo lema anterior, vimos que $\sigma \in Gal(\mathbb{L}|\mathbb{K})$ permuta as raízes de f, ou seja, $\sigma(R_f) = R_f$. Supondo $R_f = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ podemos escrever $\mathbb{L} = \mathbb{K}(\alpha_1, \cdots, \alpha_n)$. Considere a aplicação $\varphi : Gal(\mathbb{L}|\mathbb{K}) \longrightarrow S_{R_f} \approx S_n$ definida por $\sigma \longmapsto \sigma_{|R_f}$. Temos que φ é um homomorfismo. Mostraremos que é injetiva. Para isto, considere $\sigma \in Ker_\varphi$. Logo $\sigma_{|R_f} = Id$, ou seja, $\sigma(\alpha_i) = \alpha_i$. Então, dado $\alpha \in \mathbb{L}$, temos

$$\alpha = f(\alpha_1, \cdots, \alpha_n) = \sum a_{i_1 i_2 \cdots i_n} \cdot \alpha_1^{i_1} \cdots \alpha_n^{i_n}, \quad a_{i_1 i_2 \cdots i_n} \in \mathbb{K}.$$

Logo $\sigma(\alpha) = \sum a_{i_1 i_2 \cdots i_n} \cdot \alpha_1^{i_1} \cdots \alpha_n^{i_n} = \alpha$, ou seja, $\sigma = Id$. Portanto φ é injetiva e, pelo teorema de isomorfismo entre grupos, segue que $Gal(\mathbb{L}|\mathbb{K})$ é isomorfo a imagem de σ por φ, que é um subgrupo de S_n. ■

Para os próximos resultados, precisamos definir um caso especial de raízes de polinômios na forma $f = x^n - 1$, as quais chamamos raízes n-ésimas da unidade.

Definição 3.1.7. *Considere um corpo $\mathbb{K} \subseteq \mathbb{C}$ e $f = x^n - 1 \in \mathbb{K}[x]$. As raízes de f são dadas por $R_f = \{1, \omega, \cdots, \omega^{n-1}\}$, em que $\omega = e^{2\pi i/n}$. Além disso, R_f é um grupo cíclico multiplicativo gerado por ω. Lembrando que, se $(R_f, \cdot)$ é cíclico, então $\langle \omega \rangle = \langle \omega^t \rangle \Leftrightarrow mdc(n,t) = 1$. Cada gerador de $(R_f, \cdot)$ é chamado raiz n-ésima primitiva da unidade. O número destes geradores é dado por $\phi(n)$, onde ϕ representa a função de Euler.*

Em outras palavras, seja n um número inteiro positivo. Um elemento $\zeta_n \in \mathbb{C}$ é uma *raiz n-ésima da unidade* se $\zeta_n^n = 1$. Dessa forma, $\zeta_n = e^{2\pi i/n} = cos(2\pi/n) + isen(2\pi/n)$. Além disso, ζ_n é dito *raiz primitiva n-ésima da unidade* se $\zeta_n^n = 1$ mas $\zeta_n^d \neq 1$ para qualquer $1 \leq d < n$. As raízes n-ésimas da unidade são raízes do polinômio $x^n - 1$. Geometricamente, as raízes n-ésimas da unidade são precisamente os n vértices do polígono regular inscrito na circunferência unitária $\{z \in \mathbb{C};\ |z| = 1\}$, sendo um dos vértices o número 1, raiz trivial.

O número complexo ζ^m é uma raiz primitiva n-ésima da unidade se, e somente se, $mdc(m,n) = 1$, isto é, o número de raízes primitivas n-ésimas da unidade é dado pela função de Euler em n :

$$\phi(n) = \#\{0 < m < n : mdc(m,n) = 1, m \in \mathbb{Z}\},$$

ou seja, o número de raízes primitivas n-ésimas da unidade é dado pela cardinalidade do conjunto de inteiros positivos menores que n que são coprimos com n.

O teorema a seguir associa o grupo de Galois da extensão gerada pelas raízes n-ésimas primitivas da unidade de $f = x^n - 1$ ao conjunto dos elementos simetrizáveis do grupo das classes de resto $\mathbb{Z}_n$.

Teorema 3.1.8. *[10] Sejam corpos $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{C}$ e $f = x^n - 1 \in \mathbb{Q}[x]$. Então $Gal(\mathbb{K}(R_f)|\mathbb{K}) \approx U(\mathbb{Z}_n) = \left\{\overline{r} \in \mathbb{Z}_n \mid \overline{r} \cdot \overline{s} = \overline{1},\ com\ \overline{s} \in \mathbb{Z}_n\right\}$. Em particular, $Gal(\mathbb{K}(R_f)|\mathbb{K})$ é abeliano.*

Demonstração. Considere $\sigma \in Gal(\mathbb{K}(R_f)|\mathbb{K})$. Temos que $R_f = \{1, \omega, \cdots, \omega^{n-1}\} = \langle\omega\rangle$, então $\sigma(\omega) = \omega^i$ com $1 \leq i \leq n-1$. Note que

$$R_f = \langle\omega\rangle = \langle\sigma(\omega)\rangle = \langle\omega^i\rangle \Leftrightarrow mdc(n,i) = 1 \Leftrightarrow \bar{i} \in U(\mathbb{Z}_n).$$

Então considere a aplicação $\varphi : Gal(\mathbb{K}(R_f)|\mathbb{K}) \longrightarrow U(\mathbb{Z}_n)$ definida por $\sigma \longmapsto \bar{i}$, se $\sigma(\omega) = \omega^i$, um homomorfismo sobrejetor. Seja $\sigma \in Ker_\varphi$ tal que $\sigma(\omega) = \omega^i$, então

$$\varphi(\sigma) = \bar{i} \Rightarrow \bar{i} = \overline{1} \Rightarrow n|i-1.$$

Mas $1 \leq i \leq n-1$, de onde segue que $i = 1$. Portanto φ é injetiva e, pelo teorema de isomorfismo entre grupos, segue que $Gal(\mathbb{K}(R_f)|\mathbb{K}) \approx U(\mathbb{Z}_n)$. ■

O teorema a seguir apresenta o caso particular onde o grupo de Galois é da forma $Gal(\mathbb{L}|\mathbb{Q}(\omega))$.

Teorema 3.1.9. *[10] Considere os corpos $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L}$, o polinômio $f = x^n - 1 \in \mathbb{K}[x]$ tal que $\sqrt[n]{a} \notin \mathbb{K}$ e $\mathbb{L} = \mathbb{K}(R_f)$. Se $\omega \in \mathbb{K}$ é uma raiz n-ésima primitiva da unidade, então $Gal(\mathbb{L}|\mathbb{K})$ é isomorfo a um subgrupo de $\mathbb{Z}_n$. Em particular, $Gal(\mathbb{L}|\mathbb{K})$ é abeliano.*

Demonstração. A prova segue o mesmo processo da anterior. Seja $\alpha = \sqrt[n]{a}$. Então temos $R_f = \{\alpha, \alpha\omega, \cdots, \alpha\omega^{n-1}\}$ e $\mathbb{L} = \mathbb{K}(\alpha, \omega) = \mathbb{K}(\alpha)$, pois $\omega \in \mathbb{K}$. Seja $\sigma \in Gal(\mathbb{L}|\mathbb{K})$, com $\sigma(\alpha) = \alpha\omega^i$, com $0 \leq i \leq n-1$. Considere $\varphi : Gal(\mathbb{L}|\mathbb{K}) \longrightarrow \mathbb{Z}_n$ definida por $\sigma \longmapsto \bar{i}$, se $\sigma(\alpha) = \alpha\omega^i$, um homomorfismo. Suponha $\sigma \in Ker_\varphi$ tal que $\sigma(\alpha) = \alpha\omega^i$, então

$$\varphi(\sigma) = \overline{0} \Rightarrow \bar{i} = \overline{0} \Rightarrow n|i.$$

Mas temos que $0 \leq i \leq n-1$, o que implica em $i = 0$, ou seja, σ é injetiva. Portanto $Gal(\mathbb{L}|\mathbb{K})$ é isomorfa a um subgrupo de $\mathbb{Z}_n$. ■

Os próximos três resultados nos fornecem ferramentas para obter informações numéricas mais precisas sobre a ordem do grupo de Galois para uma extensão finita $\mathbb{L}|\mathbb{K}$. Para isto, precisamos definir o conceito de caráter de grupos, dado abaixo.

Definição 3.1.10. *Se G é um grupo e $\mathbb{K}$ um corpo, então definimos um caráter como o homomorfismo de grupos de G em $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.*

Tomando $G = \mathbb{L}^*$, temos que os $\mathbb{K}$-automorfismos de $\mathbb{L}$, ou seja, os elementos de $Gal(\mathbb{L}|\mathbb{K})$, podem ser vistos como caráteres de $\mathbb{L}^*$ em $\mathbb{L}^*$. Os próximos lemas garantem um limitante para a ordem de $Gal(\mathbb{L}|\mathbb{K})$.

Lema 3.1.11. *(de Dedekind) Sejam $\mathbb{L}$ um corpo e $\tau_1, \cdots, \tau_n$ caráteres distintos de G em $\mathbb{L}^*$. Então $\tau_1, \cdots, \tau_n$ são linearmente independentes sobre $\mathbb{K}$, ou seja, se $\sum_i c_i\tau_i(g) = 0$, para quaisquer $g \in G$ e $c_i \in \mathbb{L}$, então todo $c_i = 0$.*

Demonstração. Suponha que o lema é falso. Considere k o menor inteiro tal que existem $c_i \in \mathbb{L}$ e para todo $g \in G$ com

$$\sum_{i=1}^{k} c_i\tau_i(g) = 0. \quad (I)$$

Então, pela minimalidade de k, temos todos $c_i \neq 0$. Como $\tau_1 \neq \tau_2$, existe $h \in G$ tal que $\tau_1(h) \neq \tau_2(h)$. Multiplicando (I) por $\tau_1(h)$, temos

$$\sum_{i=1}^{k} c_i\tau_1(h)\tau_i(g) = 0. \quad (II)$$

Além disso, substituindo gh em (I), temos

$$\sum_{i=1}^{k} c_i \tau_i(hg) = \sum_{i=1}^{k} c_i \tau_i(h)\tau_i(g) = 0.$$

Subtraindo esta última de (II), temos

$$\sum_{i=1}^{k} (c_i(\tau_1(h) - \tau_i(h)))\tau_i(g) = 0$$

Esta expressão envolve $k-1$ termos dos τ_i com não todos coeficientes nulos. Isto contradiz a minimalidade de k. Portanto o lema fica provado. ■

Existe uma interpretação vetorial do lema de Dedekind. Se V é o conjunto de todas as funções de G em $\mathbb{K}$, então V é um $\mathbb{K}$-espaço vetorial com a adição de funções usual e operação por escalar. O lema de Dedekind, neste sentido, mostra que o conjunto de todos os caráteres de G em $\mathbb{K}^*$ forma um conjunto linearmente independente em V [11].

Lema 3.1.12. *Considere a extensão $\mathbb{L}|\mathbb{K}$ finita e separável. Então $o(Gal(\mathbb{L}|\mathbb{K})) \leq [\mathbb{L} : \mathbb{K}]$.*

Demonstração. Como a extensão $\mathbb{L}|\mathbb{K}$ é finita, então $Gal(\mathbb{L}|\mathbb{K})$ é um grupo finito, ou seja, $o(Gal(\mathbb{L}|\mathbb{K})) < \infty$. Considere $Gal(\mathbb{L}|\mathbb{K}) = \{\tau_1, \cdots, \tau_n\}$ e suponha que $[\mathbb{L} : \mathbb{K}] < n$. Seja $\{\alpha_1, \cdots, \alpha_n\}$ uma base de $\mathbb{L}$ como um $\mathbb{K}$-espaço vetorial. A matriz

$$A = \begin{pmatrix} \tau_1(\alpha_1) & \tau_1(\alpha_2) & \cdots & \tau_1(\alpha_m) \\ \tau_2(\alpha_1) & \tau_2(\alpha_2) & \cdots & \tau_2(\alpha_m) \\ . & . & \cdots & . \\ . & . & \cdots & . \\ . & . & \cdots & . \\ \tau_n(\alpha_1) & \tau_n(\alpha_2) & \cdots & \tau_n(\alpha_m) \end{pmatrix} \in M_{n\times m}(\mathbb{L})$$

possui posto $\leq m < n$ e portanto suas linhas são linearmente dependentes sobre $\mathbb{L}$, ou seja, existem $c_i \in \mathbb{L}$, não todos nulos, tais que

$$\sum_{i=1}^{n} c_i \tau_i(\alpha_j) = 0, \quad j = 1, \cdots, m.$$

Colocando $G = \mathbb{L}^*$, temos que dado $g \in G$ existem $\beta_j \in \mathbb{K}$ tais que $g = \sum_j \beta_j \alpha_j$. Portanto

$$\sum_i c_i \tau_i(g) = \sum_i c_i \tau_i(\sum_j \beta_j \alpha_j) = \sum_i c_i(\beta_j \sum_j \tau_j(\alpha_j)) = \sum_j \beta_j (\sum_i) c_i \tau_i(\alpha_j) = 0.$$

Então todo c_i deve ser nulo, pelo lema de Dedekind, o que contradiz a escolha destes elementos. Logo não vale que $[\mathbb{L} : \mathbb{K}] < n = o(Gal(\mathbb{L}|\mathbb{K}))$, como supomos. Portanto $o(Gal(\mathbb{L}|\mathbb{K})) \leq [\mathbb{L} : \mathbb{K}]$. ■

O teorema a seguir determina para quais extensões a igualdade do lema anterior é válida, ou seja, quando a ordem do grupo $Gal(\mathbb{L}|\mathbb{K})$ é igual ao grau da extensão $\mathbb{L}|\mathbb{K}$.

Teorema 3.1.13. *Considere a extensão $\mathbb{L}|\mathbb{K}$ finita e separável. Então $o(Gal(\mathbb{L}|\mathbb{K})) = [\mathbb{L} : \mathbb{K}]$ se, e somente se, $\mathbb{L}|\mathbb{K}$ é uma extensão de Galois.*

Demonstração. Primeiro, como $\mathbb{L}|\mathbb{K}$ é finita e separável, segue do Teorema do Elemento Primitivo que existe $\alpha \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\alpha)$. Considere $f = min_{\alpha,\mathbb{K}}$ e suponha que $n = gr(f)$.

Suponhamos que $\mathbb{L}|\mathbb{K}$ é galoisiana. Então $\mathbb{L}|\mathbb{K}$ é normal, o que implica em $R_f \subseteq \mathbb{L}$. Deste modo, $\mathbb{L} = \mathbb{K}(\alpha) \subseteq \mathbb{K}(R_f) \subseteq \mathbb{L}$, ou seja, $\mathbb{L} = \mathbb{K}(R_f)$. Como f é separável, temos que f tem n raízes distintas em $\mathbb{L}$ e que $[\mathbb{L} : \mathbb{K}] = [\mathbb{K}(\alpha) : \mathbb{K}] = gr(f) = n$. Suponha que $R_f = \{\alpha_1, \cdots, \alpha_n\}$ com $\alpha = \alpha_1$. Existem isomorfismos $\rho_i : \mathbb{K}(\alpha) \Rightarrow \mathbb{K}(\alpha_i)$ tais que $\rho_i(\alpha) = \alpha_i$ e $\rho_i|_{\mathbb{K}} = Id$. Como $\rho_i : \mathbb{L} \Rightarrow \mathbb{K}(\alpha_i)$ é isomorfismo e $\mathbb{K}(\alpha_i) \subseteq \mathbb{L}$, então $\rho_i \in Aut(\mathbb{L})$. Então, temos que $\rho_i \in Gal(\mathbb{L}|\mathbb{K})$. Portanto $o(Gal(\mathbb{L}|\mathbb{K})) \geq n = [\mathbb{L} : \mathbb{K}]$. Pelo lema anterior, temos $o(Gal(\mathbb{L}|\mathbb{K})) \leq n = [\mathbb{L} : \mathbb{K}]$, de onde segue a igualdade que queríamos mostrar.

Reciprocamente, suponha $o(Gal(\mathbb{L}|\mathbb{K})) = [\mathbb{L} : \mathbb{K}]$. Considere a aplicação $\varphi : Gal(\mathbb{L}|\mathbb{K}) \longrightarrow R_f \cap \mathbb{L}$ definida por $\rho \longmapsto \rho(\alpha)$. Temos que φ é injetiva, e portanto $o(Gal(\mathbb{L}|\mathbb{K})) \leq |R_f \cap \mathbb{L}| \leq gr(f)$ ([10]). Logo $R_f \subseteq \mathbb{L}$. Então

$$\mathbb{K}(R_f) \subseteq \mathbb{L} = \mathbb{K}(\alpha) \subseteq \mathbb{K}(R_f) \Rightarrow \mathbb{L} = \mathbb{K}(R_f),$$

e portanto $\mathbb{L}|\mathbb{K}$ é de Galois. ■

Corolário 3.1.14. *Sejam $\mathbb{L}$ uma extensão do corpo $\mathbb{K}$ e $\alpha \in \mathbb{L}$ algébrico sobre $\mathbb{K}$. Então a ordem de $Gal(\mathbb{L}|\mathbb{K})$ é igual ao número de raízes distintas de $f = min_{\alpha,\mathbb{K}}$ em $\mathbb{K}(\alpha)$. Portanto $\mathbb{L}|\mathbb{K}$ é de Galois se, e somente se, $f = min_{\alpha,\mathbb{K}}$ possui $n = gr(f)$ raízes distintas em $\mathbb{K}(\alpha)$.*

Demonstração. Seja $\tau \in Gal(\mathbb{K}(\alpha)|\mathbb{K})$. Vimos que $\tau(\alpha)$ é uma raiz de $min_{\alpha,\mathbb{K}}$. Além disso, se $\sigma, \tau \in Gal(\mathbb{K}(\alpha)|\mathbb{K})$ são tais que $\sigma \neq \tau$ então $\sigma(\alpha) \neq \tau(\alpha)$, pois $\mathbb{K}$-automorfismos em $\mathbb{K}(\alpha)$ são determinados por sua ação. Portanto $o(Gal(\mathbb{K}(\alpha)|\mathbb{K})) \leq n$. Por outro lado, seja β outra raiz de $min_{\alpha,\mathbb{K}}$ em $\mathbb{K}(\alpha)$. Considere $\tau : \mathbb{K}(\alpha) \longrightarrow \mathbb{K}(\alpha)$ definida por $\tau(g(\alpha)) = g(\beta)$, para algum $g \in \mathbb{K}[x]$. Então τ é um $\mathbb{K}$-automorfismo e $\tau(\alpha) = \beta$, pela definição de τ. Portanto $o(Gal(\mathbb{K}(\alpha)|\mathbb{K}))$ é igual ao número de raízes de f em $\mathbb{K}(\alpha)$. Como $[\mathbb{K}(\alpha) : \mathbb{K}] = gr(min_{\alpha,\mathbb{K}})$, segue que $\mathbb{K}(\alpha)$ é de Galois se, e só se, $min_{\alpha,\mathbb{K}}$ possui n raízes distintas em $\mathbb{K}(\alpha)$. ■

Existem dois casos em que uma extensão $\mathbb{K}(\alpha)|\mathbb{K}$ não seja de Galois. Primeiro, se $min_{\alpha,\mathbb{K}}$ não possui todas as suas raízes em $\mathbb{K}(\alpha)$ e segundo, se $min_{\alpha,\mathbb{K}}$ possui raízes repetidas.

Corolário 3.1.15. *[10] Se $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ e $\mathbb{L}|\mathbb{K}$ é de Galois, então $[\mathbb{L} : \mathbb{M}] = o(Gal(\mathbb{L}|\mathbb{M}))$.*

3.2 Corpo Fixo

Como vimos, a ideia principal da Teoria de Galois é associar extensões de corpos a grupos. No tópico anterior, vimos como tomar uma extensão $\mathbb{L}|\mathbb{K}$ e associá-la a um grupo, $Gal(\mathbb{L}|\mathbb{K})$. De forma geral, se $\mathbb{M}$ é um corpo tal que $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$, podemos associar a extensão $\mathbb{L}|\mathbb{M}$ ao grupo $Gal(\mathbb{L}|\mathbb{M})$, que é um subgrupo de $Gal(\mathbb{L}|\mathbb{K})$, como veremos a seguir.

Reciprocamente, dado um subgrupo de $Gal(\mathbb{L}|\mathbb{K})$, podemos associá-lo a um subcorpo de $\mathbb{L}$ que contém $\mathbb{K}$, ou seja, definiremos uma extensão a partir de um grupo. Podemos fazer isto para um subconjunto qualquer de $Aut(\mathbb{L})$.

Proposição 3.2.1. *Sejam $\mathbb{L}|\mathbb{K}$ uma extensão de corpos e $S \subseteq Aut(\mathbb{L})$. Considere*

$$\mathscr{F}(S) = \{\alpha \in \mathbb{L} \mid \tau(\alpha) = \alpha, \text{ para algum } \tau \in S\}$$

Então $\mathscr{F}(S)$ é um subcorpo de $\mathbb{L}$. Se $S \subseteq Gal(\mathbb{L}|\mathbb{K})$, então $\mathbb{K} \subseteq \mathscr{F}(S)$.

Demonstração. Dados $\alpha, \beta \in \mathscr{F}(S)$ e $\tau \in S$, temos $\tau(\alpha \pm \beta) = \tau(\alpha) \pm \tau(\beta) = \alpha \pm \beta$ e $\tau(\alpha\beta) = \tau(\alpha)\tau(\beta)$. Além disso, se $0 \neq \alpha \in \mathscr{F}(S)$, então $\tau(\alpha^{-1}) = (\tau(\alpha))^{-1} = \alpha^{-1}$. Disto segue que $\mathscr{F}(S)$ é um subcorpo de $\mathbb{L}$. A segunda parte segue diretamente da definição de grupo de Galois. ■

Definição 3.2.2. *O subcorpo $\mathscr{F}(S)$ de $\mathbb{L}$ dado na proposição acima é chamado de corpo fixo de S.*

Se $S \subseteq Gal(\mathbb{L}|\mathbb{K})$, então $\mathscr{F}(S)$ é chamado corpo intermediário de $\mathbb{L}|\mathbb{K}$. O resultado a seguir fornece algumas propriedades básicas envolvendo grupos de Galois e corpos fixos. A demonstração pode ser encontrada em [11].

Lema 3.2.3. *Considere o corpo $\mathbb{L}$.*

1. *Se $\mathbb{K}_1 \subseteq \mathbb{K}_2$ são subcorpos de $\mathbb{L}$, então $Gal(\mathbb{L}|\mathbb{K}_2) \subseteq Gal(\mathbb{L}|\mathbb{K}_1)$.*
2. *Se $\mathbb{K}$ é um subcorpo de $\mathbb{L}$, então $\mathbb{K} \subseteq \mathscr{F}(Gal(\mathbb{L}|\mathbb{K}))$.*
3. *Se $S_1 \subseteq S_2$ são subconjuntos de $Aut(\mathbb{L})$, então $\mathscr{F}(S_2) \subseteq \mathscr{F}(S_1)$.*
4. *Se $S \subseteq Aut(\mathbb{L})$, então $S \subseteq Gal(\mathbb{K}|\mathscr{F}(S))$.*
5. *Se $\mathbb{K} = \mathscr{F}(S)$, para algum $S \subseteq Aut(\mathbb{L})$, então $\mathbb{K} = \mathscr{F}(Gal(\mathbb{L}|\mathbb{K}))$.*
6. *Se $H = Gal(\mathbb{L}|\mathbb{K})$, para algum subcorpo $\mathbb{K}$ de $\mathbb{L}$, então $H = Gal(\mathbb{L}|\mathscr{F}(H))$.*

Corolário 3.2.4. *Seja $\mathbb{L}$ uma extensão do corpo $\mathbb{K}$. Então existe uma correspondência biunívoca de reversão de inclusão (ou seja, $H_1 \subseteq H_2 \Leftrightarrow \mathscr{F}(H_2) \subseteq \mathscr{F}(H_1)$) entre o conjunto dos subgrupos de $Gal(\mathbb{L}|\mathbb{K})$ da forma $Gal(\mathbb{L}|\mathbb{M})$, para algum subcorpo $\mathbb{M} \supseteq \mathbb{K}$ de $\mathbb{L}$, e o conjunto de subcorpos de $\mathbb{L}$ que contêm $\mathbb{K}$, que são da forma $\mathscr{F}(S)$, para algum $S \in Aut(\mathbb{L})$. Esta correspondência é dada por $\mathbb{M} \mapsto Gal(\mathbb{L}|\mathbb{M})$ e sua inversa é dada por $H \mapsto \mathscr{F}(H)$.*

Demonstração. Este resultado segue diretamente do lema anterior. Se $\mathscr{G}$ e $\mathscr{F}$ representam o conjunto dos grupos e corpos em questão, respectivamente, então a aplicação que associa um subcorpo $\mathbb{M}$ de $\mathbb{L}$ ao subgrupo $Gal(\mathbb{L}|\mathbb{M})$ de $Aut(\mathbb{L})$ associa $\mathscr{F}$ a $\mathscr{G}$. Esta aplicação é injetiva e sobrejetiva pelo item 5 do lema anterior, portanto uma bijeção. Por outro lado, sua inversa é dada associando H com $\mathscr{F}(H)$ pelo item 6 do lema. ■

Lema 3.2.5. *[10] Seja $\mathbb{L}|\mathbb{K}$ uma extensão finita, separável e simples, ou seja, $\mathbb{L} = \mathbb{K}(\alpha)$, para algum $\alpha \in \mathbb{L}$. Se $H = \{\tau_1, \cdots, \tau_n\}$ é um subgrupo de $Gal(\mathbb{L}|\mathbb{K})$ e $f(x) = (x - \tau_1(\alpha)) \cdots (x - \tau_n(\alpha))$, então temos $f \in \mathscr{F}(H)[x]$ e $[\mathbb{L} : \mathscr{F}(H)] \leq o(H)$.*

Lema 3.2.6. *[10] Seja $\mathbb{L}|\mathbb{K}$ uma extensão finita e separável tal que $\alpha \in \mathbb{L} \setminus \mathbb{K}$. Se $\mathbb{L}|\mathbb{K}$ é galoisiana, então existe $\tau \in Gal(\mathbb{L}|\mathbb{K})$ tal que $\tau(\alpha) \neq \alpha$.*

Vimos anteriormente que $\mathbb{L}|\mathbb{K}$ finita e separável é de Galois se, e somente se, $[\mathbb{L} : \mathbb{K}] = o(Gal(\mathbb{L}|\mathbb{K}))$. O teorema a seguir apresenta uma condição não-numérica para que uma extensão seja galoisiana.

Teorema 3.2.7. *Uma extensão $\mathbb{L}|\mathbb{K}$ finita e separável é de Galois se, e somente se, $\mathscr{F}(Gal(\mathbb{L}|\mathbb{K})) = \mathbb{K}$.*

Demonstração. Suponha $\mathbb{L}|\mathbb{K}$ galoisiana. Pelo item 2 do Lema 3.19, temos que $\mathbb{K} \subseteq \mathscr{F}(Gal(\mathbb{L}|\mathbb{K}))$. Se $\mathbb{K} \subsetneq \mathscr{F}(Gal(\mathbb{L}|\mathbb{K}))$, existe $\alpha \in \mathscr{F}(Gal(\mathbb{L}|\mathbb{K})) \setminus \mathbb{K}$, então $\alpha \in \mathbb{L} \setminus \mathbb{K}$ e pelo lema anterior existe $\tau \in Gal(\mathbb{L}|\mathbb{K})$ tal que $\tau(\alpha) \neq \alpha$, ou seja, $\alpha \notin \mathscr{F}(Gal(\mathbb{L}|\mathbb{K}))$, uma

contradição. Portanto $\mathbb{K} = \mathscr{F}(Gal(\mathbb{L}|\mathbb{K}))$.

Reciprocamente, suponha $\mathscr{F}(Gal(\mathbb{L}|\mathbb{K})) = \mathbb{K}$. Sabemos que $o(Gal(\mathbb{L}|\mathbb{K})) \leq [\mathbb{L} : \mathbb{K}]$. Pelo lema 3.21 temos $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathscr{F}(Gal(\mathbb{L}|\mathbb{K}))] \leq o(Gal(\mathbb{L}|\mathbb{K}))$. Logo $o(Gal(\mathbb{L}|\mathbb{K})) = [\mathbb{L} : \mathbb{K}]$ e portanto $\mathbb{L}|\mathbb{K}$ é galoisiana. ■

O corolário a seguir decorre dos últimos resultados.

Corolário 3.2.8. *[10] Seja $\mathbb{L}|\mathbb{K}$ finita e separável. As seguintes afirmações são equivalentes.*

1. *$\mathbb{L}|\mathbb{K}$ é de Galois.*
2. *$\mathbb{L}|\mathbb{K}$ é normal.*
3. *$[\mathbb{L} : \mathbb{K}] = o(Gal(\mathbb{L}|\mathbb{K}))$*
4. *$\mathscr{F}(Gal(\mathbb{L}|\mathbb{K})) = \mathbb{K}$.*

Os dois próximos teoremas finalizam as propriedades dos grupos galoisianos e corpos fixos, neste tópico. Suas respectivas justificativas podem ser consultadas em [10]. O primeiro nos diz quando um subgrupo de um grupo de Galois é também um grupo de Galois, associado a uma extensão de um corpo fixo, enquanto que o segundo apresenta uma condição, em termos de grupos de Galois, para que um corpo intermediário de uma extensão seja galoisiano.

Teorema 3.2.9. *[10] Se $\mathbb{L}|\mathbb{K}$ é uma extensão de Galois e H é um subgrupo de $Gal(\mathbb{L}|\mathbb{K})$, então $[\mathbb{L} : \mathscr{F}(H)] = o(H)$ e $H = Gal(\mathbb{L}|\mathscr{F}(H))$.*

Teorema 3.2.10. *[10] Sejam $\mathbb{L}|\mathbb{K}$ uma extensão de Galois e $\mathbb{M}$ um corpo tal que $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$. Então as seguintes afirmações são equivalentes.*

1. *$\mathbb{M}|\mathbb{K}$ é de Galois.*
2. *$Gal(\mathbb{L}|\mathbb{M})$ é subgrupo de $Gal(\mathbb{L}|\mathbb{K})$ e o grupo quociente $Gal(\mathbb{L}|\mathbb{K})/Gal(\mathbb{L}|\mathbb{M})$ é isomorfo a $Gal(\mathbb{M}|\mathbb{K})$.*

3.3 Teorema de Correspondência de Galois

Nosso último tópico apresenta um teorema de grande importância na teoria de Galois, considerado seu Teorema fundamental, que descreve corpos intermediários de uma extensão galoisiana $\mathbb{L}|\mathbb{K}$ em termos dos subgrupos do grupo de Galois $Gal(\mathbb{L}|\mathbb{K})$, estabelecendo uma correspondência entre eles. Deste modo, podemos transpor questões relacionadas a corpos para questões sobre grupos finitos, uma ferramenta muito útil.

Teorema 3.3.1. *(Correspondência de Galois) Sejam $\mathbb{L}|\mathbb{K}$ uma extensão galoisiana finita e $G = Gal(\mathbb{L}|\mathbb{K})$. Existe uma correspondência biunívoca de reversão de inclusão entre corpos intermediários de $\mathbb{L}|\mathbb{K}$ e subgrupos de G, dada por $\mathbb{M} \longmapsto Gal(\mathbb{L}|\mathbb{M})$ e $H \longmapsto \mathscr{F}(H)$, em que $\mathbb{M}$ é um corpo tal que $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ e H é subgrupo de G. Além disso, se $\mathbb{M} \Longleftrightarrow H$, então $[\mathbb{L} : \mathbb{M}] = o(H)$ e $[\mathbb{M} : \mathbb{K}] = (G : H)$, o índice de H em G. Além disso, H é subgrupo normal de G se, e só se, $\mathbb{M}|\mathbb{K}$ é de Galois. Quando isto ocorre, temos que $Gal(\mathbb{M}|\mathbb{K})$ é isomorfo a G/H.*

Demonstração. Pelo lema 3.19 e corolário 3.20, existem mapas dados por $\mathbb{M} \longmapsto Gal(\mathbb{L}|\mathbb{M})$ e $H \longmapsto \mathscr{F}(H)$ que nos dão uma correspondência biunívoca de reversão de inclusão (ou seja, $H_1 \subseteq H_2 \Longleftrightarrow \mathscr{F}(H_2) \subseteq \mathscr{F}(H_1)$) entre o conjunto de corpos fixos $\mathbb{M}$ tal que $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ e o

conjunto de subgrupos de G da forma $Gal(\mathbb{L}|\mathbb{M})$. Então seja $\mathbb{M}$ um subcorpo de $\mathbb{L}$ que contém $\mathbb{K}$.

Como $\mathbb{L}|\mathbb{K}$ é de Galois, por hipótese, então é normal e separável. Logo $\mathbb{L}|\mathbb{M}$ é também normal e separável e portanto galoisiana. Então segue que $\mathbb{M} = \mathscr{F}(Gal(\mathbb{L}|\mathbb{M}))$, ou seja, todo corpo intermediário é um corpo fixo. Além disso, se H é subgrupo de G, então H é um grupo finito e portanto $H = Gal(\mathbb{L}|\mathscr{F}(H))$, pelo teorema 3.25. Portanto todo subgrupo de G nestas condições é um grupo de Galois. Então os mapas definidos acima nos garantem a correspondência desejada. Lembramos que $o(Gal(\mathbb{L}|\mathbb{K})) = [\mathbb{L} : \mathbb{K}]$ se $\mathbb{L}|\mathbb{K}$ é de Galois. Então, se $\mathbb{M} \Longleftrightarrow H$, temos $o(H) = [\mathbb{L} : \mathbb{M}]$, pois $\mathbb{L}|\mathbb{M}$ é de Galois e $H = Gal(\mathbb{L}|\mathbb{M})$. Portanto temos

$$(G : H) = \frac{o(G)}{o(H)} = \frac{[\mathbb{L} : \mathbb{K}]}{[\mathbb{L} : \mathbb{M}]} = [\mathbb{M} : \mathbb{K}]$$

Agora, suponha que H é subgrupo normal de G e considere $\mathbb{M} = \mathscr{F}(H)$. Sejam $\alpha \in \mathbb{M}$ e β uma raiz de $min_{\alpha,\mathbb{K}}$ em $\mathbb{L}$. Pelo teorema da extensão de isomorfismo, existe um $\sigma \in G$ tal que $\sigma(\alpha) = \beta$. Dado $\tau \in H$, temos que $\tau(\beta) = \sigma(\sigma^{-1}\tau\sigma(\alpha))$. No entanto, como H é normal em G, temos que $\sigma^{-1}\tau\sigma \in H$, portanto $\sigma^{-1}\tau\sigma(\alpha) = \alpha$. Logo $\tau(\beta) = \sigma(\alpha) = \beta$, de onde segue que $\beta \in \mathscr{F}(H) = \mathbb{M}$. Como $min_{\alpha,\mathbb{K}}$ fatora em $\mathbb{L}$, isto mostra que $min_{\alpha,\mathbb{K}}$ fatora também em $\mathbb{M}$. Portanto $\mathbb{M}$ é normal sobre $\mathbb{K}$. Como $\mathbb{L}|\mathbb{K}$ é separável e $\mathbb{M} \subseteq \mathbb{L}$, a extensão $\mathbb{M}|\mathbb{K}$ é também separável. Portanto $\mathbb{M}|\mathbb{K}$ é normal e separável, ou seja, é uma extensão galoisiana.

Reciprocamente, suponha que $\mathbb{M}|\mathbb{K}$ é de Galois. Considere $\theta : G \longrightarrow Gal(\mathbb{M}|\mathbb{K})$ dada por $\theta(\sigma) = \sigma_{|\mathbb{M}}$. Como $\mathbb{M}|\mathbb{K}$ é normal, temos que $\sigma_{|\mathbb{M}} \in Gal(\mathbb{M}|\mathbb{K})$ e portanto θ é um homomorfismo de grupos bem-definido. Seu núcleo é dado por

$$Ker_\theta = \left\{\sigma \in \mathbb{L};\ \sigma_{|\mathbb{M}} = Id\right\} = Gal(\mathbb{L}|\mathbb{M}) = H.$$

Então segue que H é subgrupo normal de G. O mapa θ é sobrejetivo pois, se $\tau \in Gal(\mathbb{M}|\mathbb{K})$ existe $\sigma \in G$ tal que $\sigma_{|\mathbb{M}} = \tau$ pelo teorema de extensão de isomorfismo. Isto mostra que $Gal(\mathbb{M}|\mathbb{K})$ e G/H são isomorfos. ■

3.4 Corpo de números e anel dos inteiros

Quando um corpo é uma extensão finita do corpo dos racionais, temos um caso particular de extensão, importante conceito em nosso estudo.

Definição 3.4.1. *Um número $\alpha \in \mathbb{C}$ é chamado número algébrico se é algébrico sobre o corpo dos racionais, ou seja, existe um polinômio não nulo $f \in \mathbb{Q}[x]$ tal que $f(\alpha) = 0$.*

Teorema 3.4.2. *[9] O conjunto A dos números algébricos é um subcorpo de $\mathbb{C}$.*

Estamos interessados em certos subcorpos de A, que definimos a seguir.

Definição 3.4.3. *Um subcorpo $\mathbb{L} \subseteq \mathbb{C}$ é dito um corpo de números se $\mathbb{K}$ é uma extensão finita de $\mathbb{Q}$, ou seja, se $[\mathbb{L} : \mathbb{Q}]$ é finito.*

Esta definição implica que todo elemento de um corpo de números $\mathbb{L}$ é algébrico, e portanto $\mathbb{L} \subseteq A$. Consideramos subcorpos $\mathbb{L} \subseteq A$ pois $[A : \mathbb{Q}]$ não é finito [9]. Se $\mathbb{L}$ é um corpo de números, então $\mathbb{L} = \mathbb{Q}(\alpha_1, ..., \alpha_n)$, onde $\alpha_1, ..., \alpha_n$ são números algébricos. Este conjunto de números algébricos geradores da extensão pode ser tomado como uma base de $\mathbb{L}$ como $\mathbb{Q}$-espaço vetorial. Podemos reduzir esta observação ao seguinte resultado.

Teorema 3.4.4. *[9] Se $\mathbb{L}$ é um corpo de números, então $\mathbb{L} = \mathbb{Q}(\alpha)$, para algum número algébrico α.*

Um caso especial de números algébricos é dado tomando polinômios mônicos com coeficientes em $\mathbb{Z}$, definido a seguir.

Definição 3.4.5. *Um número complexo θ é um inteiro algébrico se existe um polinômio mônico com coeficientes inteiros, ou seja, $p(x) \in \mathbb{Z}[x]$, tal que $p(\theta) = 0$.*

Se $\theta \in \mathbb{C}$ é raiz de uma equação cujos coeficientes são inteiros algébricos, então θ é também um inteiro algébrico. Com isso, é possível determinar novos inteiros algébricos, conhecendo-se alguns.

Pode ser mostrado que o conjunto dos inteiros algébricos de $\mathbb{C}$ é um subanel do corpo dos números algébricos [9]. Esse conjunto, dado por $B = \{\alpha \in \mathbb{C};\ irr(\alpha, \mathbb{Q}) \in \mathbb{Z}[x]\}$, tal que $irr(\alpha, \mathbb{Q})$ denota um polinômio irredutível de α sobre $\mathbb{Q}$, é denominado *anel dos inteiros algébricos*.

Dado um corpo de números $\mathbb{L}$ de grau n, um elemento $\alpha \in \mathbb{L}$ é denominado *inteiro algébrico do corpo* $\mathbb{L}$ se existe um polinômio mônico não nulo $f(x)$ com coeficientes inteiros tal que $f(\alpha) = 0$. O conjunto formado pelos inteiros algébricos do corpo $\mathbb{L}$ é precisamente o conjunto dos elementos de $\mathbb{L}$ que são inteiros algébricos, ou seja, esse conjunto é dado por $\mathscr{O}_{\mathbb{L}} = B \cap \mathbb{L}$. Pode ser mostrado que esse conjunto é um anel, denominado *anel dos inteiros algébricos de* $\mathbb{L}$.

Definição 3.4.6. *Uma $\mathbb{Z}$-base para $\mathscr{O}_{\mathbb{L}}$, visto como um grupo aditivo, é chamada de base integral de $\mathbb{L}$ ou de $\mathscr{O}_{\mathbb{L}}$.*

Se $\mathbb{L} = \mathbb{Q}(\alpha)$ é um corpo de números, então existe uma série de distintos monomorfismos $\sigma : \mathbb{L} \longrightarrow \mathbb{C}$. Esse conjunto de monomorfismos será de grande importância em nosso trabalho posteriormente. O resultado a seguir nos garante o número de elementos deste conjunto.

Teorema 3.4.7. *[9] Seja $\mathbb{L} = \mathbb{Q}(\alpha)$ um corpo de números de grau n sobre $\mathbb{Q}$. Então existem exatamente n distintos monomorfismos $\sigma_i : \mathbb{L} \longrightarrow \mathbb{C}$, com $i = 1, 2, ..., n$. Os elementos $\sigma_i(\alpha) = \alpha_i$ são os distintos zeros em $\mathbb{C}$ do polinômio minimal de α sobre $\mathbb{Q}$.*

3.5 Módulo, norma, traço e discriminante

O conceito de A-módulo, definido abaixo, em que A é um anel qualquer, é uma generalização da noção de $\mathbb{K}$-espaço vetorial, agora considerando o conjunto dos "escalares", que definem a operação externa, como um anel e não um corpo.

Definição 3.5.1. *Dado um anel comutativo com unidade A, definimos um A-módulo como um grupo abeliano M, com uma operação $\varphi : A \times M \longrightarrow M$ dada por $(a, m) \longrightarrow am$, que satisfaz as seguintes propriedades, quaisquer que sejam $a, b \in A$ e $m, n \in M$:*

1. *a operação φ é distributiva em relação a adição, ou seja, $(a+b)m = am + bm$ e $a(m+n) = am + an$;*
2. *a operação φ é associativa , ou seja, $(ab)m = a(bm)$;*
3. *$1m = m$, tal que 1 é a unidade do anel A.*

A seguir é definido um caso particular de um módulo, de modo que o A-módulo é gerado por uma família de elementos a ele pertencente.

Definição 2.4.12. Um A-módulo M é dito um *A-módulo livre* quando existe uma família $(x_i)_{i\in I}$ de elementos de M que satisfaz as seguintes propriedades:

1. a família $(x_i)_{i\in I}$ é linearmente independente;
2. todo elemento $x \in M$ é uma combinação linear da família $(x_i)_{i\in I}$.

A família de elementos que satisfaz essas condições é chamada de base do A-módulo livre e o número de elementos da base é denominado posto de M. Quando I é um conjunto finito, dizemos que o A-módulo livre é finitamente gerado.

Considere a extensão $\mathbb{L}$ do corpo $\mathbb{K}$, com grau $[\mathbb{L}:\mathbb{K}] = n$, e $\sigma_1, \sigma_2, \cdots, \sigma_n$ os n monomorfismos de $\mathbb{L}$ em $\mathbb{C}$. Seja $\alpha \in \mathbb{L}$.

Definição 3.5.2. *Definimos a norma e o traço de α relativos a extensão $\mathbb{L}/\mathbb{K}$, respectivamente, como*

$$N_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \quad e \quad Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Proposição 3.5.3. *Tomando $x, y \in \mathbb{L}$ e $a \in \mathbb{K}$, as seguintes propriedades são válidas em relação a norma e traço relativos à extensão $\mathbb{L}/\mathbb{K}$:*

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

Essas propriedades decorrem diretamente das propriedades de somatório, produtório e monomorfismo.

Sejam $\mathbb{L}$ um corpo de números de grau n, $\mathscr{O}_{\mathbb{L}}$ seu anel de inteiros algébricos e $\mathscr{A}$ um ideal não nulo do anel $\mathscr{O}_{\mathbb{L}}$. A *Norma do ideal $\mathscr{A}$* é definida como o número de elementos do anel quociente $\mathscr{O}_{\mathbb{L}}/\mathscr{A}$, isto é, $\mathscr{N}(\mathscr{A}) = \#(\mathscr{O}_{\mathbb{L}}/\mathscr{A})$, em que # denota a cardinalidade.

Teorema 3.5.4. *[9] Se $\mathscr{A} = \langle\alpha\rangle$ é um ideal principal do anel $\mathscr{O}_{\mathbb{L}}$, isto é, um ideal gerado por α, então $\mathscr{N}(\mathscr{A}) = |\mathscr{N}(\alpha)|$, ou seja, a norma do ideal $\mathscr{A}$ é igual ao valor absoluto da norma do elemento α.*

Proposição 3.5.5. *[9] Se $\alpha \in \mathbb{L}$ é um inteiro algébrico, então $N_{\mathbb{L}/\mathbb{Q}}(\alpha)$ e $Tr_{\mathbb{L}/\mathbb{Q}}(\alpha)$ são números inteiros.*

Proposição 3.5.6. *[7] Se $\mathbb{Q} \subset \mathbb{L}$ é uma extensão finita de grau n, $\mathscr{O}_{\mathbb{L}}$ é o anel dos inteiros algébricos do corpo $\mathbb{L}$ e $\mathscr{A}$ é um ideal não nulo de $\mathscr{O}_{\mathbb{L}}$, então $\mathscr{A}$ e $\mathscr{O}_{\mathbb{L}}$ são $\mathbb{Z}$-módulos livres de posto n.*

Definição 3.5.7. *Sejam $\mathbb{L}$ um corpo de números de grau n, $\sigma_1, \sigma_2, \cdots, \sigma_n$ os monomorfismos de $\mathbb{L}$ em $\mathbb{C}$ e $\{\alpha_1, \cdots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{Q}$. O discriminante dessa base é definido como*

$$D(\alpha_1, \cdots, \alpha_n) = det[\sigma_i(\alpha_j)]^2.$$

Os resultados a seguir trazem importantes propriedades sobre o discriminante de uma base.

Proposição 3.5.8. *[9] Se $\{\alpha_1, ..., \alpha_n\}$ é uma base de $\mathbb{K}$ como $\mathbb{Q}$-espaço vetorial formada por inteiros, então o discriminante $D(\alpha_1, \cdots, \alpha_n)$ é um número racional não nulo.*

Proposição 3.5.9. *[9] Se $\alpha_1, \cdots, \alpha_n$ são elementos de $\mathscr{O}_\mathbb{L}$ que formam uma $\mathbb{Q}$-base para o corpo $\mathbb{L}$ e o discriminante $D(\alpha_1, \cdots, \alpha_n)$ é livre de quadrados, então $\{\alpha_1, \cdots, \alpha_n\}$ é uma base integral.*

Proposição 3.5.10. *[9] Se $\mathbb{L}$ é um corpo de números de grau n, $\{\alpha_1, \cdots, \alpha_n\}$ e $\{\beta_1, \cdots, \beta_n\}$ são bases integrais de $\mathbb{L}$, então*

$$D(\alpha_1, \cdots, \alpha_n) = D(\beta_1, \cdots, \beta_n).$$

A ultima proposição garante a unicidade do discriminante das bases, considerando essas bases integrais. Desse modo, o discriminante independe da base de $\mathscr{O}_\mathbb{L}$ escolhida.

Proposição 3.5.11. *[9] Se $\{\alpha_1, ..., \alpha_n\}$ é uma $\mathbb{Q}$-base do corpo $\mathbb{L}$, então*

$$D(\alpha_1, ..., \alpha_n) = det(Tr(\alpha_i \alpha_j)).$$

Sejam $\mathbb{L}$ um corpo de números, $\mathscr{O}_\mathbb{L}$ seu anel de inteiros algébricos e $\{\alpha_1, \cdots, \alpha_n\}$ uma base de $\mathscr{O}_\mathbb{L}$. O *discriminante do corpo* $\mathbb{L}$ é definido como $\mathscr{D}_\mathbb{L} = det(\sigma_j(\alpha_i))^2$, onde $\alpha_1, \alpha_2, \cdots, \alpha_n$ formam uma base qualquer de $\mathbb{L}$ sobre $\mathbb{Q}$.

CAPÍTULO

4

O método de Krüskemper

Neste capítulo apresentamos o conteúdo teórico necessário para o método de Krüskemper-Taussky para a construção de reticulados, objetivo de estudo de nosso trabalho. O método fornece um algoritmo para a construção de reticulados, baseados nos trabalhos de Taussky e Krüskemper, que computa a matriz geradora de um reticulado inteiro, a partir de sua matriz de Gram. Isto produz um reticulado algébrico, no sentido de que o reticulado é construído através de mergulhos em um corpo de números totalmente real, com diversidade máxima.

4.1 Noções preliminares

Seja A é um anel comutativo com unidade. Uma *forma bilinear sobre A* é um par (M,b), em que M é um A-módulo finitamente gerado e $b : M \times M \longrightarrow A$ é uma função bilinear simétrica, ou seja, linear em ambas as variáveis tal que $b(u,v) = b(v,u), \forall u,v \in M$. Quando M é um A-módulo livre e $\{v_1, v_2, \cdots, v_n\}$ é uma base de M, então b pode ser descrita como uma matriz $B = b(v_i, v_j)$ simétrica $n \times n$ sobre A. Reciprocamente, toda matriz simétrica B quadrada de ordem n, sobre um anel A, define a forma bilinear (A^n, B). O determinante $det(M,b)$ é definido como $det(M,b) = det(B)$. Se $det(M,b)$ é a unidade do anel A, a forma bilinear (M,b) é dita regular.

Sejam $\beta : R \longrightarrow A$ um homomorfismo de anéis tal que A é um R-módulo finitamente gerado e $s \in Hom_R(A,R)$, ou seja, s é uma aplicação tal que $c \cdot s(a) = s(ca), \forall c \in R, \forall a \in A$. Então a aplicação $(x,y) \in A \times A \longrightarrow s(xy)$ define uma forma bilinear (A,s) sobre R. De forma geral, se $\mathscr{I}$ é um ideal em A tal que $\mathscr{I}$ é um R-módulo finitamente gerado, então $(x,y) \in \mathscr{I} \times \mathscr{I} \longrightarrow s(xy)$ define uma forma bilinear $(\mathscr{I}, s)$ sobre R. Neste caso, $(\mathscr{I}, s)$ é chamada *forma traço em escala* do anel quociente A/R.

Um reticulado integral é definido como um par (M,b), tal que M é um $\mathbb{Z}$-módulo livre de posto n, e $b : M \times M \longrightarrow \mathbb{Z}$ é uma forma bilinear simétrica. O reticulado (M,b) é dito definido positivo (respectivamente negativo) se $b(x,x) > 0$ (respectivamente $b(x,x) < 0$), para todo $0 \neq x \in M$ [16]. Seja $\mathscr{O}_{\mathbb{K}}$ o anel dos inteiros algébricos do corpo $\mathbb{K}$. Considere o codiferente da extensão $\mathbb{K}|\mathbb{Q}$ dado por $\mathscr{D}^{-1}_{\mathbb{K}|\mathbb{Q}} = \left\{x \in \mathbb{K};\ Tr_{\mathbb{K}|\mathbb{Q}}(x\mathscr{O}_{\mathbb{K}}) \subseteq \mathbb{Z}\right\}$. Sejam $\bar{\cdot} : \mathbb{K} \longrightarrow \mathbb{K}$ uma $\mathbb{Q}$-involução de $\mathbb{K}$, ou seja, uma aplicação aditiva e multiplicativa tal que $\bar{\bar{x}} = x, \forall x \in \mathbb{K}$, e $F = \{x \in \mathbb{K};\ \bar{x} = x\}$ o corpo fixo da involução.

Definição 4.1.1. *Dado um ideal $\mathscr{I}$ de $\mathscr{O}_{\mathbb{K}}$ e $\alpha \in F$ tal que $\alpha\mathscr{I}\overline{\mathscr{I}} \subseteq \mathscr{D}^{-1}_{\mathbb{K}|\mathbb{Q}}$, definimos um reticulado ideal como um reticulado integral $(\mathscr{I}, b_\alpha)$, onde $b_\alpha : \mathscr{I} \times \mathscr{I} \longrightarrow \mathbb{Z}$ é uma forma bilinear tal que $b_\alpha(x,y) = Tr_{\mathbb{K}|\mathbb{Q}}(\alpha x\bar{y})$, $\forall x, y \in \mathscr{I}$.*

O reticulado ideal é integral, garantido pela condição $\alpha\mathscr{I}\overline{\mathscr{I}} \subseteq \mathscr{D}^{-1}_{\mathbb{K}|\mathbb{Q}}$. Além disso, α é tomado no corpo fixo F para garantir que a forma traço é simétrica [16], pois

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

onde a ultima igualdade é válida pois $Tr_{\mathbb{K}|\mathbb{Q}}(z) \in \mathbb{Q}$, $\forall \in \mathbb{K}$.

Seja $\mathbb{K}$ um corpo de números de grau n, isto é, $\mathbb{K} = \mathbb{Q}(\theta)$, com $\theta \in \mathbb{C}$ uma raiz de um polinômio mônico irredutível $p(x) \in \mathbb{Z}[x]$. As n raízes distintas de $p(x)$ em seu corpo de raízes, a saber, $\theta_1, \theta_2, \cdots, \theta_n$, são chamadas conjugados de θ. Os *mergulhos* em $\mathbb{K}$ são homomorfismos $\sigma_i(\theta) = \theta_i$, para todo $i = 1, 2, \cdots, n$. Assim, os mergulhos σ_i, para $i = 1, \cdots, n$, são os n $\mathbb{Q}$-homomorfismos distintos de $\mathbb{K}$ em $\mathbb{C}$ tal que $\sigma_1, \cdots, \sigma_{r_1}$ são reais e $\sigma_{r_1+1}, \cdots, \sigma_{r_1+r_2}$, $\sigma_{r_1+r_2+1}, \cdots, \sigma_{r_1+2r_2}$ são imaginários, onde $\sigma_{r_1+r_2+i}$ é o complexo conjugado de σ_{r_1+i}, para todo $i = 1, \cdots, r_2$. Neste caso, $n = r_1 + 2r_2$. Se todos os mergulhos em $\mathbb{K}$ forem reais, neste caso $r_1 = n$ e $r_2 = 0$, (resp. complexos, neste caso, $r_1 = 0$ e $2r_2 = n$), $\mathbb{K}$ é dito totalmente real (resp. totalmente complexo).

Definição 4.1.2. *Definimos como mergulho canônico o homomorfismo $\sigma : \mathbb{K} \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ definido por*

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

Se $\mathbb{K}$ é totalmente real, definimos $\sigma : \mathbb{K} \longrightarrow \mathbb{R}^n$ como

$$\sigma(x) = (\sigma_1(x), ..., \sigma_{r_1}(x), ..., \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x) ..., \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)) \in \mathbb{R}^n,$$

de modo que $\Re$ e $\Im$ denotam a parte real e imaginária, respectivamente.

O mergulho canônico associa uma base de $\mathbb{K}$ (como um $\mathbb{Q}$-espaço vetorial) a uma base do $\mathbb{R}^n$, como mostra o próximo resultado.

Teorema 4.1.3. *[9] Se $\{w_1, w_2, ..., w_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, então $\sigma(w_1), \sigma(w_2), ..., \sigma(w_n)$ são linearmente independentes e, portanto, uma base de $\mathbb{R}^n$.*

Para a prova do teorema, basta verificar que $det(\sigma(w_i)_{i=1}^n)$ é diferente de zero. Tomando $\alpha \in \mathbb{K}$ um elemento tal que $\sigma_i(\alpha)$ é real positivo, $\forall i$, podemos generalizar a definição de mergulho pela adjunção de α. Definimos o *mergulho rotacionado* como a aplicação $\sigma_\alpha : \mathbb{K} \longrightarrow \mathbb{R}^n$ dado por

$$\sigma_\alpha(x) = (\sqrt{\alpha_1}\sigma_1(x), ..., \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x)), \sqrt{2\alpha_{r_1+1}}\Im(\sigma_{r_1+1}(x)), ...,$$

$$\sqrt{2\alpha_{r_1+r_2}}\Re(\sigma_{r_1+r_2}(x)), \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x)).$$

O teorema acima pode ser estendido também para mergulhos rotacionados, de modo que a imagem do mergulho rotacionado de uma base de $\mathbb{K}$ nos dá uma base de $\mathbb{R}^n$. Como consequência, temos o seguinte resultado.

Proposição 4.1.4. *[16] Se G é um $\mathbb{Z}$-módulo livre de posto n do anel $\mathscr{O}_{\mathbb{K}}$ com uma $\mathbb{Z}$-base $\{w_1, w_2, ..., w_n\}$, então a imagem $\sigma_\alpha(G)$ é um reticulado no $\mathbb{R}^n$ com geradores $\sigma_\alpha(w_1), ..., \sigma_\alpha(w_n)$.*

Como qualquer ideal $\mathscr{I}$ do anel dos inteiros algébricos $\mathscr{O}_{\mathbb{K}}$ possui uma $\mathbb{Z}$-base com n elementos, podemos utilizar o resultado acima considerando $\mathscr{I} \subseteq \mathscr{O}_{\mathbb{K}}$. Deste modo, se $\{\omega_1, \omega_2, ..., \omega_n\}$ é uma $\mathbb{Z}$-base de $\mathscr{I} \subseteq \mathscr{O}_{\mathbb{K}}$, então o reticulado $\sigma_\alpha(\mathscr{I})$ possui geradores $\sigma_\alpha(\omega_1), ..., \sigma_\alpha(\omega_n)$, com uma matriz geradora dada por

$$\begin{pmatrix} \sqrt{\alpha_1}\sigma_1(\omega_1) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(\omega_1) & \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(\omega_1) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(\omega_1) \\ . & \cdots & . & . & \cdots & . \\ . & \cdots & . & . & \cdots & . \\ . & \cdots & . & . & \cdots & . \\ \sqrt{\alpha_1}\sigma_1(\omega_n) & \cdots & \sqrt{\alpha_{r_1}}\sigma_{r_1}(\omega_n) & \sqrt{2\alpha_{r_1+1}}\Re\sigma_{r_1+1}(\omega_n) & \cdots & \sqrt{2\alpha_{r_1+r_2}}\Im\sigma_{r_1+r_2}(\omega_n) \end{pmatrix}$$

com $\alpha_i = \sigma_i(\alpha)$, $\forall i$ [16].

Quando $\mathbb{K}$ é um corpo totalmente real, o reticulado $\sigma_\alpha(\mathscr{I})$ dado acima é um reticulado ideal definido positivo [16]. Basta verificar que a forma bilinear associada $(\mathscr{I}, b_\alpha)$ é uma forma traço.

Como vimos, o determinante de um reticulado é definido como o determinante da matriz de Gram e, de modo equivalente, fornece o volume ao quadrado da região fundamental. No entanto, no caso de reticulados ideais, podemos determinar o determinante através de propriedades algébricas do corpo de números $\mathbb{K}$. O resultado a seguir estabelece essa relação.

Proposição 4.1.5. *[16] Sejam $\mathbb{K}$ um corpo de números, com discriminante $d_{\mathbb{K}}$, $\mathscr{I}$ um ideal em $\mathscr{O}_{\mathbb{K}}$ e $(\mathscr{I}, b_\alpha)$ um reticulado ideal. O determinante de $(\mathscr{I}, b_\alpha)$ é dado por*

$$|det(b_\alpha)| = N(\alpha)N(\mathscr{I})^2|d_{\mathbb{K}}|.$$

Dados dois vetores $x, y \in \mathbb{R}^n$, sua *diversidade* é definida como o número de coordenadas diferentes de x e y, ou seja, a cardinalidade do conjunto $\{i;\ x_i \neq y_i,\ i = 1, 2, ..., n\}$. Dado um subconjunto $S \subseteq \mathbb{R}^n$, a diversidade de S é definida como a menor das diversidades entre os elementos de S, ou seja, por

$$\min_{x,y \in S} \#\{i;\ x_i \neq y_i,\ 1 \leq i \leq n\}.$$

Como um reticulado está contido no $\mathbb{R}^n$, podemos definir a diversidade para os reticulados, reformulando como o número de componentes não-nulas de qualquer vetor não-nulo do reticulado [16].

Definição 4.1.6. *A diversidade de um reticulado $\Lambda \in \mathbb{R}^n$ é definida por*

$$div(\Lambda) = \min_{0 \neq x \in \Lambda} \#\{i;\ x_i \neq 0,\ 1 \leq i \leq n\}.$$

Deste Modo, a diversidade será máxima quando todas as componentes entre dois pontos são distintas. Isto é obtido via reticulados conhecidos ao se considerar uma rotação da região fundamental deste reticulado, obtêm-se a região fundamental do reticulado rotacionado. Desta forma todos os pontos reticulados têm diversidade máxima. Neste sentido, uma alternativa é considerar reticulados algébricos que sejam obtidos via corpos de números totalmente reais.

O resultado a seguir apresenta os parâmetros para determinar a diversidade em reticulados ideais.

Teorema 4.1.7. *[16] Reticulados ideais $\Lambda = (\mathscr{I}, b_\alpha)$ possuem diversidade dada por*

$$div(\Lambda) = r_1 + r_2.$$

Demonstração. Seja $0 \neq X \in \Lambda$ um ponto qualquer. Então X é dado por

$$X = (\sqrt{\alpha_1}\sigma_1(x), ..., \sqrt{\alpha_{r_1}}\sigma_{r_1}(x), \sqrt{2\alpha_{r_1+1}}\Re(\sigma_{r_1+1}(x)), ..., \sqrt{2\alpha_{r_1+r_2}}\Im(\sigma_{r_1+r_2}(x)),$$

com $x \in \mathscr{I} \subseteq \mathscr{O}_{\mathbb{K}}$. Como $X \neq 0$, temos que $x \neq 0$ e portanto os primeiros r_1 coeficientes são não nulos. Como as partes real e imaginária de qualquer um dos mergulhos complexos não podem zerar simultaneamente, temos que o número mínimo de coeficientes não nulos entre os $2r_2$ restantes é r_2. Logo temos uma diversidade $L \geq r_1 + r_2$. Além disto, aplicando os mergulhos canônicos em $x = 1$, obtemos exatamente $r_1 + r_2$ coeficientes não nulos, o que conclui que $div(\Lambda) = r_1 + r_2$. ■

Deste modo, a partir do teorema acima, temos que reticulados ideais construídos a partir de corpos de números totalmente reais, ou seja, com $r_1 = n$ e $r_2 = 0$, possuem diversidade máxima n. A partir da diversidade do reticulado, podemos definir o conceito de distância produto mínima, um parâmetro de grande importância para os reticulados construídos.

Definição 4.1.8. *Dado Λ um reticulado n-dimensional com diversidade máxima $div(\Lambda) = n$, definimos a distância produto mínima por*

$$d_{p,min}(\Lambda) = \min_{0 \neq x \in \Lambda} \prod_{i=1}^{n} |x_i|.$$

Se $\mathbb{K}$ é um corpo de números totalmente real, podemos reescrever a distância produto mínima a partir de propriedades algébricas de $\mathbb{K}$, dado pelo resultado a seguir.

Teorema 4.1.9. *[16] Sejam $\mathbb{K}$ um corpo de números de grau n totalmente real, com discriminante $d_{\mathbb{K}}$, e $\mathscr{I}$ um ideal do anel dos inteiros $\mathscr{O}_{\mathbb{K}}$. A distância produto mínima do reticulado ideal $\Lambda = (\mathscr{I}, b_\alpha)$, de determinante $det(b_\alpha)$, é dada por*

$$d_{p,min}(\Lambda) = \sqrt{\frac{det(b_\alpha)}{d_{\mathbb{K}}}}\, min(\mathscr{I}),$$

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

Demonstração. Seja $X = \sigma_\alpha(x)$ um ponto do reticulado no $\mathbb{R}^n$, tal que $x \in \mathscr{I} \subseteq \mathscr{O}_{\mathbb{K}}$ é seu inteiro algébrico correspondente. Então

$$d_{p,min}(\Lambda) = \min_{0 \neq X \in \Lambda} \prod_{i=1}^{n} |\sqrt{\sigma_i(\alpha)}\sigma_i(x)| = \sqrt{N(\alpha)} \min_{0 \neq x \in \mathscr{I}} |N(x)|.$$

Substituindo $N(\alpha) = \frac{|det(b_\alpha)|}{N(\mathscr{I})^2 |d_{\mathbb{K}}|}$, o resultado fica provado. ■

Quando $\mathscr{I}$ é um ideal principal, a distância produto mínima de $\Lambda = (\mathscr{I}, b_\alpha)$ é dada por

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

pois $\min_{0 \neq x \in \mathscr{I}} |N(x)| = N(\mathscr{I})$, quando $\mathscr{I}$ é ideal principal.

Podemos ainda reescrever a expressão para a distância produto mínima utilizando outro conceito algébrico, que definiremos a seguir. Com isso, introduzimos na computação da distância uma $\mathbb{Z}$-base com n elementos, que será obtida através do algoritmo de construção do método, como veremos posteriormente.

Definição 4.1.10. *Uma ordem $\mathfrak{D}$ no corpo $\mathbb{K}$ é um subanel de $\mathbb{K}$ que como um $\mathbb{Z}$-módulo é finitamente gerado e possui posto máximo $n = [\mathbb{K} : \mathbb{Q}]$.*

Pode ser mostrado que $\mathscr{D} \subset \mathscr{O}_{\mathbb{K}}$, para qualquer ordem de $\mathbb{K}$, e que $\mathscr{O}_{\mathbb{K}}$ é também uma ordem, chamada *ordem maximal* de $\mathbb{K}$ [16]. Se $\mathscr{I}$ é um ideal não-nulo da ordem $\mathfrak{D}$, então $\mathscr{I}$ é um $\mathbb{Z}$-módulo de posto máximo n. Neste caso, todos os conceitos e resultados sobre reticulados ideais vistos até aqui se estendem para ideais em uma ordem. A distância produto mínima é dada pelo seguinte resultado.

Teorema 4.1.11. *[16] Sejam $\mathfrak{D}$ uma ordem do corpo $\mathbb{K}$, com discriminante $d_{\mathbb{K}}$, e $\mathscr{I}$ um ideal de $\mathfrak{D}$. A distância produto mínima de um reticulado ideal $\Lambda = (\mathscr{I}, b_\alpha)$ de determinante $det(b_\alpha)$ é dada por*

$$d_{p,min}(\Lambda) = \sqrt{\frac{det(b_\alpha)}{d_{\mathbb{K}}}} \frac{min(\mathscr{I})}{[\mathscr{O}_{\mathbb{K}} : \mathscr{D}]},$$

em que $min(\mathscr{I}) = \min_{0 \neq x \in \mathscr{I}} \frac{N(x)}{N(\mathscr{I})}$ e $[\mathscr{O}_{\mathbb{K}} : \mathscr{D}]$ é o índice de $\mathscr{D}$ em $\mathscr{O}_{\mathbb{K}}$.

A *distância produto mínima relativa* de Λ, definida a seguir, será usada para comparação considerando sempre reticulados com volume igual a 1.

Definição 4.1.12. *A distância produto mínima relativa do reticulado $\Lambda = (\mathscr{I}, b_\alpha)$, denotada por $d_{p,rel}(\Lambda)$, é definida pela distância produto mínima da versão escalonada $\frac{1}{\sqrt[2n]{det(b_\alpha)}} \cdot \Lambda$, isto é,*

$$d_{p,rel}(\Lambda) = \frac{1}{\sqrt{det(b_\alpha)}} \cdot d_{p,min}(\Lambda).$$

A distância produto mínima relativa não depende da escolha de α. Para comparar distância produto minima relativa em diferente dimensões, trabalhamos com a distância produto mínima relativa normalizada $\sqrt[n]{d_{p,rel}(\Lambda)}$.

Seja $\mathbb{K}$ um corpo de números e $\mathscr{O}_{\mathbb{K}}$ seu anel dos inteiros algébricos. Se $I_{\mathbb{K}}$ denota o grupo dos ideais fracionários de $\mathbb{K}$ e $P_{\mathbb{K}}$ denota o subgrupo de $\mathbb{K}$ formado por ideais principais, então o *ideal class group*, denotado por $Cl(\mathbb{K})$, é $Cl(\mathbb{K}) = I_{\mathbb{K}}/P_{\mathbb{K}}$. O *class number* de $\mathbb{K}$, denotado por $h(\mathbb{K})$, é a cardinalidade de $Cl(\mathbb{K})$. Em particular, se $\mathscr{O}_{\mathbb{K}}$ é um ideal principal, então $h(\mathbb{K}) = 1$. O *class number* de um corpo $\mathbb{K}$ pode ser entendido como a medida de quão principal um anel dos inteiros é, ou seja, qual a proporção dos ideais principais entre todos os ideais.

Se $\mathscr{I}$ é um ideal principal, então $\min\{\mathscr{I}\} = 1$ e consequentemente, a distância produto minima de Λ é dada por

$$d_{p,\min}(\Lambda) = \sqrt{\frac{\det(b_\alpha)}{d_{\mathbb{K}}}} \frac{1}{[\mathscr{O}_{\mathbb{K}} : \mathfrak{D}]}.$$

4.2 Teoremas de Taussky e Krüskemper

Os teoremas de Taussky e Krüskemper, apresentados abaixo, garantem que qualquer reticulado inteiro pode ser construído como um reticulado ideal do quociente $\mathbb{Z}[x]/\langle f \rangle$, com $f \in \mathbb{Z}[x]$ um polinômio mônico irredutível.

Uma matriz S simétrica não-singular $n \times n$ sobre um corpo $\mathbb{K}$ é dita uma *matriz de forma traço em escala* se, e somente se, existe uma extensão $\mathbb{L}|\mathbb{K}$ de grau n, e se existem um fator de escala $\alpha \in \mathbb{L}\setminus\{0\}$ e uma base $\{w_1, \cdots, w_n\}$ de $\mathbb{L}$ sobre $\mathbb{K}$ tais que

$$S = \left[Tr_{\mathbb{L}|\mathbb{K}}(\alpha \cdot w_i \cdot w_j)\right].$$

Pelo trabalho de Taussky em [12] podemos caracterizar essas matrizes pelo seguinte teorema.

Teorema 4.2.1. *[15] Uma matriz S simétrica não-singular $n \times n$ sobre um corpo $\mathbb{K}$ é a matriz de uma forma traço em escala se, e somente se, existe uma matriz A, $n \times n$ sobre $\mathbb{K}$, com polinômio característico irredutível em $\mathbb{K}[x]$ tal que $AS = SA^t$.*

Demonstração. Suponha que S é uma matriz de uma forma traço em escala, ou seja, existem uma extensão $\mathbb{L}|\mathbb{K}$ de grau n, um fator de escala $\alpha \in \mathbb{L}\setminus\{0\}$ e uma base $\{w_1, \cdots, w_n\}$ tais que

$$S = \left[Tr_{\mathbb{L}|\mathbb{K}}(\alpha \cdot w_i \cdot w_j)\right].$$

Sejam $\theta \in \mathbb{L}$ um gerador primitivo de $\mathbb{L}$ sobre $\mathbb{K}$ e $f \in \mathbb{K}[x]$ o polinômio irredutível de θ. Além disso, considere V como a soma direta de $\mathbb{L}$ com si mesmo n vezes e $\sigma \in V$ o vetor $[1, \theta, \cdots, \theta^{n-1}]^t$. Tomando C como a matriz companheira de f, temos $C\sigma = \theta\sigma$. Logo C define um operador linear sobre V para o qual σ é um autovetor associado ao autovalor θ. Seja ω o vetor coluna $[w_1, \cdots, w_n]^t$. Como $\{w_1, \cdots, w_n\}$ e $\left\{1, \theta, \cdots, \theta^{n-1}\right\}$ são ambas bases de $\mathbb{L}$ sobre $\mathbb{K}$, temos que existe uma matriz não-singular mudança de base P sobre $\mathbb{K}$ tal que $P\omega = \sigma$. Colocando $A = P^{-1}CP$, temos $A\omega = \theta\omega$, ou seja, A é semelhante à C, portanto o polinômio característico de A é igual a $f \in \mathbb{K}[x]$, que é irredutível.

Além disso, sejam $\sigma_1, \cdots, \sigma_n$ distintos $\mathbb{K}$-lineares mergulhos de $\mathbb{L}$ em seu fecho normal sobre $\mathbb{K}$. Tomando as matrizes

$$M = [\sigma_i(w_j)]$$

e

$$D(\theta) = \begin{pmatrix} \sigma_1(\theta) & 0 & \cdots & 0 \\ 0 & \sigma_2(\theta) & \cdots & 0 \\ . & . & \cdots & . \\ . & . & \cdots & . \\ . & . & \cdots & . \\ 0 & 0 & \cdots & \sigma_n(\theta) \end{pmatrix}$$

temos

$$AM^t = M^t D(\theta)$$

e

$$MA^t = D(\theta)M.$$

A matriz S é representada da seguinte forma. Considere outra matriz diagonal

$$D(\alpha) = \begin{pmatrix} \sigma_1(\alpha) & 0 & \cdots & 0 \\ 0 & \sigma_2(\alpha) & \cdots & 0 \\ . & . & \cdots & . \\ . & . & \cdots & . \\ . & . & \cdots & . \\ 0 & 0 & \cdots & \sigma_n(\alpha) \end{pmatrix}.$$

Então

$$S = [Tr_{\mathbb{L}|\mathbb{K}}(\alpha w_i w_j)] = M^t D(\alpha) M.$$

No entanto, temos

$$AM^tD(\alpha)M = M^tD(\theta)D(\alpha)M$$

e

$$M^tD(\alpha)MA^t = M^tD(\alpha)D(\theta)M.$$

Como matrizes diagonais comutam, temos

$$AM^tD(\alpha)M = M^tD(\alpha)MA^t,$$

ou seja, $AS = SA^t$. A recíproca pode ser encontrada em (1), em [12]. ■

Consideremos M um $\mathbb{Z}$-módulo livre finitamente gerado de posto n e $b : M \times M \longrightarrow \mathbb{Z}$ uma forma bilinear simétrica. Sejam $f \in \mathbb{Z}[x]$ um polinômio mônico irredutível de grau n e θ uma raiz de f. Então $\mathbb{Z}[x]/\langle f\rangle = \mathbb{Z}[\theta]$ é um $\mathbb{Z}$-módulo livre de posto n, com base $\left\{1, \theta, \theta^2, \cdots, \theta^{n-1}\right\}$ [16]. Considerando $\mathscr{A}$ um ideal de $\mathbb{Z}[\theta]$, colocamos $\mathscr{A}^{\#} = \{c \in \mathbb{Q}(\theta) \mid Tr(c\mathscr{A}) \subseteq \mathbb{Z}\}$. A partir disto, podemos enunciar o teorema de Taussky. Antes, precisamos dos seguintes lemas, cujas demonstrações se encontram em [13] e [14].

Lema 4.2.2. *[13] O número algébrico θ é raiz do polinômio característico da matriz A (no teorema abaixo) e os componentes do vetor correspondente v_θ podem ser escolhidos de modo a formar a base de um ideal no anel formado por polinômios em θ com coeficientes inteiros racionais.*

Lema 4.2.3. *[14] Se a matriz A corresponde a classe ideal determinada pelo ideal $\mathscr{A} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ e sua transposta A^t corresponde ao ideal $\mathscr{B} = (\beta_1, \beta_2, \cdots, \beta_n)$, então $\mathscr{B}$ pertence a classe inversa de $\mathscr{A}$.*

Teorema 4.2.4. *(Taussky) [16] Seja $B \in M_n(\mathbb{Z})$ uma matriz simétrica não singular. Seja $A \in M_n(\mathbb{Z})$ uma matriz tal que seu polinômio característico χ_A é irredutível e $B^{-1}AB = A^t$. Então B é a matriz de um reticulado ideal.*

Demonstração. Seja $\theta \in \mathbb{C}$ uma raiz de χ_A. Como χ_A é mônico irredutível, com coeficientes em $\mathbb{Z}$, então θ é um inteiro algébrico. Pelo Lema 4.2.2, existe um autovetor $v_\theta = (v_1, \cdots, v_n)^t$ de A associado a θ, com $v_i \in \mathbb{Z}[\theta]$ e tal que $\{v_1, \cdots, v_n\}$ forma uma $\mathbb{Z}$-base de um ideal de $\mathbb{Z}[\theta]$. Pela prova do Lema 4.2.3, temos que existe um autovetor $v'_\theta = (v'_1, \cdots, v'_n)^t$ de A^t associado a θ tal que $v'_i \in \mathbb{Q}(\theta)$ e

$$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(v_i v'_j) = \delta_{ij}, \quad \forall i, j$$

Como $A^t = B^{-1}AB$, temos que $A^tB^{-1}v_\theta = B^{-1}Av_\theta = \theta B^{-1}v_\theta$ e portanto v'_θ e $B^{-1}v_\theta$ são ambos autovetores de A^t associados a θ. Como $\chi_A = \chi_{A^t}$ é irredutível sobre $\mathbb{Q}$, temos que é também separável, de onde segue que os autovalores são distintos e, portanto, os subespaços de autovetores associados são de dimensão 1. Logo existe $\alpha \in \mathbb{Q}(\theta)$ tal que $v'_\theta = \alpha B^{-1}v_\theta$, ou seja, $Bv'_\theta = \alpha v_\theta$. Se $B = (b_{ij})$, temos que

$$\sum_{j=1}^{n} b_{ij}v'_j = \alpha v_i, \ \forall i.$$

Então

$$\sum_{j=1}^{n} b_{ij}v'_j v_k = \alpha v_i v_k, \ \forall i, k.$$

Logo, temos

$$\sum_{j=1}^{n} b_{ij}Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(v'_j v_k) = Tr_{\mathbb{Q}(\theta|\mathbb{Q})}(\alpha v_i v_k).$$

Portanto, como $Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(v_i v'_j) = \delta_{ij}$, temos que $b_{ik} = Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\alpha v_i v_k)$, de onde concluímos que B é a matriz de um reticulado ideal $\mathscr{A} = \mathbb{Z}v_1 \oplus \mathbb{Z}v_2 \oplus \cdots \oplus \mathbb{Z}v_n$. ■

Podemos reescrever os últimos resultados da seguinte forma: dada uma matriz B simétrica $n \times n$ com coeficientes inteiros tal que $detB \neq 0$, M uma matriz quadrada de ordem n com coeficientes inteiros tal que $BM^t = MB$, onde o polinômio característico χ_M de M é irredutível e $A := \mathbb{Z}[x]/\langle \chi_M \rangle$, então existe $c \in \mathbb{Q}(A)$ e $v_1, \cdots, v_n \in A$ tal que $\mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$ é um ideal em A e $B = Tr(cv_i v_j)$. Além disso, $(v_1, \cdots, v_n)^t \in \mathbb{Q}(A)^n$ é um autovetor de M, com coeficientes em $\mathbb{Q}(A)$.

Dada qualquer matriz simétrica quadrada de ordem n com coeficientes inteiros, podemos sempre encontrar A tal que $BA^t = AB$. De fato, escolhendo qualquer matriz S simétrica de ordem n com coeficientes inteiros e colocando $A := BS$, temos então $BA^t = B(BS)^t = BS^tB^t = (BS)B = AB$. Além disto, o Lema 4.2.5 garante que existe tal matriz A com polinômio característico irredutível.

Lema 4.2.5. *(Krüskemper) Dada qualquer matriz B simétrica $n \times n$ sobre $\mathbb{Z}$, com $det(B) \neq 0$, existe uma matriz A simétrica $n \times n$, com entradas inteiras, tal que $BA^t = AB$ e polinômio característico $\chi_A \in \mathbb{Z}[x]$ irredutível. Além disso, χ_A pode ser assumido totalmente real, ou seja, suas raízes são todas reais.*

Demonstração. Seja $N = (x_{ij})$ uma matriz simétrica $n \times n$ cujos coeficientes $x_{ij} = x_{ji}$ são indeterminados. Escolhendo C uma matriz invertível $n \times n$ com coeficientes em $\mathbb{Q}$ tal que C^tBC é uma matriz diagonal, em [17] é mostrado que $C^{-1}N(C^{-1})^t$ é uma matriz simétrica com coeficientes indeterminados, de modo que o polinômio característico de $(C^tBC)C^{-1}N(C^{-1})^t$ é irredutível, e portanto o polinômio característico de BN é também irredutível. Pelo teorema da irredutibilidade de Hilbert, existe $a_{ij} = a_{ji} \in \mathbb{Q}$ tal que $\chi_{B(aij)}(x)$ é irredutível. Escolhendo $a \in \mathbb{Z}$ tal que todo $aa_{ij} \in \mathbb{Z}$, temos que $\chi_{B(aa_{ij})}(x) = a^n \chi_{B(aij)}(a^{-1}x)$ é irredutível. Definindo $A = B(aa_{ij})$, temos $BA^t = B(aa_{ij})^t B^t = AB$.

Por fim, segundo [17] podemos escolher os coeficientes a_{ij} de modo que $\chi_{B(aij)}$ seja totalmente real e, por consequência, com $\chi_{B(aaij)}$ também totalmente real. ■

Segue diretamente deste Lema o seguinte resultado:

Teorema 4.2.6. *(Krüskemper) Seja (M,b) uma forma bilinear sobre $\mathbb{Z}$ tal que $det(M,b) \neq 0$. Então existem um polinômio $f \in \mathbb{Z}[x]$ mônico irredutível, algum ideal $I \subset A := \mathbb{Z}[x]/\langle f(x) \rangle$, e $\alpha \in (I^2)^{\#}$ tais que $(M,b) = (I, Tr_\alpha)$. Além disso, podemos assumir f totalmente real.*

Em termos de reticulados, podemos reescrever o teorema de Krüskemper do seguinte modo, como colocado em [16]: dado (M,b) um reticulado ideal, existem um inteiro algébrico θ, um ideal I de $\mathbb{Z}[\theta]$ e $\alpha \in (I^2)^{\#} \subseteq \mathbb{Q}(\theta)$ tais que b é isomorfo ao bilinear $I \times I \longrightarrow \mathbb{Z}$ dado por $(x,y) \longmapsto Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\alpha xy)$. Neste caso, θ pode ser assumido totalmente real.

4.3 Algoritmo para a construção dos reticulados

A partir dos teoremas de Taussky e Krüskemper, apresentamos o algoritmo de construção, cuja entrada é a matriz de Gram B de um reticulado, fornecendo uma matriz geradora do reticulado, baseado no trabalho de [16]. O algoritmo determina um conjunto $\{v_1, v_2, \cdots, v_n\}$ e um

elemento α tais que $I = \mathbb{Z}v_1 \oplus \mathbb{Z}v_2 \oplus \cdots \oplus \mathbb{Z}v_n$ e de modo que o reticulado ideal (I, b_α) dado por

$$b_\alpha : I \times I \longrightarrow \mathbb{Z}$$

$$(x,y) \longmapsto Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\alpha xy)$$

possui B como matriz de Gram.

Então, dada a matriz de Gram B de um reticulado, a construção é dada pelo seguinte procedimento.

Passo 1: Determinação da matriz A

Uma matriz A, $n \times n$ com entradas inteiras, satisfazendo $AB = BA^t$, cujo polinômio característico χ_A é irredutível, pode ser gerada aleatoriamente ou construída de modo a obter um corpo de números com polinômio minimal χ_A.

Passo 2: Determinação de uma $\mathbb{Z}$-base para o ideal I

A prova do teorema de Taussky garante que existe um autovetor v_θ da matriz A associado ao autovalor θ, raiz de χ_A, tal que $I = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$. Segundo [13], temos que

$$v_j := (-1)^{i+j}\Delta_{ij}(A - \theta I_n),$$

onde Δ_{ij} é a j-ésima menor, fixada uma i-ésima linha de $A - \theta I_n$, sendo I_n a matriz identidade de ordem n.

A proposição abaixo mostra que v_θ é, de fato, autovetor de A associado a θ.

Proposição 4.3.1. *[16] O vetor v_θ é um autovetor da matriz A associado a θ.*

Demonstração. Queremos mostrar que $Av_\theta = \theta v_\theta$. Para isto, sejam $v_\theta = (v_1, v_2, ..., v_n)$ e $(A)_i$ a i-ésima linha de $A = (a_{ij})_{i,j=1}^n$. Sem perda de generalidade, podemos considerar $i = 1$. Mostraremos que $(A)_1 v_\theta = \theta v_1$. De fato,

$$(A)_1 v_\theta = a_{11}\Delta_{11}(A - \theta I_n) + a_{12}(-1)\Delta_{12}(A - \theta I_n) + ... + a_{1n}(-1)^{1+n}\Delta_{1n}(A - \theta I_n)$$

$$= det(A - \theta I_n) + \theta\Delta(A - \theta \mathbb{I}_n) = \theta v_1$$

Procedendo de modo análogo para $i = 2, 3, ..., n$, temos

$$(A)_i v_\theta = a_{i1}\Delta_{a11}(A - \theta I_n) + a_{i2}(-1)\Delta_{12}(A - \theta I_n) + ... + a_{in}(-1)^{1+n}\Delta_{1n}(A - \theta I_n)$$

$$= det(\tilde{A}) + \theta v_i,$$

na qual $\tilde{A}$ é a matriz obtida de $A - \theta I_n$ substituindo a primeira linha pela i-ésima linha. Como $det(\tilde{A}) = 0$, temos que $(A)_i v_\theta = \theta v_i$, para todo $i = 1, 2, ..., n$, o que prova que v_θ é autovetor de A. ■

Passo 3: Cálculo do elemento α

A prova do teorema de Taussky mostrou que existe um autovetor $v'_\theta = (v'_1, ..., v'_n)$ da matriz A^t associado a θ, de modo que cada $v'_i \in \mathbb{Q}(\theta)$ e de modo que $Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(v_i v'_j) = \delta_{ij}, \forall i, j$. Para calcular α, precisamos antes determinar v'_θ, dado pelo seguinte resultado.

Proposição 4.3.2. *[16] Seja v'_θ uma base dual de $\mathbb{Z}[\theta]$ para a forma traço $Tr(v_i v'_j) = \delta_{ij}, \forall i, j$. Então*

$$v'_j := \sum_{i=1}^{n} m_{ij}\theta^{i-1},$$

na qual $(m_{ij})_{i,j} = 1^n$ é a matriz dada por $G^{-1}(V^t)^{-1}$, com

$$G = (Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^{i-1}\theta^{j-1}))_{i,j=1}^{n}$$

e $V = (v_1, v_2, ..., v_n)$ é a matriz de coordenadas de $v_1, v_2, ..., v_n$ na base $\left\{1, \theta, ..., \theta^{n-1}\right\}$.

Demonstração. Os elementos $\{v_i\}_{i=1}^{n}$ da base podem ser expressos na base dual como

$$v_i = \sum_{i=1}^{n} a_{ij} v'_j.$$

Multiplicando esta igualdade por v_k e aplicando a forma traço, obtemos

$$Tr(v_i v_k) = \sum_{i=1}^{n} a_{ij} Tr(v'_j v_k) = a_{ik}.$$

Substituindo esta igualdade na anterior, obtemos que

$$v_i = \sum_{i=1}^{n} Tr(v_i v_j) v'_j,$$

que pode ser reescrito como

$$\begin{aligned}(v'_1, v'_2, ..., v'_n) &= (v_1, v_2, ..., v_n)(Tr(v_i v_j)_{i,j=1}^{n})^{-1} \\ &= (1, \theta, ..., \theta^{n-1}) V (V^t G V)^{-1} \\ &= (1, \theta, ..., \theta^{n-1}) G^{-1} (V^t)^{-1}.\end{aligned}$$

Isto implica em

$$v'_i = \sum_{i=1}^{n} m_{ij}\theta^j.$$

■

Retomando a prova do teorema de Taussky, conhecendo v'_θ, o elemento α é dado por $\alpha v_\theta = B v'_\theta$.

Passo 4: Cálculo da matriz geradora do reticulado

O último passo da construção é determinar a matriz geradora do reticulado, dada por

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(v_1) & \sqrt{\alpha_2}\sigma_2(v_1) & \cdots & \sqrt{\alpha_n}\sigma_n(v_1) \\ \sqrt{\alpha_1}\sigma_1(v_2) & \sqrt{\alpha_2}\sigma_2(v_2) & \cdots & \sqrt{\alpha_n}\sigma_n(v_2) \\ . & . & \cdots & . \\ . & . & \cdots & . \\ . & . & \cdots & . \\ \sqrt{\alpha_1}\sigma_1(v_n) & \sqrt{\alpha_2}\sigma_2(v_n) & \cdots & \sqrt{\alpha_n}\sigma_n(v_n) \end{pmatrix}$$

onde σ_i, com $i = 1, 2, ..., n$, denota os mergulhos reais em $\mathbb{Q}(\theta)$ e $\alpha_i = \sigma_i(\alpha)$, para $i = 1, 2, ..., n$.

Capítulo

5

Construções

Neste capítulo apresentamos os resultados obtidos pelas construções via o método descrito, no qual utilizamos os softwares Wolfram Mathematica 11.0 e PARI/GP para calcular o índice $[\mathscr{O}_{\mathbb{K}} : \mathfrak{D}]$ e o class number $h(\mathbb{K})$, respectivamente. O objetivo de nosso projeto é construir reticulados com melhor (maior) distância produto mínima possível. Neste sentido, utilizamos o software Wolfram Mathematica para implementar o algoritmo acima para computar os reticulados.

Lembrando que o class number de um corpo indica qual a proporção dos ideais principais entre todos os ideais, estamos interessados em determinar reticulados sobre ideais $\mathscr{O}_{\mathbb{K}}$ principais, ou seja, com $h(\mathbb{K}) = 1$. Deste modo, encontramos reticulados com distância produto mínima otimizada, pois $min(\mathscr{I}) = \min_{0 \neq x \in \mathscr{I}} \frac{N(x)}{N(\mathscr{I})}$ é um componente difícil de ser calculado em reticulados sobre ideias não-principais.

Para obter reticulados com maior distância produto mínima possível precisamos, então, seguir as seguintes condições:

- Utilizar uma ordem $\mathfrak{D} = \mathbb{Z}[\theta]$ de $\mathscr{O}_{\mathbb{K}}$ que seja maximal, ou seja, $[\mathscr{O}_{\mathbb{K}} : \mathfrak{D}] = 1$. Para isto, buscamos um corpo de números $\mathbb{K}$ com base integral canônica;
- trabalhar com corpos de números cujos anéis dos inteiros algébricos $\mathscr{O}_{\mathbb{K}}$ seja domínio de ideais principais, ou seja, com class number $h(\mathbb{K}) = 1$ e, portanto, $\min_{0 \neq x \in \mathscr{I}} \frac{N(x)}{N(\mathscr{I})} = 1$;
- trabalhar com corpos de números com menor discriminante possível.

Realizamos alguns testes onde verificamos que nem sempre o reticulado com o menor discriminante resulta em melhor distância produto, uma vez que existem outras variáveis envolvidas no processo, às vezes de nada adianta ter um discriminante menor se, por exemplo, $[\mathscr{O}_{\mathbb{K}} : \mathfrak{D}]$ for maior que 1, ou se o class number $h(K)$ relacionado for diferente de 1. Nos testes realizados notamos que corpos com valores altos para discriminantes ainda compensam, desde que $[\mathscr{O}_{\mathbb{K}} : \mathfrak{D}] = 1$ e $h(K) = 1$.

Lembramos que a matriz geradora de um reticulado ideal é dada por

$$M = \begin{pmatrix} \sqrt{\sigma_1(\alpha)}\sigma_1(v_1) & \cdots & \sqrt{\sigma_n(\alpha)}\sigma_n(v_1) \\ . & \cdots & . \\ . & \cdots & . \\ . & \cdots & . \\ \sqrt{\sigma_1(\alpha)}\sigma_1(v_n) & \cdots & \sqrt{\sigma_n(\alpha)}\sigma_n(v_n) \end{pmatrix}$$

de modo que $\alpha \in \mathbb{K}$ satisfaz $\sigma_i(\alpha) > 0, \forall i$, e $\{v_1, ..., v_n\}$ uma $\mathbb{Z}$-base do ideal $\mathscr{I}$. Além disso, por [18] temos que M satisfaz

$$MM^t = (Tr_{\mathbb{K}|\mathbb{Q}}(\alpha v_i v_j)))_{i,j=1}^n.$$

Então adotando $\alpha = 1$ e tomando $\{1, \theta, ..., \theta^{n-1}\}$ uma $\mathbb{Z}$-base de $\mathbb{Z}[\theta] \subseteq \mathscr{O}_{\mathbb{K}}$, com $\mathbb{K} = \mathbb{Q}(\theta)$, então a matriz G dada no passo 3 do algoritmo acima satisfaz

$$d_{\mathbb{K}} = (det(\sigma_i)(\theta^{j-1})_{i,j=1}^n)^2 = det(M^2) = det(M)det(M^t) = det(MM^t) =$$

$$det(Tr_{\mathbb{K}|\mathbb{Q}}(\theta^{i-1}\theta^{j-1})))_{i,j=1}^n = det(G),$$

pois $G = Tr_{\mathbb{K}|\mathbb{Q}}(\theta^{i-1}\theta^{j-1})))_{i,j=1}^n$.

5.1 Reticulado A_2

Uma matriz geradora para o reticulado A_2 é dada por $M = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix}$. Então sua matriz de Gram associada é dada por $B = MM^t = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$.

(1) No primeiro passo, calculamos a matriz A. Através da rotina abaixo, no Software Wolfram Mathematica, determinamos a matriz A. O primeiro passo do algoritmo é, dada como entrada uma matriz geradora do reticulado, determinar uma matriz A que satisfaz $AB = BA^t$, na qual B é a matriz de Gram.

```
M = {{-1, 1, 0}, {0, -1, 1}};
M.Transpose[M] // MatrixForm
   transposição      forma de matr
```

$$\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$$

```
B = {{2, -1}, {-1, 2}};

A = {{a11, a12}, {a21, a22}};

T = A.B
```

```
{{2 a11 - a12, -a11 + 2 a12}, {2 a21 - a22, -a21 + 2 a22}}
```

```
S = B.Transpose[A]
      transposição
```

```
{{2 a11 - a12, 2 a21 - a22}, {-a11 + 2 a12, -a21 + 2 a22}}
```

Figura 5.1: Algoritmo para calcular a matriz A.

Estabelecida a relação acima, $AB = BA^t$, o próximo passo do algoritmo é determinar A de modo que seu polinômio característico $\chi_A(x)$ seja irredutível. Colocamos como padrão estabelecer as entradas de A como inteiros entre -2 e 2. Testes feitos com maior número de entradas, como entre -5 e 5, obtiveram os mesmos resultados. Encontrada tal matriz, calculamos o discriminante e a base integral do corpo gerado por uma das raízes do polinômio característico, como mostra a segunda parte do algoritmo, representado na figura 5.2.

```
t1 = 2; t = 2;
For[a11 = -t1, a11 ≤ t, a11++,
 para cada
  For[a12 = -t1, a12 ≤ t, a12++,
   para cada
    For[a21 = -t1, a21 ≤ t, a21++,
     para cada
      For[a22 = -t1, a22 ≤ t, a22++,
       para cada
        r11 = -a11 + 2 a12 - 2 a21 + a22;
        If[r11 == 0,
         se
          m = {{a11, a12}, {a21, a22}};
          tt = CharacteristicPolynomial[m, x];
               polinômio característico
          T = IrreduciblePolynomialQ[tt];
              polinômio irredutível?
          If[T == True,
           se      verdadeiro
            SS = Solve[tt == 0, x];
                 resolve
            ib = NumberFieldIntegralBasis
                 base de inteiros de corpo numérico
              z = SS[[2]][[1]][[2]];
            dk = NumberFieldDiscriminant[z];
                 discriminante de corpo numérico
            If[dk ≤ 12,
             se
              vet = {tt, dk, m, ib};
              Print[vet];];];];];];];];];
              escreve
```

Figura 5.2: Algoritmo para determinar o discriminante e a base integral do corpo.

Como a distância produto mínima envolve $1/\sqrt[n]{d_{\mathbb{K}}}$ e $1/[\mathscr{O}_{\mathbb{K}} : \mathfrak{D}]$, buscamos encontrar o corpo com menor discriminante, de modo que a base integral não possua componentes com denominador maior que 1. Neste caso, temos $[\mathscr{O}_{\mathbb{K}} : \mathfrak{D}] = 1$, e quanto menor o discriminante, maior a distância produto mínima. As saídas do algoritmo pelo software são dadas na figura 5.3, onde são representadas dentro das chaves as informações relevantes, a saber: o polinômio característico, o discriminante do corpo e a matriz A procurada, respectivamente.

$\{-2+2x+x^2, 12, \{\{-2,-2\},\{-1,0\}\}\}$

$\{-3+x^2, 12, \{\{-2,-1\},\{1,2\}\}\}$

$\{-2+2x+x^2, 12, \{\{-2,1\},\{2,0\}\}\}$

$\{-3+x^2, 12, \{\{-1,-2\},\{-1,1\}\}\}$

$\{-3+x^2, 12, \{\{-1,1\},\{2,1\}\}\}$

$\{-2-2x+x^2, 12, \{\{0,-2\},\{-1,2\}\}\}$

$\{-2+2x+x^2, 12, \{\{0,-1\},\{-2,-2\}\}\}$

$\{-2-2x+x^2, 12, \{\{0,1\},\{2,2\}\}\}$

$\{-2+2x+x^2, 12, \{\{0,2\},\{1,-2\}\}\}$

$\{-3+x^2, 12, \{\{1,-1\},\{-2,-1\}\}\}$

$\{-3+x^2, 12, \{\{1,2\},\{1,-1\}\}\}$

$\{-2-2x+x^2, 12, \{\{2,-1\},\{-2,0\}\}\}$

$\{-3+x^2, 12, \{\{2,1\},\{-1,-2\}\}\}$

$\{-2-2x+x^2, 12, \{\{2,2\},\{1,0\}\}\}$

Figura 5.3: Saídas (resultados) da rotina acima.

Além disto, a terceira variável envolvida no cálculo da distância é $min(\mathscr{I}) = \min_{0\neq x\in\mathscr{I}} \frac{N(x)}{N(\mathscr{I})}$. Como este é um valor difícil de ser calculado, estamos interessados no caso em que $min(\mathscr{I}) = 1$, que é válido se $h(\mathbb{K}) = 1$, ou seja, se $\mathscr{O}_\mathbb{K}$ é ideal principal. Para determinar se $min(\mathscr{I}) = 1$, utilizamos o software PARI, onde colocamos como entrada o polinômio característico da matriz A e, se a saída do algoritmo é igual a 1, então $h(\mathbb{K}) = 1$. O algoritmo é dado na figura 5.4. Para $\chi_A(x) = x^2 - 3$, temos $h(\mathbb{K}) = 1$.

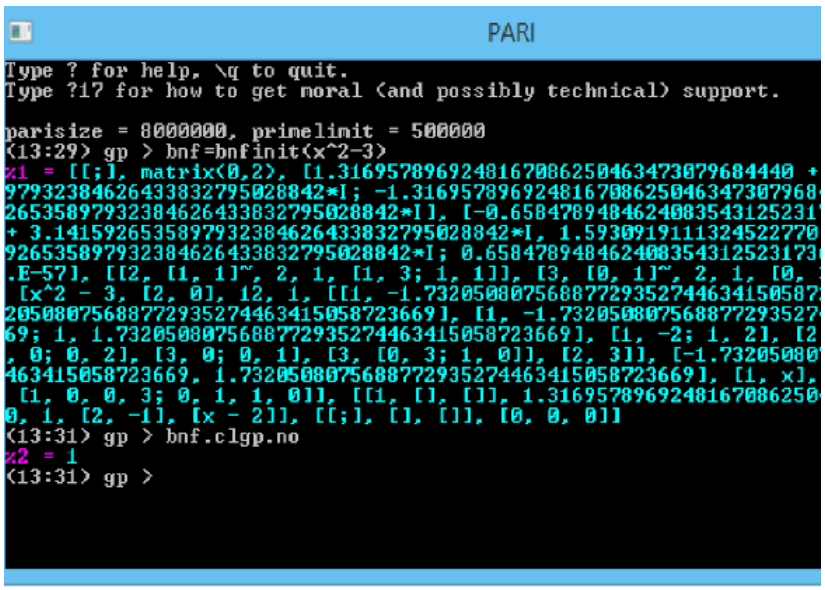

Figura 5.4: Algoritmo para determinar se $\mathscr{O}_\mathbb{K}$ é ideal principal - PARI.

Para o reticulado A_2, o menor discriminante encontrado pelo algoritmo foi $d_\mathbb{K} = 12$, com base integral canônica para o corpo de números $\mathbb{K} = \mathbb{Q}(\sqrt{3}.)$ Utilizamos para a construção uma

das matrizes encontradas, cujo polinômio característico é $\chi_A = x^2 - 3$.

Então, seja $\mathbb{K}$ o corpo de números dado pelo polinômio $x^2 - 3$. A matriz

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

possui polinômio característico $\chi_A(x) = x^2 - 3$, irredutível sobre $\mathbb{Q}$, e satisfaz a relação $B^{-1}AB = A^t$.

(2) Agora, calculemos o autovetor $v_\theta = (v_1, v_2)^t$ de A associado a θ tal que $\{v_1, v_2\}$ é uma $\mathbb{Z}$-base do ideal $\mathscr{I}$. Lembramos que

$$v_j = (-1)^{i+j}\Delta_{ij}(A - \theta I_2),$$

na qual $\Delta_{ij}(A - \theta I_2)$ é a menor obtida fixando uma das linhas, digamos a i-ésima linha. Tomando $i = 1$, ou seja, fixando a primeira linha, temos que

$$v_1 = (-1)^2\Delta_{11}(A - \theta I_2) = 1 - \theta$$

e

$$v_2 = (-1)^3\Delta_{12}(A - \theta I_2) = -1 \cdot 2 = -2.$$

Logo $v_\theta = (1 - \theta, -2)^t$.

(3) Para determinar o elemento α, precisamos calcular o autovetor $v'_\theta = (v'_1, v'_2)^t$ de A^t associado a θ, de modo que α é dado por $\alpha v_\theta = Bv'_\theta$. Lembramos que

$$v'_j = \sum_{i=1}^{2} m_{ij}\theta^{i-1}$$

com $(m_{ij})_{i,j=1}^2 = G^{-1}(V^t)^{-1}$, tal que V é a matriz de coordenadas de v_1, v_2 na base $\{1, \theta\}$ e $G = Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^{i-1}\theta^{j-1})))_{i,j=1}^2$.

Considerando $V = \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix}$, temos que $(1, \theta) \cdot \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix} = (v_1, v_2) = (1 - \theta, -2)$, de onde segue que $V = \begin{pmatrix} 1 & -2 \\ -1 & 0 \end{pmatrix}$. Logo $(V^t)^{-1} = \begin{pmatrix} 0 & -1/2 \\ -1 & -1/2 \end{pmatrix}$.
Além disso, temos

$$G = Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^{i-1}\theta^{j-1})))_{i,j=1}^2 = \begin{pmatrix} Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(1) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta) \\ Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^2) \end{pmatrix}.$$

Como θ é uma raiz de $\chi_A(x)$, e suas raízes são $-\sqrt{3}$ e $\sqrt{3}$, temos que os mergulhos reais de θ são dados por $\sigma_1(\theta) = -\sqrt{3}$ e $\sigma_2(\theta) = \sqrt{3}$. Então temos
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(1) = \sigma_1(1) + \sigma_2(1) = 2$,
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta) = \sigma_1(\theta) + \sigma_2(\theta) = 0$ e
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^2) = \sigma_1(\theta^2) + \sigma_2(\theta^2) = \sigma_1(\theta)^2 + \sigma_2(\theta)^2 = 6$.

Portanto

$$G = \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix},$$

com $d_{\mathbb{K}} = det(G) = 12$. Logo

$$G^{-1} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/6 \end{pmatrix}.$$

Com isso, temos

$$(m_{ij})_{i,j=1}^{2} = G^{-1}(V^t)^{-1} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/6 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1/2 \\ -1 & -1/2 \end{pmatrix} = \begin{pmatrix} 0 & -1/4 \\ -1/6 & -1/12 \end{pmatrix}.$$

Então

$$v_1' = \sum_{i=1}^{2} m_{i1}\theta^{i-1} = -\theta/6$$

e

$$v_2' = \sum_{i=1}^{2} m_{i2}\theta^{i-1} = -1/4 - \theta/12.$$

Portanto $v_\theta' = (-\theta/6, -1/4 - \theta/12)^t$. Por fim, o elemento α é dado por

$$\alpha \cdot \begin{pmatrix} 1-\theta \\ -2 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} -\theta/6 \\ -1/4 - \theta/12 \end{pmatrix}$$

cuja solução é $\alpha = 1/4$, pela segunda linha do sistema.

(4) No último passo, calculamos a matriz geradora do reticulado obtida pelo método.

Lembramos que a matriz é dada por

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(v_1) & \sqrt{\alpha_2}\sigma_2(v_1) \\ \sqrt{\alpha_1}\sigma_1(v_2) & \sqrt{\alpha_2}\sigma_2(v_2) \end{pmatrix}.$$

Temos
$\alpha_1 = \sigma_1(\alpha) = \sigma_1(1/4) = 1/4$,
$\alpha_2 = \sigma_2(\alpha) = \sigma_2(1/4) = 1/4$,
$\sigma_1(v_1) = \sigma_1(1-\theta) = \sigma_1(1) - \sigma_1(\theta) = 1 + \sqrt{3}$,
$\sigma_2(v_1) = \sigma_2(1-\theta) = \sigma_2(1) - \sigma_2(\theta) = 1 - \sqrt{3}$,
$\sigma_1(v_2) = \sigma_1(-2) = -2$ e
$\sigma_2(v_2) = \sigma_2(-2) = -2$.

Portanto a matriz geradora do reticulado A_2 é dada por

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

O reticulado construído é A_2 em uma versão rotacionada. Por fim, calculamos a distância produto mínima. Temos que $det(B) = 3$, $[\mathscr{O}_{\mathbb{K}} : \mathbb{Z}[\theta]] = 1$, $d_{\mathbb{K}} = 12$ e $h(\mathbb{K}) = 1 = min(\mathscr{I})$. Além disso, a norma mínima de A_2 é $\mu = 2$. Adotamos a distância produto mínima relativa, dada por

$$\sqrt{d_{p,rel}(A_2)} = \left(\frac{1}{\sqrt{det(B)}}\sqrt{\frac{det(B)}{d_{\mathbb{K}}}}\frac{min(\mathscr{I})}{[\mathscr{O}_{\mathbb{K}} : \mathbb{Z}[\theta]]}\right)^{1/2} = \left(\frac{1}{\sqrt{3}}\sqrt{\frac{3}{12}}\right)^{1/2} = 0.53728.$$

5.2 Reticulado D_3

Uma matriz geradora para o reticulado D_3 é dada por $M = \begin{pmatrix} -1 & -1 & -1 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$, cuja matriz de Gram associada é dada por $B = MM^t = \begin{pmatrix} 2 & 0 & -1 \\ 0 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix}$.

(1) A matriz A foi calculada segundo o algoritmo implementado no Wolfram Mathematica. As figura 5.5 e 5.6 representam o algoritmo para D_3 no software.

```
M = {{-1, -1, 0}, {1, -1, 0}, {0, 1, -1}};
M.Transpose[M] // MatrixForm
   transposição        forma de matriz
```

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

```
B = {{2, 0, -1}, {0, 2, -1}, {-1, -1, 2}};

A = {{a11, a12, a13}, {a21, a22, a23}, {a31, a32, a33}};

T = A.B

{{2 a11 - a13, 2 a12 - a13, -a11 - a12 + 2 a13}, {2 a21 - a23, 2 a22 - a23, -a21 - a22 + 2 a23},
 {2 a31 - a33, 2 a32 - a33, -a31 - a32 + 2 a33}}

S = B.Transpose[A]
      transposição

{{2 a11 - a13, 2 a21 - a23, 2 a31 - a33}, {2 a12 - a13, 2 a22 - a23, 2 a32 - a33},
 {-a11 - a12 + 2 a13, -a21 - a22 + 2 a23, -a31 - a32 + 2 a33}}
```

Figura 5.5: Algoritmo para calcular a matriz A.

Para matrizes A com entradas inteiras entre -2 e 2, utilizamos o algoritmo representado na figura 5.6.

```
m = {{a11, a12, a13}, {a21, a22, a23}, {a31, a32, a33}};
tt = CharacteristicPolynomial[m, x];
        polinômio característico
T = IrreduciblePolynomialQ[tt];
      polinômio irredutível?
If[T == True,
se      verdadeiro

 SS = Solve[tt == 0, x];
        resolve
 z = SS[[3]][[1]][[2]];
 dk = NumberFieldDiscriminant[z];
        discriminante de corpo numérico
 ib = NumberFieldIntegralBasis[z];
        base de inteiros de corpo numérico
 If[dk ≤ 316,
 se
  vet = {tt, dk, ib, m};
  Print[vet];];];];];];];];];];];];];];];];];];
  escreve
```

Figura 5.6: Algoritmo para determinar o discriminante e a base integral do corpo.

A figura 5.7 apresenta alguns dos resultados obtidos pela saídas do algoritmo, em que são representados respectivamente o polinômio característico, o discriminante do corpo, a base integral do corpo e a matriz A procurada.

```
{2 + 4 x - x^2 - x^3, 316, {1, AlgebraicNumber[Root[-2 - 4 #1 + #1^2 + #1^3 &, 2], {0, 1, 0}],
  AlgebraicNumber[Root[-2 - 4 #1 + #1^2 + #1^3 &, 2], {0, 0, 1}]}, {{-1, -1, -1}, {0, 2, 1}, {-1, -1, -2}}}
{1 + 5 x - x^2 - x^3, 148, {1, AlgebraicNumber[Root[-1 - 5 #1 + #1^2 + #1^3 &, 3], {0, 1, 0}],
  AlgebraicNumber[Root[-1 - 5 #1 + #1^2 + #1^3 &, 3], {1/2, 0, 1/2}]}, {{1, -1, -1}, {0, -2, 1}, {-1, 2, 0}}}
{2 + 4 x - x^2 - x^3, 316, {1, AlgebraicNumber[Root[-2 - 4 #1 + #1^2 + #1^3 &, 2], {0, 1, 0}],
  AlgebraicNumber[Root[-2 - 4 #1 + #1^2 + #1^3 &, 2], {0, 0, 1}]}, {{1, -1, -1}, {0, 0, 1}, {-2, 0, -2}}}
{-4 + 4 x + 2 x^2 - x^3, 148, {1, AlgebraicNumber[Root[4 - 4 #1 - 2 #1^2 + #1^3 &, 3], {0, 1, 0}],
  AlgebraicNumber[Root[4 - 4 #1 - 2 #1^2 + #1^3 &, 3], {0, 0, 1/2}]}, {{2, -1, -1}, {0, -1, 1}, {-1, 2, 1}}}
{-2 + 3 x + 2 x^2 - x^3, 316, {1, AlgebraicNumber[Root[2 - 3 #1 - 2 #1^2 + #1^3 &, 2], {0, 1, 0}],
  AlgebraicNumber[Root[2 - 3 #1 - 2 #1^2 + #1^3 &, 2], {0, 0, 1}]}, {{2, -1, -1}, {0, 1, 1}, {-2, 0, -1}}}
{2 - 4 x - 5 x^2 - x^3, 316, {1, AlgebraicNumber[Root[-2 + 4 #1 + 5 #1^2 + #1^3 &, 2], {0, 1, 0}],
  AlgebraicNumber[Root[-2 + 4 #1 + 5 #1^2 + #1^3 &, 2], {0, 0, 1}]}, {{-1, -1, 0}, {-2, -2, -2}, {0, -1, -2}}}
{2 + 4 x - x^2 - x^3, 316, {1, AlgebraicNumber[Root[-2 - 4 #1 + #1^2 + #1^3 &, 2], {0, 1, 0}],
  AlgebraicNumber[Root[-2 - 4 #1 + #1^2 + #1^3 &, 2], {0, 0, 1}]}, {{-1, -1, 0}, {-2, -2, -2}, {2, 1, 2}}}
{8 + 4 x - 3 x^2 - x^3, 316, {1, AlgebraicNumber[Root[-8 - 4 #1 + 3 #1^2 + #1^3 &, 1], {0, 1, 0}],
  AlgebraicNumber[Root[-8 - 4 #1 + 3 #1^2 + #1^3 &, 1], {0, 1/2, 1/2}]}, {{-1, -1, 0}, {-2, 0, -2}, {0, -2, -2}}}
```

Figura 5.7: Saídas (resultados) da rotina acima.

A melhor relação discriminante/base integral foi o corpo com $d_{\mathbb{K}} = 316$ e base integral canônica, ou seja, $[\mathscr{O}_{\mathbb{K}} : \mathbb{Z}[\theta]] = 1$. Corpos com discriminantes menores foram encontrados, mas cujas bases integrais continham componentes com denominadores maiores que 1 e, neste caso, $[\mathscr{O}_{\mathbb{K}} : \mathbb{Z}[\theta]] > 1$, fator que influencia mais em uma distância produto mínima menor. Uma das matrizes encontradas é dada abaixo, cujo polinômio característico é $\chi_A(x) = x^3 + x^2 - 4x - 2$. Através do software PARI, utilizando este polinômio, temos que $h(\mathbb{K}) = 1$.

Seja $\mathbb{K}$ o corpo de números dado pelo polinômio $x^3 + x^2 - 4x - 2$. A matriz

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

possui polinômio característico $\chi_A(x) = x^3 + x^2 - 4x - 2$, irredutível sobre $\mathbb{Q}$, e satisfaz a condição $B^{-1}AB = A^t$.

(2) O autovetor $v_\theta = (v_1, v_2, v_3)^t$ de A associado a θ tal que $\{v_1, v_2, v_3\}$ é uma $\mathbb{Z}$-base do ideal $\mathscr{I}$ tem componentes

$$v_j = (-1)^{i+j}\Delta_{ij}(A - \theta I_3),$$

cuja $\Delta_{ij}(A - \theta I_3)$ é a menor obtida fixando uma das linhas, digamos a i-ésima linha. Tomando $i = 1$, ou seja, fixando a primeira linha, temos que

$$\Delta_{11}(A - \theta I_3) = det \begin{pmatrix} 2-\theta & 1 \\ -1 & -2-\theta \end{pmatrix} = \theta^2 - 3$$

$$\Delta_{12}(A - \theta I_3) = det \begin{pmatrix} 0 & 1 \\ -1 & -2-\theta \end{pmatrix} = 1$$

$$\Delta_{13}(A - \theta I_3) = det \begin{pmatrix} 0 & 2-\theta \\ -1 & -1 \end{pmatrix} = 2 - \theta$$

Então

$$v_1 = (-1)^2\Delta_{11}(A-\theta I_3) = \theta^2 - 3,$$
$$v_2 = (-1)^3\Delta_{12}(A-\theta I_3) = -1,$$
$$v_3 = (-1)^4\Delta_{13}(A-\theta I_3) = 2-\theta.$$

Logo $v_\theta = (\theta^2-3,-1,2-\theta)^t$.

(3) Para determinar o elemento α, precisamos calcular o autovetor $v'_\theta = (v'_1, v'_2, v'_3)^t$ de A^t associado a θ. Suas componentes são dadas por

$$v'_j = \sum_{i=1}^{3} m_{ij}\theta^{i-1}$$

com $(m_{ij})_{i,j=1}^3 = G^{-1}(V^t)^{-1}$, na qual V é a matriz de coordenadas de v_1, v_2, v_3 na base $\{1, \theta, \theta^2\}$ e $G = Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^{i-1}\theta^{j-1})))_{i,j=1}^3$.

Considerando $V = \begin{pmatrix} v_{11} & v_{12} & v_{13} \\ v_{21} & v_{22} & v_{23} \\ v_{31} & v_{32} & v_{33} \end{pmatrix}$, temos que $(1,\theta,\theta^2)\cdot\begin{pmatrix} v_{11} & v_{12} & v_{13} \\ v_{21} & v_{22} & v_{23} \\ v_{31} & v_{32} & v_{33} \end{pmatrix} = (v_1, v_2, v_3) =$ $(\theta^2-3,-1,2-\theta)$, de onde segue que $V = \begin{pmatrix} -3 & -1 & 2 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}$. Logo $(V^t)^{-1} = \begin{pmatrix} 0 & -1 & 0 \\ 0 & -2 & -1 \\ 1 & -3 & 0 \end{pmatrix}$.

Além disso, temos

$$G = Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^{i-1}\theta^{j-1})))_{i,j=1}^3 = \begin{pmatrix} Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(1) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^2) \\ Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^2) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^3) \\ Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^2) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^3) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^4) \end{pmatrix}.$$

Como θ é uma raiz de $\chi_A(x)$, e o conjunto de suas raízes é $\{-0.47068, -2.34292, 1.81361\}$, temos que os mergulhos reais de θ são dados por $\sigma_1(\theta) = -0,47068$, $\sigma_2(\theta) = -2,34292$ e $\sigma_3(\theta) = 1,81361$. Então temos
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(1) = \sigma_1(1) + \sigma_2(1) + \sigma_3(1) = 3,$
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta) = \sigma_1(\theta) + \sigma_2(\theta) + \sigma_3(\theta) = -1,$
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^2) = \sigma_1(\theta^2) + \sigma_2(\theta^2) + \sigma_3(\theta^2) = \sigma_1(\theta)^2 + \sigma_2(\theta)^2 + \sigma_3(\theta)^2 = 9,$
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^3) = \sigma_1(\theta^3) + \sigma_2(\theta^3) + \sigma_3(\theta^3) = \sigma_1(\theta)^3 + \sigma_2(\theta)^3 + \sigma_3(\theta)^3 = -7,$
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^4) = \sigma_1(\theta^4) + \sigma_2(\theta^4) + \sigma_3(\theta^4) = \sigma_1(\theta)^4 + \sigma_2(\theta)^4 + \sigma_3(\theta)^4 = 41.$

Portanto

$$G = \begin{pmatrix} 3 & -1 & 9 \\ -1 & 9 & -7 \\ 9 & -7 & 41 \end{pmatrix},$$

com $d_{\mathbb{K}} = det(G) = 316$. Logo

$$G^{-1} = \begin{pmatrix} \frac{80}{79} & \frac{-11}{158} & \frac{-37}{158} \\ \frac{-11}{158} & \frac{21}{158} & \frac{3}{79} \\ \frac{-37}{158} & \frac{3}{79} & \frac{13}{158} \end{pmatrix}.$$

Com isso, temos

$$(m_{ij})_{i,j=1}^3 = G^{-1}(V^t)^{-1} =$$

$$\begin{pmatrix} \frac{80}{79} & \frac{-11}{158} & \frac{-37}{158} \\ \frac{-11}{158} & \frac{21}{158} & \frac{3}{79} \\ \frac{-37}{158} & \frac{3}{79} & \frac{13}{158} \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 & 0 \\ 0 & -2 & -1 \\ 1 & -3 & 0 \end{pmatrix} = \begin{pmatrix} \frac{-37}{158} & \frac{-27}{158} & \frac{11}{158} \\ \frac{3}{79} & \frac{-49}{158} & \frac{-21}{158} \\ \frac{13}{158} & \frac{-7}{79} & \frac{-3}{79} \end{pmatrix}.$$

Então

$$v'_1 = \sum_{i=1}^{3} m_{i1}\theta^{i-1} = \frac{-37}{158} + \frac{3}{79}\theta + \frac{13}{158}\theta^2,$$

$$v'_2 = \sum_{i=1}^{3} m_{i2}\theta^{i-1} = \frac{-27}{158} - \frac{49}{158}\theta - \frac{7}{79}\theta^2,$$

e

$$v'_3 = \sum_{i=1}^{3} m_{i3}\theta^{i-1} = \frac{11}{158} - \frac{21}{158}\theta - \frac{3}{79}\theta^2.$$

Portanto

$$v'_\theta = (\frac{-37}{158} + \frac{3}{79}\theta + \frac{13}{158}\theta^2, \frac{-27}{158} - \frac{49}{158}\theta - \frac{7}{79}\theta^2, \frac{11}{158} - \frac{21}{158}\theta - \frac{3}{79}\theta^2)^t$$

Por fim, o elemento α é dado por $\alpha v_\theta = Bv'_\theta$, ou seja,

$$\alpha \cdot \begin{pmatrix} \theta^2 - 3 \\ -1 \\ 2 - \theta \end{pmatrix} = \begin{pmatrix} 2 & 0 & -1 \\ 0 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} \frac{-37}{158} + \frac{3}{79}\theta + \frac{13}{158}\theta^2 \\ \frac{-27}{158} - \frac{49}{158}\theta - \frac{7}{79}\theta^2 \\ \frac{11}{158} - \frac{21}{158}\theta - \frac{3}{79}\theta^2 \end{pmatrix}.$$

Pela segunda linha do sistema, temos $\alpha = \frac{65+77\theta+11\theta^2}{158}$.

(4) A matriz geradora do reticulado obtida é dada por

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(v_1) & \sqrt{\alpha_2}\sigma_2(v_1) & \sqrt{\alpha_3}\sigma_3(v_1) \\ \sqrt{\alpha_1}\sigma_1(v_2) & \sqrt{\alpha_2}\sigma_2(v_2) & \sqrt{\alpha_3}\sigma_3(v_2) \\ \sqrt{\alpha_1}\sigma_1(v_3) & \sqrt{\alpha_2}\sigma_2(v_3) & \sqrt{\alpha_3}\sigma_3(v_3) \end{pmatrix}.$$

Temos
$\alpha_1 = \sigma_1(\alpha) = \sigma_1(\frac{65+77\theta+11\theta^2}{158}) = \frac{65}{158} + \frac{77}{158}\sigma_1(\theta) + \frac{11}{158}\sigma_1(\theta)^2 = 0,21285,$
$\alpha_2 = \sigma_2(\alpha) = \sigma_2(\frac{65+77\theta+11\theta^2}{158}) = \frac{65}{158} + \frac{77}{158}\sigma_2(\theta) + \frac{11}{158}\sigma_2(\theta)^2 = 0,03391,$
$\alpha_3 = \sigma_3(\alpha) = \sigma_3(\frac{65+77\theta+11\theta^2}{158}) = \frac{65}{158} + \frac{77}{158}\sigma_3(\theta) + \frac{11}{158}\sigma_3(\theta)^2 = 1,75322,$
$\sigma_1(v_1) = \sigma_1(\theta^2 - 3) = \sigma_1(\theta)^2 - \sigma_1(3) = -2,77846,$
$\sigma_2(v_1) = \sigma_2(\theta^2 - 3) = \sigma_2(\theta)^2 - \sigma_2(3) = 2,48929,$
$\sigma_3(v_1) = \sigma_3(\theta^2 - 3) = \sigma_3(\theta)^2 - \sigma_3(3) = 0,28916,$
$\sigma_1(v_2) = \sigma_2(v_2) = \sigma_3(v_2) = -1$
$\sigma_1(v_3) = \sigma_1(2 - \theta) = \sigma_1(2) - \sigma_1(\theta) = 2,47068,$
$\sigma_2(v_3) = \sigma_2(2 - \theta) = \sigma_2(2) - \sigma_2(\theta) = 4,34292,$
$\sigma_3(v_3) = \sigma_3(2 - \theta) = \sigma_3(2) - \sigma_3(\theta) = 0,18639.$

Portanto a matriz geradora do reticulado A_2 é dada por

$$M = \begin{pmatrix} -1,28188 & 0,45845 & 0,38288 \\ -0,46136 & -0,18417 & -1,32409 \\ 1,13988 & 0,79984 & 0,24680 \end{pmatrix}.$$

Para finalizar, calculamos a distância produto mínima. Temos que $det(B) = 4$, $[\mathscr{O}_{\mathbb{K}} : \mathbb{Z}[\theta]] = 1$, $d_{\mathbb{K}} = 316$ e $h(\mathbb{K}) = 1 = min(\mathscr{I})$. A distância produto mínima relativa é dada

$$\sqrt[3]{d_{p,rel}(D_3)} = (\frac{1}{\sqrt{det(B)}}\sqrt{\frac{det(B)}{d_{\mathbb{K}}}}\frac{min(\mathscr{I})}{[\mathscr{O}_{\mathbb{K}} : \mathbb{Z}[\theta]]})^{1/3} = (\frac{1}{\sqrt{4}}\sqrt{\frac{4}{316}})^{1/3} = 0.38316.$$

5.3 Reticulado D_4

Uma matriz geradora para o reticulado D_4 é dada por $M = \begin{pmatrix} -1 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}$, cuja matriz de Gram associada é dada por $B = MM^t = \begin{pmatrix} 2 & 0 & -1 & 0 \\ 0 & 2 & -1 & 0 \\ -1 & -1 & 2 & 1 \\ 0 & 0 & -1 & 2 \end{pmatrix}$.

(1) Através do Mathematica, computamos a matriz A e calculamos a base integral e discriminante do corpo. As figuras 5.8 e 5.9 representam o algoritmo no software.

```
M = {{-1, -1, 0, 0}, {1, -1, 0, 0}, {0, 1, -1, 0}, {0, 0, 1, -1}};
M.Transpose[M] // MatrixForm
   transposição      forma de matriz
```

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

```
B = {{2, 0, -1, 0}, {0, 2, -1, 0}, {-1, -1, 2, -1}, {0, 0, -1, 2}};
A = {{a11, a12, a13, a14}, {a21, a22, a23, a24}, {a31, a32, a33, a34}, {a41, a42, a43, a44}};
T = A.B
```

```
{{2 a11 - a13, 2 a12 - a13, -a11 - a12 + 2 a13 - a14, -a13 + 2 a14}, {2 a21 - a23, 2 a22 - a23, -a21 - a22 + 2 a23 - a24, -a23 + 2 a24},
 {2 a31 - a33, 2 a32 - a33, -a31 - a32 + 2 a33 - a34, -a33 + 2 a34}, {2 a41 - a43, 2 a42 - a43, -a41 - a42 + 2 a43 - a44, -a43 + 2 a44}}
```

```
S = B. Transpose[A]
      transposição
```

```
{{2 a11 - a13, 2 a21 - a23, 2 a31 - a33, 2 a41 - a43}, {2 a12 - a13, 2 a22 - a23, 2 a32 - a33, 2 a42 - a43},
 {-a11 - a12 + 2 a13 - a14, -a21 - a22 + 2 a23 - a24, -a31 - a32 + 2 a33 - a34, -a41 - a42 + 2 a43 - a44},
 {-a13 + 2 a14, -a23 + 2 a24, -a33 + 2 a34, -a43 + 2 a44}}
```

Figura 5.8: Algoritmo para calcular a matriz A.

Para matrizes A com entradas inteiras entre -2 e 2, utilizamos o algoritmo representado na figura 5.9.

```
m = {{a11, a12, a13, a14}, {a21, a22, a23, a24}, {a31, a32, a33, a34},
   {a41, a42, a43, a44}};
tt = CharacteristicPolynomial[m, x];
     |polinômio característico
T = IrreduciblePolynomialQ[tt];
    |polinômio irredutível?
If[T == True,
|se      |verdadeiro

 SS = Solve[tt == 0, x];
      |resolve
 z = SS[[4]][[1]][[2]];
 dk = NumberFieldDiscriminant[z];
      |discriminante de corpo numérico
 ib = NumberFieldIntegralBasis[z];
      |base de inteiros de corpo numérico
 If[dk ≤ 2048,
 |se
  vet = {tt, dk, ib, m};
  Print[vet];
  |escreve
```

Figura 5.9: Algoritmo para determinar o discriminante e a base integral do corpo.

A figura 5.10 apresenta alguns dos resultados obtidos pela saídas do algoritmo, em que são representados respectivamente o polinômio característico, o discriminante do corpo, a base integral do corpo e a matriz A procurada.

```
{-4 - 16 x - 4 x^2 + 4 x^3 + x^4, 2000,
 {1, AlgebraicNumber[Root[-4 - 16 #1 - 4 #1^2 + 4 #1^3 + #1^4 &, 4], {0, 1, 0, 0}], AlgebraicNumber[Root[-4 - 16 #1 - 4 #1^2 + 4 #1^3 + #1^4 &, 4], {1/2, 1/2, 1/4, 0}],
  AlgebraicNumber[Root[-4 - 16 #1 - 4 #1^2 + 4 #1^3 + #1^4 &, 4], {0, 1/2, 0, 1/4}]}, {{-2, 0, 1, -2}, {0, -1, 1, 1}, {2, 0, -2, 0}, {-2, 1, 1, 1}}}
{-2 + 8 x - 8 x^2 + x^4, 2048, {1, AlgebraicNumber[Root[-2 + 8 #1 - 8 #1^2 + #1^4 &, 2], {0, 1, 0, 0}], AlgebraicNumber[Root[-2 + 8 #1 - 8 #1^2 + #1^4 &, 2], {0, 0, 1, 0}],
  AlgebraicNumber[Root[-2 + 8 #1 - 8 #1^2 + #1^4 &, 2], {0, 0, 0, 1}]}, {{-2, 0, 1, -1}, {0, 2, 1, 1}, {2, -1, -1, 0}, {-1, 1, 1, 1}}}
{2 + 16 x + 20 x^2 + 8 x^3 + x^4, 2048,
 {1, AlgebraicNumber[Root[2 + 16 #1 + 20 #1^2 + 8 #1^3 + #1^4 &, 4], {0, 1, 0, 0}], AlgebraicNumber[Root[2 + 16 #1 + 20 #1^2 + 8 #1^3 + #1^4 &, 4], {0, 0, 1, 0}],
  AlgebraicNumber[Root[2 + 16 #1 + 20 #1^2 + 8 #1^3 + #1^4 &, 4], {0, 0, 0, 1}]}, {{-2, 0, 1, 0}, {0, -2, 1, 2}, {1, 0, -2, -1}, {-1, 1, -1, -2}}}
{-17 - 20 x - 2 x^2 + 4 x^3 + x^4, 2048,
 {1, AlgebraicNumber[Root[-17 - 20 #1 - 2 #1^2 + 4 #1^3 + #1^4 &, 4], {0, 1, 0, 0}], AlgebraicNumber[Root[-17 - 20 #1 - 2 #1^2 + 4 #1^3 + #1^4 &, 4], {0, 0, 1, 0}],
  AlgebraicNumber[Root[-17 - 20 #1 - 2 #1^2 + 4 #1^3 + #1^4 &, 4], {0, 0, 0, 1}]}, {{-2, 0, 1, 0}, {0, -1, 1, -1}, {1, 1, -2, -1}, {-1, -2, -1, 1}}}
{-1 - 8 x + 4 x^3 + x^4, 1600, {1, AlgebraicNumber[Root[-1 - 8 #1 + 4 #1^3 + #1^4 &, 4], {0, 1, 0, 0}], AlgebraicNumber[Root[-1 - 8 #1 + 4 #1^3 + #1^4 &, 4], {1/2, 0, 1/2, 0}],
  AlgebraicNumber[Root[-1 - 8 #1 + 4 #1^3 + #1^4 &, 4], {1/2, 1/2, 1/2, 1/2}]}, {{-2, 0, 1, 0}, {0, -1, 1, -1}, {2, 2, 0, 1}, {-1, -2, -1, -1}}}
{-1 - 4 x + 2 x^2 + 4 x^3 + x^4, 2048,
 {1, AlgebraicNumber[Root[-1 - 4 #1 + 2 #1^2 + 4 #1^3 + #1^4 &, 4], {0, 1, 0, 0}], AlgebraicNumber[Root[-1 - 4 #1 + 2 #1^2 + 4 #1^3 + #1^4 &, 4], {0, 0, 1, 0}],
  AlgebraicNumber[Root[-1 - 4 #1 + 2 #1^2 + 4 #1^3 + #1^4 &, 4], {0, 0, 0, 1}]}, {{-2, 0, 1, 0}, {0, -1, 1, 1}, {2, 1, 0, 0}, {-1, 0, -1, -1}}}
```

Figura 5.10: Saídas (resultados) da rotina acima.

O corpo com menor discriminante cuja base integral é canônica possui $d_{\mathbb{K}} = 2048$. Através do PARI, pelo polinômio característico da matriz A encontrada, $\chi_A(x) = x^4 - 8x^2 + 8x - 2$, temos $h(\mathbb{K}) = 1$.

Seja $\mathbb{K}$ o corpo de números dado pelo polinômio x^4-8x^2+8x-2. A matriz

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

possui polinômio característico $\chi_A(x)=x^4-8x^2+8x-2$, irredutível sobre $\mathbb{Q}$, e satisfaz a condição $B^{-1}AB=A^t$.

(2) O autovetor $v_\theta=(v_1,v_2,v_3,v_4)^t$ de A associado a θ tal que $\{v_1,v_2,v_3,v_4\}$ é uma $\mathbb{Z}$-base do ideal $\mathscr{I}$ tem componentes

$$v_j=(-1)^{i+j}\Delta_{ij}(A-\theta I_4),$$

na qual $\Delta_{ij}(A-\theta I_4)$ é a menor obtida fixando uma das linhas, digamos a i-ésima linha. Tomando $i=1$, ou seja, fixando a primeira linha, temos que

$$\Delta_{11}(A-\theta I_4)=det\begin{pmatrix}1-\theta & -1 & 0\\ -1 & 1-\theta & -1\\ 0 & -1 & -\theta\end{pmatrix}=-\theta^3+2\theta^2+\theta-1$$
$$\Delta_{12}(A-\theta I_4)=det\begin{pmatrix}0 & -1 & 0\\ 1 & 1-\theta & -1\\ 1 & -1 & -\theta\end{pmatrix}=1-\theta$$
$$\Delta_{13}(A-\theta I_4)=det\begin{pmatrix}0 & 1-\theta & 0\\ 1 & -1 & -1\\ 1 & 0 & -\theta\end{pmatrix}=-\theta^2+2\theta-1$$
$$\Delta_{14}(A-\theta I_4)=det\begin{pmatrix}0 & 1-\theta & -1\\ 1 & -1 & 1-\theta\\ 1 & 0 & -1\end{pmatrix}=\theta^2-3\theta+1$$

Então

$$v_1=(-1)^2\Delta_{11}(A-\theta I_4)=-\theta^3+2\theta^2+\theta-1,$$
$$v_2=(-1)^3\Delta_{12}(A-\theta I_4)=\theta-1,$$
$$v_3=(-1)^4\Delta_{13}(A-\theta I_4)=-\theta^2+2\theta-1,$$
$$v_4=(-1)^5\Delta_{14}(A-\theta I_4)=-\theta^2+3\theta-1.$$

Logo $v_\theta=(-\theta^3+2\theta^2+\theta-1,\theta-1,-\theta^2+2\theta-1,-\theta^2+3\theta-1)^t$.

(3) Para determinar o elemento α, precisamos calcular o autovetor $v'_\theta=(v'_1,v'_2,v'_3,v'_4)^t$ de A^t associado a θ. Suas componentes são dadas por

$$v'_j=\sum_{i=1}^{4}m_{ij}\theta^{i-1}$$

com $(m_{ij})_{i,j=1}^4=G^{-1}(V^t)^{-1}$, tal que V é a matriz de coordenadas de v_1,v_2,v_3,v_4 na base $\{1,\theta,\theta^2,\theta^3\}$ e $G=Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^{i-1}\theta^{j-1})))_{i,j=1}^4$.

Considerando $V = \begin{pmatrix} v_{11} & v_{12} & v_{13} & v_{14} \\ v_{21} & v_{22} & v_{23} & v_{24} \\ v_{31} & v_{32} & v_{33} & v_{34} \\ v_{41} & v_{42} & v_{43} & v_{44} \end{pmatrix}$, temos que $(1,\theta,\theta^2,\theta^3)\cdot \begin{pmatrix} v_{11} & v_{12} & v_{13} & v_{14} \\ v_{21} & v_{22} & v_{23} & v_{24} \\ v_{31} & v_{32} & v_{33} & v_{34} \\ v_{41} & v_{42} & v_{43} & v_{44} \end{pmatrix} =$
$(v_1,v_2,v_3,v_4) = (-\theta^3+2\theta^2+\theta-1, \theta-1, -\theta^2+2\theta-1, -\theta^2+3\theta-1)$ implica em

$$V = \begin{pmatrix} -1 & -1 & -1 & -1 \\ 1 & 1 & 2 & 3 \\ 2 & 0 & -1 & -1 \\ -1 & 0 & 0 & 0 \end{pmatrix}.$$

Portanto

$$(V^t)^{-1} = \begin{pmatrix} 0 & -1 & -1 & 1 \\ 0 & 0 & -1 & 1 \\ 0 & 1 & -2 & 1 \\ -1 & 3 & -4 & 2 \end{pmatrix}.$$

Por outro lado, temos

$$G = Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^{i-1}\theta^{j-1})))_{i,j=1}^4 = \begin{pmatrix} Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(1) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^2) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^3) \\ Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^2) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^3) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^4) \\ Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^2) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^3) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^4) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^5) \\ Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^3) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^4) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^5) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^6) \end{pmatrix}.$$

Como θ é uma raiz de $\chi_A(x)$, e o conjunto de suas raízes é dado por $\{\sqrt{2}-\sqrt{2-\sqrt{2}}, \sqrt{2}+\sqrt{2-\sqrt{2}}, -\sqrt{2}-\sqrt{2+\sqrt{2}}, -\sqrt{2}+\sqrt{2+\sqrt{2}}\}$, temos que os mergulhos reais de θ são dados por $\sigma_1(\theta) = \sqrt{2}-\sqrt{2-\sqrt{2}}$, $\sigma_2(\theta) = \sqrt{2}+\sqrt{2-\sqrt{2}}$, $\sigma_3(\theta) = -\sqrt{2}-\sqrt{2+\sqrt{2}}$ e $\sigma_4(\theta) = -\sqrt{2}+\sqrt{2+\sqrt{2}}$. Então temos

$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(1) = \sigma_1(1)+\sigma_2(1)+\sigma_3(1)+\sigma_4(1) = 4,$
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta) = \sigma_1(\theta)+\sigma_2(\theta)+\sigma_3(\theta)+\sigma_4(\theta) = 0,$
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^2) = \sigma_1(\theta)^2+\sigma_2(\theta)^2+\sigma_3(\theta)^2+\sigma_4(\theta)^2 = 16,$
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^3) = \sigma_1(\theta)^3+\sigma_2(\theta)^3+\sigma_3(\theta)^3+\sigma_4(\theta)^3 = -24,$
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^4) = \sigma_1(\theta)^4+\sigma_2(\theta)^4+\sigma_3(\theta)^4+\sigma_4(\theta)^4 = 136,$
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^5) = \sigma_1(\theta)^5+\sigma_2(\theta)^5+\sigma_3(\theta)^5+\sigma_4(\theta)^5 = -320,$
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^6) = \sigma_1(\theta)^6+\sigma_2(\theta)^6+\sigma_3(\theta)^6+\sigma_4(\theta)^6 = 1312.$

Portanto

$$G = \begin{pmatrix} 4 & 0 & 16 & -24 \\ 0 & 16 & -24 & 136 \\ 16 & -24 & 136 & -320 \\ -24 & 136 & -320 & 1312 \end{pmatrix},$$

com $d_{\mathbb{K}} = det(G) = 2048$. Logo

$$G^{-1} = \begin{pmatrix} \frac{67}{4} & \frac{-131}{4} & \frac{9}{4} & \frac{17}{4} \\ \frac{-131}{4} & \frac{265}{4} & \frac{-19}{4} & \frac{-69}{8} \\ \frac{9}{4} & \frac{-19}{4} & \frac{3}{8} & \frac{5}{8} \\ \frac{17}{4} & \frac{-69}{8} & \frac{5}{8} & \frac{9}{8} \end{pmatrix}.$$

Com isso, temos

$$(m_{ij})_{i,j=1}^{4} = G^{-1}(V^t)^{-1} =$$

$$\begin{pmatrix} \frac{67}{4} & \frac{-131}{4} & \frac{9}{4} & \frac{17}{4} \\ \frac{-131}{4} & \frac{265}{4} & \frac{-19}{4} & \frac{-69}{8} \\ \frac{9}{4} & \frac{-19}{4} & \frac{3}{8} & \frac{5}{8} \\ \frac{17}{4} & \frac{-69}{8} & \frac{5}{8} & \frac{9}{8} \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 & -1 & 1 \\ 0 & 0 & -1 & 1 \\ 0 & 1 & -2 & 1 \\ -1 & 3 & -4 & 2 \end{pmatrix} = \begin{pmatrix} \frac{-17}{4} & \frac{-7}{4} & \frac{11}{2} & \frac{-21}{4} \\ \frac{69}{8} & \frac{17}{8} & \frac{21}{2} & \frac{23}{2} \\ \frac{-5}{8} & 0 & \frac{-3}{4} & \frac{-7}{8} \\ \frac{-9}{8} & \frac{-1}{4} & \frac{-11}{8} & \frac{-3}{2} \end{pmatrix}.$$

Então

$$v_1' = \sum_{i=1}^{4} m_{i1}\theta^{i-1} = \frac{-17}{4} + \frac{69}{8}\theta - \frac{5}{8}\theta^2 - \frac{9}{8}\theta^3,$$

$$v_2' = \sum_{i=1}^{4} m_{i2}\theta^{i-1} = \frac{-7}{4} + \frac{17}{8}\theta - \frac{1}{4}\theta^3,$$

$$v_3' = \sum_{i=1}^{4} m_{i3}\theta^{i-1} = \frac{-11}{2} + \frac{21}{2}\theta - \frac{-3}{4}\theta^2 - \frac{11}{8}\theta^3,$$

$$v_4' = \sum_{i=1}^{4} m_{i4}\theta^{i-1} = \frac{-21}{4} + \frac{23}{2}\theta - \frac{-7}{8}\theta^2 - \frac{3}{2}\theta^3,$$

Portanto $v'_\theta = (\frac{-17}{4} + \frac{69}{8}\theta - \frac{5}{8}\theta^2 - \frac{9}{8}\theta^3, \frac{-7}{4} + \frac{17}{8}\theta - \frac{1}{4}\theta^3, \frac{-11}{2} + \frac{21}{2}\theta - \frac{-3}{4}\theta^2 - \frac{11}{8}\theta^3, \frac{-21}{4} + \frac{23}{2}\theta - \frac{-7}{8}\theta^2 - \frac{3}{2}\theta^3)^t$.

Por fim, o elemento α é dado por $\alpha v_\theta = Bv'_\theta$, ou seja,

$$\alpha \cdot \begin{pmatrix} -\theta^3 + 2\theta^2 + \theta - 1 \\ \theta - 1 \\ -\theta^2 + 2\theta - 1 \\ -\theta^2 + 3\theta - 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 & -1 & 0 \\ 0 & 2 & -1 & 0 \\ -1 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} \frac{-17}{4} + \frac{69}{8}\theta - \frac{5}{8}\theta^2 - \frac{9}{8}\theta^3 \\ \frac{-7}{4} + \frac{17}{8}\theta - \frac{1}{4}\theta^3 \\ \frac{-11}{2} + \frac{21}{2}\theta - \frac{-3}{4}\theta^2 - \frac{11}{8}\theta^3 \\ \frac{-21}{4} + \frac{23}{2}\theta - \frac{-7}{8}\theta^2 - \frac{3}{2}\theta^3 \end{pmatrix}.$$

Pela segunda linha do sistema, temos $\alpha = \frac{-29}{4} + 20\theta - \frac{7}{4}\theta^2 - \frac{21}{8}\theta^3$.

(4) A matriz geradora do reticulado é dada por

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(v_1) & \sqrt{\alpha_2}\sigma_2(v_1) & \sqrt{\alpha_3}\sigma_3(v_1) & \sqrt{\alpha_4}\sigma_4(v_1) \\ \sqrt{\alpha_1}\sigma_1(v_2) & \sqrt{\alpha_2}\sigma_2(v_2) & \sqrt{\alpha_3}\sigma_3(v_2) & \sqrt{\alpha_4}\sigma_4(v_2) \\ \sqrt{\alpha_1}\sigma_1(v_3) & \sqrt{\alpha_2}\sigma_2(v_3) & \sqrt{\alpha_3}\sigma_3(v_3) & \sqrt{\alpha_4}\sigma_4(v_3) \\ \sqrt{\alpha_1}\sigma_1(v_4) & \sqrt{\alpha_2}\sigma_2(v_4) & \sqrt{\alpha_3}\sigma_3(v_4) & \sqrt{\alpha_4}\sigma_4(v_4) \end{pmatrix}.$$

Temos

$\alpha_1 = \sigma_1(\alpha) = \sigma_1(\frac{-29}{4} + 20\theta - \frac{7}{4}\theta^2 - \frac{21}{8}\theta^3) = -\frac{29}{4} + 20\sigma_1(\theta) - \frac{7}{4}\sigma_1(\theta)^2 - \frac{21}{8}\sigma_1(\theta)^3 = 4,27312,$
$\alpha_2 = \sigma_2(\alpha) = \sigma_2(\frac{-29}{4} + 20\theta - \frac{7}{4}\theta^2 - \frac{21}{8}\theta^3) = -\frac{29}{4} + 20\sigma_2(\theta) - \frac{7}{4}\sigma_2(\theta)^2 - \frac{21}{8}\sigma_2(\theta)^3 = 0,84820,$
$\alpha_3 = \sigma_3(\alpha) = \sigma_3(\frac{-29}{4} + 20\theta - \frac{7}{4}\theta^2 - \frac{21}{8}\theta^3) = -\frac{29}{4} + 20\sigma_3(\theta) - \frac{7}{4}\sigma_3(\theta)^2 - \frac{21}{8}\sigma_3(\theta)^3 = 0,00061,$
$\alpha_4 = \sigma_4(\alpha) = \sigma_4(\frac{-29}{4} + 20\theta - \frac{7}{4}\theta^2 - \frac{21}{8}\theta^3) = -\frac{29}{4} + 20\sigma_4(\theta) - \frac{7}{4}\sigma_4(\theta)^2 - \frac{21}{8}\sigma_4(\theta)^3 = 0,87806,$
$\sigma_1(v_1) = 0,21768$, $\sigma_2(v_1) = 0,32647$, $\sigma_3(v_1) = 51,72790$ e $\sigma_4(v_1) = -0,27202$,
$\sigma_1(v_2) = -0,35115$, $\sigma_2(v_2) = 1,17958$, $\sigma_3(v_2) = -4,26197$ e $\sigma_4(v_2) = -0,56645$,
$\sigma_1(v_3) = -0,12330$, $\sigma_2(v_3) = -1,39141$, $\sigma_3(v_3) = -18,16440$ e $\sigma_4(v_3) = -0,32087$
$\sigma_1(v_4) = 0,52533$, $\sigma_2(v_4) = 0,78817$, $\sigma_3(v_4) = -21,42640$ e $\sigma_4(v_4) = 0,11267$.

Portanto a matriz geradora do reticulado A_2 é dada por

$$M = \begin{pmatrix} 0,44998 & 0,30067 & 1,28146 & -0,25489 \\ -0,72588 & 1,08637 & -0,10558 & -0,53079 \\ -0,25489 & -1,28146 & -0,44998 & -0,30067 \\ 1,08637 & 0,72588 & -0,53079 & 0,10558 \end{pmatrix}.$$

Calculando a distância produto mínima relativa, temos $det(B) = 4$, $[\mathscr{O}_{\mathbb{K}} : \mathbb{Z}[\theta]] = 1$, $d_{\mathbb{K}} = 2048$ e $h(\mathbb{K}) = 1 = min(\mathscr{I})$.

Então

$$\sqrt[4]{d_{p,rel}(D_4)} = (\frac{1}{\sqrt{det(B)}}\sqrt{\frac{det(B)}{d_{\mathbb{K}}}}\frac{min(\mathscr{I})}{[\mathscr{O}_{\mathbb{K}} : \mathbb{Z}[\theta]]})^{1/4} = (\frac{1}{\sqrt{4}}\sqrt{\frac{4}{2048}})^{1/4} = 0.38555.$$

5.4 Reticulado D_5

Uma matriz geradora para o reticulado D_5 é dada por

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

cuja matriz de Gram associada é dada por

$$B = MM^t = \begin{pmatrix} 2 & 0 & -1 & 0 & 0 \\ 0 & 2 & -1 & 0 & 0 \\ -1 & -1 & 2 & -1 & 0 \\ 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & -1 & 2 \end{pmatrix}.$$

(1) Através do Mathematica, computamos a matriz A e calculamos a base integral e discriminante do corpo.

O corpo com menor discriminante encontrado cuja base integral é canônica possui $d_{\mathbb{K}} = 246832$. Através do PARI/GP, pelo polinômio característico da matriz A encontrada, $\chi_A(x) = x^5 - 4x^4 - 3x^3 + 12x^2 + 3x - 8$, temos $h(\mathbb{K}) = 1$.

Seja $\mathbb{K}$ o corpo de números dado pelo polinômio $x^5 - 4x^4 - 3x^3 + 12x^2 + 3x - 8$. A matriz

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

possui polinômio característico $\chi_A(x) = x^5 - 4x^4 - 3x^3 + 12x^2 + 3x - 8$, irredutível sobre $\mathbb{Q}$, e satisfaz a condição $B^{-1}AB = A^t$.

(2) O autovetor $v_\theta = (v_1, v_2, v_3, v_4, v_5)^t$ de A associado a θ tal que $\{v_1, v_2, v_3, v_4, v_5\}$ é uma $\mathbb{Z}$-base do ideal $\mathscr{I}$ tem componentes

$$v_j = (-1)^{i+j}\Delta_{ij}(A - \theta I_5),$$

na qual $\Delta_{ij}(A-\theta I_5)$ é a menor obtida fixando uma das linhas, digamos a i-ésima linha.

Tomando $i = 1$, ou seja, fixando a primeira linha, temos que

$$\Delta_{11}(A-\theta I_5) = det\begin{pmatrix} -1-\theta & -3 & 0 & 0 \\ 0 & 4-\theta & 0 & 1 \\ 1 & -1 & 2-\theta & 0 \\ 0 & 0 & -1 & -\theta \end{pmatrix} = \theta^4 - 5\theta^3 + 2\theta^2 + 7\theta - 4$$

$$\Delta_{12}(A-\theta I_5) = det\begin{pmatrix} -1 & -3 & 0 & 0 \\ 1 & 4-\theta & 0 & 1 \\ 0 & -1 & 2-\theta & 0 \\ -1 & 0 & -1 & -\theta \end{pmatrix} = \theta^3 - 3\theta^2 - \theta + 5$$

$$\Delta_{13}(A-\theta I_5) = det\begin{pmatrix} -1 & -1-\theta & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 2-\theta & 0 \\ -1 & 0 & -1 & -\theta \end{pmatrix} = \theta^3 - 2\theta^2 - \theta + 3$$

$$\Delta_{14}(A-\theta I_5) = det\begin{pmatrix} -1 & -1-\theta & -3 & 0 \\ 1 & 0 & 4-\theta & 1 \\ 0 & 1 & -1 & 0 \\ -1 & 0 & 0 & -\theta \end{pmatrix} = 2\theta^2 - \theta - 4$$

$$\Delta_{15}(A-\theta I_5) = det\begin{pmatrix} -1 & -1-\theta & -3 & 0 \\ 1 & 0 & 4-\theta & 0 \\ 0 & 1 & -1 & 2-\theta \\ -1 & 0 & 0 & -1 \end{pmatrix} = -\theta^3 + 5\theta^2 - 8$$

Então

$$\begin{aligned} v_1 &= (-1)^2\Delta_{11}(A-\theta I_5) = \theta^4 - 5\theta^3 + 2\theta^2 + 7\theta - 4, \\ v_2 &= (-1)^3\Delta_{12}(A-\theta I_5) = -\theta^3 + 3\theta^2 + \theta - 5, \\ v_3 &= (-1)^4\Delta_{13}(A-\theta I_5) = \theta^3 - 2\theta^2 - \theta + 3, \\ v_4 &= (-1)^5\Delta_{14}(A-\theta I_5) = -2\theta^2 + \theta + 4, \\ v_5 &= (-1)^6\Delta_{15}(A-\theta I_5) = -\theta^3 + 5\theta^2 - 8. \end{aligned}$$

Logo

$$v_\theta = \begin{pmatrix} \theta^4 - 5\theta^3 + 2\theta^2 + 7\theta - 4 \\ -\theta^3 + 3\theta^2 + \theta - 5 \\ \theta^3 - 2\theta^2 - \theta + 3 \\ -2\theta^2 + \theta + 4 \\ -\theta^3 + 5\theta^2 - 8 \end{pmatrix}.$$

(3) Para encontrar o elemento α, precisamos calcular o autovetor $v'_\theta = (v'_1, v'_2, v'_3, v'_4, v'_5)^t$ de A^t associado a θ. Suas componentes são dadas por

$$v'_j = \sum_{i=1}^{5} m_{ij}\theta^{i-1}$$

com $(m_{ij})_{i,j=1}^5 = G^{-1}(V^t)^{-1}$, em que V é a matriz de coordenadas de v_1, v_2, v_3, v_4, v_5 na base $\{1, \theta, \theta^2, \theta^3, \theta^4\}$ e $G = Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^{i-1}\theta^{j-1})))_{i,j=1}^5$.

Então temos

$$V = \begin{pmatrix} -4 & -5 & 3 & 4 & -8 \\ 7 & 1 & -1 & 1 & 0 \\ 2 & 3 & -2 & -2 & 5 \\ -5 & -1 & 1 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Portanto

$$(V^t)^{-1} = \begin{pmatrix} 0 & -1 & 0 & 1 & 1 \\ 0 & 2 & 2 & 1 & 0 \\ 0 & -1 & 1 & 2 & 2 \\ 0 & 3 & 5 & 2 & 1 \\ 1 & -1 & 9 & 3 & 5 \end{pmatrix}.$$

Por outro lado, temos

$$G = Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^{i-1}\theta^{j-1})))_{i,j=1}^5 =$$

$$\begin{pmatrix} Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(1) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^2) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^3) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^4) \\ Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^2) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^3) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^4) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^5) \\ Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^2) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^3) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^4) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^5) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^6) \\ Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^3) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^4) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^5) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^6) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^7) \\ Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^4) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^5) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^6) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^7) & Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^8) \end{pmatrix}.$$

Como θ é uma raiz de $\chi_A(x)$, e o conjunto de suas raízes é dado por $\{-1.2645203, -1.1576566, 0.8781279, 1.5634155, 3.9806334\}$, temos que os mergulhos reais de θ são dados por $\sigma_1(\theta) = -1.2645203$, $\sigma_2(\theta) = -1.1576566$, $\sigma_3(\theta) = 0.8781279$, $\sigma_4(\theta) = 1.5634155$ e $\sigma_5(\theta) = 3.9806334$. Então temos

$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(1) = \sigma_1(1) + \sigma_2(1) + \sigma_3(1) + \sigma_4(1) + \sigma_5(1) = 5,$
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta) = \sigma_1(\theta) + \sigma_2(\theta) + \sigma_3(\theta) + \sigma_4(\theta) + \sigma_5(\theta) = 4,$
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^2) = \sigma_1(\theta)^2 + \sigma_2(\theta)^2 + \sigma_3(\theta)^2 + \sigma_4(\theta)^2 + \sigma_5(\theta)^2 = 22,$
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^3) = \sigma_1(\theta)^3 + \sigma_2(\theta)^3 + \sigma_3(\theta)^3 + \sigma_4(\theta)^3 + \sigma_5(\theta)^3 = 64,$
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^4) = \sigma_1(\theta)^4 + \sigma_2(\theta)^4 + \sigma_3(\theta)^4 + \sigma_4(\theta)^4 + \sigma_5(\theta)^4 = 262,$
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^5) = \sigma_1(\theta)^5 + \sigma_2(\theta)^5 + \sigma_3(\theta)^5 + \sigma_4(\theta)^5 + \sigma_5(\theta)^5 = 1004,$
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^6) = \sigma_1(\theta)^6 + \sigma_2(\theta)^6 + \sigma_3(\theta)^6 + \sigma_4(\theta)^6 + \sigma_5(\theta)^6 = 4000,$
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^7) = \sigma_1(\theta)^7 + \sigma_2(\theta)^7 + \sigma_3(\theta)^7 + \sigma_4(\theta)^7 + \sigma_5(\theta)^7 = 15852,$
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^8) = \sigma_1(\theta)^8 + \sigma_2(\theta)^8 + \sigma_3(\theta)^8 + \sigma_4(\theta)^8 + \sigma_5(\theta)^8 = 63086.$

Portanto

$$G = \begin{pmatrix} 5 & 4 & 22 & 64 & 262 \\ 4 & 22 & 64 & 262 & 1004 \\ 22 & 64 & 262 & 1004 & 4000 \\ 64 & 262 & 1004 & 4000 & 15852 \\ 262 & 1004 & 4000 & 15852 & 63086 \end{pmatrix},$$

com $d_{\mathbb{K}} = det(G) = 246832$. Então, temos

$$(m_{ij})_{i,j=1}^{5} = G^{-1}(V^t)^{-1} =$$

$$\begin{pmatrix} -\frac{17863}{15427} & -\frac{59777}{15427} & -\frac{48234}{15427} & -\frac{12436}{15427} & \frac{3170}{15427} \\ \frac{25515}{15427} & \frac{142811}{30854} & \frac{117781}{30854} & \frac{12692}{15427} & -\frac{20657}{30854} \\ \frac{8167}{15427} & \frac{56271}{30854} & \frac{49535}{30854} & \frac{9902}{15427} & \frac{32304}{15427} \\ -\frac{16432}{15427} & -\frac{86143}{30854} & -\frac{70501}{30854} & -\frac{13833}{30854} & \frac{12495}{30854} \\ \frac{6559}{30854} & \frac{16301}{30854} & \frac{13105}{30854} & \frac{1921}{30854} & -\frac{3127}{30854} \end{pmatrix}.$$

Então o autovetor v'_θ é dado por

$$v'_\theta = \begin{pmatrix} 1 & \theta & \theta^2 & \theta^3 & \theta^4 \end{pmatrix} \cdot \begin{pmatrix} -\frac{17863}{15427} & -\frac{59777}{15427} & -\frac{48234}{15427} & -\frac{12436}{15427} & \frac{3170}{15427} \\ \frac{25515}{15427} & \frac{142811}{30854} & \frac{117781}{30854} & \frac{12692}{15427} & -\frac{20657}{30854} \\ \frac{8167}{15427} & \frac{56271}{30854} & \frac{49535}{30854} & \frac{9902}{15427} & \frac{32304}{15427} \\ -\frac{16432}{15427} & -\frac{86143}{30854} & -\frac{70501}{30854} & -\frac{13833}{30854} & \frac{12495}{30854} \\ \frac{6559}{30854} & \frac{16301}{30854} & \frac{13105}{30854} & \frac{1921}{30854} & -\frac{3127}{30854} \end{pmatrix} =$$

$$\begin{pmatrix} -\frac{17863}{15427} + \frac{25515\theta}{15427} + \frac{8167\theta^2}{15427} - \frac{16432\theta^3}{15427} + \frac{6559\theta^4}{30854} \\ -\frac{59777}{15427} + \frac{142811\theta}{30854} + \frac{56271\theta^2}{30854} - \frac{86143\theta^3}{30854} + \frac{16301\theta^4}{30854} \\ -\frac{48234}{15427} + \frac{117781\theta}{30854} + \frac{49535\theta^2}{30854} - \frac{70501\theta^3}{30854} + \frac{13105\theta^4}{30854} \\ -\frac{12436}{15427} + \frac{12692\theta}{15427} + \frac{9902\theta^2}{15427} - \frac{13833\theta^3}{30854} + \frac{1921\theta^4}{30854} \\ \frac{3170}{15427} - \frac{20657\theta}{30854} + \frac{2304\theta^2}{15427} + \frac{12495\theta^3}{30854} - \frac{3127\theta^4}{30854} \end{pmatrix}$$

O elemento α é dado por $\alpha v_\theta = Bv'_\theta$, de onde segue o sistema matricial:

$$\alpha \cdot \begin{pmatrix} \theta^4 - 5\theta^3 + 2\theta^2 + 7\theta - 4 \\ -\theta^3 + 3\theta^2 + \theta - 5 \\ \theta^3 - 2\theta^2 - \theta + 3 \\ -2\theta^2 + \theta + 4 \\ -\theta^3 + 5\theta^2 - 8 \end{pmatrix} =$$

$$\begin{pmatrix} \frac{12508}{15427} - \frac{15721\theta}{30854} - \frac{16867\theta^2}{30854} + \frac{4773\theta^3}{30854} + \frac{13\theta^4}{30854} \\ -\frac{71320}{15427} + \frac{167841\theta}{30854} + \frac{63007\theta^2}{30854} - \frac{101785\theta^3}{30854} + \frac{19497\theta^4}{30854} \\ -\frac{6392}{15427} + \frac{16337\theta}{30854} + \frac{6661\theta^2}{30854} - \frac{4081\theta^3}{15427} + \frac{1429\theta^4}{30854} \\ \frac{20192}{15427} - \frac{23178\theta}{15427} - \frac{14535\theta^2}{30854} + \frac{15170\theta^3}{15427} - \frac{3068\theta^4}{15427} \\ \frac{18776}{15427} - \frac{33349\theta}{15427} - \frac{5294\theta^2}{15427} + \frac{38823\theta^3}{30854} - \frac{8175\theta^4}{30854} \end{pmatrix}$$

Pela quarta linha do sistema, temos

$$\alpha = \frac{\frac{20192}{15427} - \frac{23178\theta}{15427} - \frac{14535\theta^2}{30854} + \frac{15170\theta^3}{15427} - \frac{3068\theta^4}{15427}}{-2\theta^2+\theta+4}$$

(4) A matriz geradora do reticulado é dada por

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(v_1) & \sqrt{\alpha_2}\sigma_2(v_1) & \sqrt{\alpha_3}\sigma_3(v_1) & \sqrt{\alpha_4}\sigma_4(v_1) & \sqrt{\alpha_5}\sigma_5(v_1) \\ \sqrt{\alpha_1}\sigma_1(v_2) & \sqrt{\alpha_2}\sigma_2(v_2) & \sqrt{\alpha_3}\sigma_3(v_2) & \sqrt{\alpha_4}\sigma_4(v_2) & \sqrt{\alpha_5}\sigma_5(v_2) \\ \sqrt{\alpha_1}\sigma_1(v_3) & \sqrt{\alpha_2}\sigma_2(v_3) & \sqrt{\alpha_3}\sigma_3(v_3) & \sqrt{\alpha_4}\sigma_4(v_3) & \sqrt{\alpha_5}\sigma_5(v_3) \\ \sqrt{\alpha_1}\sigma_1(v_4) & \sqrt{\alpha_2}\sigma_2(v_4) & \sqrt{\alpha_3}\sigma_3(v_4) & \sqrt{\alpha_4}\sigma_4(v_4) & \sqrt{\alpha_5}\sigma_5(v_4) \\ \sqrt{\alpha_1}\sigma_1(v_5) & \sqrt{\alpha_2}\sigma_2(v_5) & \sqrt{\alpha_3}\sigma_3(v_5) & \sqrt{\alpha_4}\sigma_4(v_5) & \sqrt{\alpha_5}\sigma_5(v_5) \end{pmatrix}.$$

Então:

$$\alpha_1 = \sigma_1(\alpha) = \frac{\frac{20192}{15427} - \frac{23178\sigma_1(\theta)}{15427} - \frac{14535\sigma_1(\theta)^2}{30854} + \frac{15170\sigma_1(\theta)^3}{15427} - \frac{3068\sigma_1(\theta)^4}{15427}}{-2\sigma_1(\theta)^2+\sigma_1(\theta)+4} = 0.0893574,$$
$$\alpha_2 = \sigma_2(\alpha) = \frac{\frac{20192}{15427} - \frac{23178\sigma_2(\theta)}{15427} - \frac{14535\sigma_2(\theta)^2}{30854} + \frac{15170\sigma_2(\theta)^3}{15427} - \frac{3068\sigma_2(\theta)^4}{15427}}{-2\sigma_2(\theta)^2+\sigma_2(\theta)+4} = 3.29642,$$
$$\alpha_3 = \sigma_3(\alpha) = \frac{\frac{20192}{15427} - \frac{23178\sigma_3(\theta)}{15427} - \frac{14535\sigma_3(\theta)^2}{30854} + \frac{15170\sigma_3(\theta)^3}{15427} - \frac{3068\sigma_3(\theta)^4}{15427}}{-2\sigma_3(\theta)^2+\sigma_3(\theta)+4} = 0.0521258,$$
$$\alpha_4 = \sigma_4(\alpha) = \frac{\frac{20192}{15427} - \frac{23178\sigma_4(\theta)}{15427} - \frac{14535\sigma_4(\theta)^2}{30854} + \frac{15170\sigma_4(\theta)^3}{15427} - \frac{3068\sigma_4(\theta)^4}{15427}}{-2\sigma_4(\theta)^2+\sigma_4(\theta)+4} = 0.560212,$$
$$\alpha_5 = \sigma_5(\alpha) = \frac{\frac{20192}{15427} - \frac{23178\sigma_5(\theta)}{15427} - \frac{14535\sigma_5(\theta)^2}{30854} + \frac{15170\sigma_5(\theta)^3}{15427} - \frac{3068\sigma_5(\theta)^4}{15427}}{-2\sigma_5(\theta)^2+\sigma_5(\theta)+4} = 0.001884.$$

Além disso, temos

$\sigma_1(v_1) = 3.01313$, $\sigma_2(v_1) = 0.13007$, $\sigma_3(v_1) = 0.898061$, $\sigma_4(v_1) = -1.30014$, $\sigma_5(v_1) = -8.74112$,
$\sigma_1(v_2) = 0.554498$, $\sigma_2(v_2) = -0.585695$, $\sigma_3(v_2) = -2.48568$, $\sigma_4(v_2) = 0.0748131$, $\sigma_5(v_2) = -16.5579$,
$\sigma_1(v_3) = -0.955486$, $\sigma_2(v_3) = -0.0741363$, $\sigma_3(v_3) = 1.25679$, $\sigma_4(v_3) = 0.369455$, $\sigma_5(v_3) = 30.4034$,
$\sigma_1(v_4) = -0.462544$, $\sigma_2(v_4) = 0.162006$, $\sigma_3(v_4) = 3.33591$, $\sigma_4(v_4) = 0.674879$, $\sigma_5(v_4) = -23.7103$,
$\sigma_1(v_5) = 2.01704$, $\sigma_2(v_5) = 0.252299$, $\sigma_3(v_5) = -4.82159$, $\sigma_4(v_5) = 0.399934$ e $\sigma_5(v_5) = 8.15231$.

Aplicando os valores encontrados, temos que a matriz geradora computada para o reticulado D_5 é dada por

$$M = \begin{pmatrix} 0.900707 & 0.236156 & 0.205037 & -0.973122 & -0.379409 \\ 0.165754 & -1.06339 & -0.567507 & 0.0559956 & -0.718698 \\ -0.285621 & -0.134602 & 0.286938 & 0.276527 & 1.31966 \\ -0.138267 & 0.294138 & 0.761624 & 0.505129 & -1.02914 \\ 0.602948 & 0.458076 & -1.10082 & 0.29934 & 0.353852 \end{pmatrix}.$$

Para a distância produto mínima relativa, temos $det(B) = 4$, $[\mathscr{O}_{\mathbb{K}} : \mathbb{Z}[\theta]] = 1$, $d_{\mathbb{K}} = 246832$ e $h(\mathbb{K}) = 1 = min(\mathscr{I})$. Então

$$\sqrt[5]{d_{p,rel}(D_5)} = (\frac{1}{\sqrt{det(B)}}\sqrt{\frac{det(B)}{d_{\mathbb{K}}}}\frac{min(\mathscr{I})}{[\mathscr{O}_{\mathbb{K}} : \mathbb{Z}[\theta]]})^{1/5} = (\frac{1}{\sqrt{4}}\sqrt{\frac{4}{246832}})^{1/5} = 0.28890.$$

5.5 Reticulado E_6

Uma matriz geradora do reticulado E_6 é dada por

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

cuja matriz de Gram associada é dada por

$$B = MM^t = \begin{pmatrix} 8 & -4 & 0 & 0 & 0 & 0 \\ -4 & 8 & 4 & 0 & 0 & 0 \\ 0 & -4 & 8 & -4 & 0 & -4 \\ 0 & 0 & -4 & 8 & -4 & 0 \\ 0 & 0 & 0 & -4 & 8 & 0 \\ 0 & 0 & -4 & 0 & 0 & 8 \end{pmatrix}.$$

(1) Através do Mathematica, computamos a matriz A e calculamos a base integral e discriminante do corpo.

O corpo com menor discriminante encontrado cuja base integral é canônica possui $d_{\mathbb{K}} = 14631616$. Através do PARI/GP, pelo polinômio característico da matriz A encontrada, $\chi_A(x) = x^6 + 2x^5 - 9x^4 - 24x^3 - 8x^2 + 8x - 1$, temos $h(\mathbb{K}) = 1$.

Seja $\mathbb{K}$ o corpo de números dado por $\chi_A(x) = x^6 + 2x^5 - 9x^4 - 24x^3 - 8x^2 + 8x - 1$. A matriz

$$A = \begin{pmatrix} -1 & 0 & -1 & 1 & 1 & 0 \\ 1 & & 01 & 0 & 0 & 0 \\ -1 & 1 & 1 & -1 & -1 & -1 \\ 1 & 0 & 0 & 0 & 1 & 2 \\ 0 & -1 & -2 & -1 & -2 & -1 \\ 0 & -1 & -1 & 2 & 1 & 0 \end{pmatrix}$$

possui polinômio característico $\chi_A(x) = x^6 + 2x^5 - 9x^4 - 24x^3 - 8x^2 + 8x - 1$, irredutível sobre $\mathbb{Q}$, e satisfaz a condição $B^{-1}AB = A^t$.

(2) O autovetor $v_\theta = (v_1, v_2, v_3, v_4, v_5, v_6)^t$ de A associado a θ tal que $\{v_1, v_2, v_3, v_4, v_5, v_6\}$ é uma $\mathbb{Z}$-base do ideal $\mathscr{I}$ tem componentes

$$v_j = (-1)^{i+j}\Delta_{ij}(A - \theta I_6),$$

em que $\Delta_{ij}(A-\theta I_5)$ é a menor obtida fixando uma das linhas, digamos a i-ésima linha.

Tomando $i=1$, ou seja, fixando a primeira linha, temos que

$$\begin{aligned}
v_1 &= \Delta_{11}(A-\theta I_6) = -\theta^5-\theta^4+8\theta^3+13\theta^2+\theta-2,\\
v_2 &= \Delta_{12}(A-\theta I_6) = -\theta^4+10\theta^2+10\theta-4,\\
v_3 &= \Delta_{13}(A-\theta I_6) = \theta^4+2\theta^3-3\theta^2-5\theta+2,\\
v_4 &= \Delta_{14}(A-\theta I_6) = -\theta^4-\theta^3+4\theta^2-4\theta-1,\\
v_5 &= \Delta_{15}(A-\theta I_6) = -\theta^2-2\theta,\\
v_6 &= \Delta_{16}(A-\theta I_6) = -2\theta^3-4\theta^2+1.
\end{aligned}$$

Então

$$v_\theta = \begin{pmatrix} -\theta^5-\theta^4+8\theta^3+13\theta^2+\theta-2 \\ -\theta^4+10\theta^2+10\theta-4 \\ \theta^4+2\theta^3-3\theta^2-5\theta+2 \\ -\theta^4-\theta^3+4\theta^2-4\theta-1 \\ -\theta^2-2\theta \\ -2\theta^3-4\theta^2+1 \end{pmatrix}.$$

(3) Para encontrar o elemento α, precisamos calcular o autovetor $v'_\theta = (v'_1, v'_2, v'_3, v'_4, v'_5, v'_6)^t$ de A^t associado a θ. Suas componentes são dadas por

$$v'_j = \sum_{i=1}^{6} m_{ij}\theta^{i-1}$$

com $(m_{ij})_{i,j=1}^6 = G^{-1}(V^t)^{-1}$, cuja V é a matriz de coordenadas de $v_1, v_2, v_3, v_4, v_5, v_6$ na base $\{1, \theta, \theta^2, \theta^3, \theta^4, \theta^5\}$ e $G = Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^{i-1}\theta^{j-1})))_{i,j=1}^6$.

Então temos

$$V = \begin{pmatrix} -2 & -4 & 2 & -1 & 0 & 1 \\ 1 & 10 & -5 & 4 & -2 & 0 \\ 13 & 10 & -3 & 4 & -1 & -4 \\ 8 & 0 & 2 & -1 & 0 & -2 \\ -1 & -1 & 1 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

e, portanto,

$$(V^t)^{-1} = \begin{pmatrix} 0 & 2 & 4 & 2 & 4 & 3 \\ 0 & -3 & -5 & -2 & -7 & -4 \\ 0 & 6 & 10 & 4 & 13 & 8 \\ 0 & -11 & -18 & -7 & -24 & -15 \\ 0 & 21 & 34 & 12 & 44 & 28 \\ -1 & -38 & -61 & -22 & -82 & -54 \end{pmatrix}.$$

Além disso, como θ é uma raiz de $\chi_A(x)$, e o conjunto de suas raízes é dado por $\{-2.4585, -1.8667, -1.37126, 0.168797, 0.290826, 3.23689\}$, temos que os mergulhos reais de θ são dados por $\sigma_1(\theta) = -2.4585$, $\sigma_2(\theta) = -1.8667$, $\sigma_3(\theta) = -1.37126$, $\sigma_4(\theta) = 0.168797$, $\sigma_5(\theta) = 0.290826$ e $\sigma_6(\theta) = 3.23689$.

Então temos

$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(1) = 6$, $Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta) = -2$, $Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^2) = 22$, $Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^3) = 10$,
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^4) = 162$, $Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^5) = 238$, $Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^6) = 1420$, $Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^7) = 3092$,
$Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^8) = 13546$, $Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^9) = 35434$, $Tr_{\mathbb{Q}(\theta)|\mathbb{Q}}(\theta^{10}) = 134872$.

Portanto

$$G = \begin{pmatrix} 6 & -2 & 22 & 10 & 162 & 238 \\ -2 & 22 & 10 & 162 & 238 & 1420 \\ 22 & 10 & 162 & 238 & 1420 & 3092 \\ 10 & 162 & 238 & 1420 & 3092 & 13546 \\ 162 & 238 & 1420 & 3092 & 13546 & 35434 \\ 238 & 1420 & 3092 & 13546 & 35434 & 134872 \end{pmatrix},$$

com $d_{\mathbb{K}} = det(G) = 14631616$. Então, temos

$$(m_{ij})_{i,j=1}^{6} = G^{-1}(V^t)^{-1} =$$

$$\begin{pmatrix} -\frac{395827}{457238} & -\frac{844455}{457238} & -\frac{1086593}{457238} & -\frac{745009}{457238} & -\frac{421012}{457238} & -\frac{614124}{457238} \\ \frac{1039443}{457238} & \frac{3064188}{457238} & \frac{4419575}{457238} & \frac{2855355}{457238} & \frac{2045955}{457238} & \frac{2806419}{457238} \\ \frac{2378808}{457238} & \frac{3702815}{457238} & \frac{5418495}{457238} & \frac{4277579}{457238} & \frac{189548}{457238} & \frac{2576415}{457238} \\ \frac{933202}{457238} & \frac{335784}{457238} & \frac{533849}{457238} & \frac{941019}{457238} & -\frac{1650314}{457238} & -\frac{283684}{457238} \\ -\frac{195898}{457238} & -\frac{373231}{457238} & -\frac{546533}{457238} & -\frac{399394}{457238} & -\frac{126854}{457238} & -\frac{292350}{457238} \\ -\frac{107044}{457238} & -\frac{51457}{457238} & -\frac{79073}{457238} & -\frac{116470}{116470} & \frac{173657}{457238} & \frac{17587}{457238} \end{pmatrix}.$$

Então o autovetor v'_θ é dado por $v'_\theta = (v'_1, v'_2, v'_3, v'_4, v'_5, v'_6)^t$, com

$$v'_1 = -\frac{395827}{457238} + \frac{1039443\theta}{457238} + \frac{2378808\theta^2}{457238} + \frac{933202\theta^3}{457238} - \frac{195898\theta^4}{457238} - \frac{107044\theta^5}{457238},$$

$$v'_2 = -\frac{844455}{457238} + \frac{3064188\theta}{457238} + \frac{3702815\theta^2}{457238} + \frac{335784\theta^3}{457238} - \frac{373231\theta^4}{457238} - \frac{51457\theta^5}{457238},$$

$$v'_3 = -\frac{1086593}{457238} + \frac{4419575\theta}{457238} + \frac{5418495\theta^2}{457238} + \frac{533849\theta^3}{457238} - \frac{546533\theta^4}{457238} - \frac{79073\theta^5}{457238},$$

$$v'_4 = -\frac{745009}{457238} + \frac{2855355\theta}{457238} + \frac{4277579\theta^2}{457238} + \frac{941019\theta^3}{457238} - \frac{399394\theta^4}{457238} - \frac{116470\theta^5}{116470},$$

$$v'_5 = -\frac{421012}{457238} + \frac{2045955\theta}{457238} + \frac{189548\theta^2}{457238} - \frac{1650314\theta^3}{457238} - \frac{126854\theta^4}{457238} + \frac{173657\theta^5}{457238},$$

$$v'_6 = -\frac{614124}{457238} + \frac{2806419\theta}{457238} + \frac{2576415\theta^2}{457238} - \frac{283684\theta^3}{457238} - \frac{292350\theta^4}{457238} + \frac{17587\theta^5}{457238}.$$

O elemento α é dado por $\alpha v_\theta = Bv'_\theta$, de onde segue

$$\alpha = -\frac{2138446}{228619} + \frac{176156746\theta}{228619} - \frac{2031863858\theta^2}{457238} - \frac{311317668\theta^3}{228619} + \frac{19403048\theta^4}{228619} + \frac{3356022\theta^5}{228619}.$$

(4) A matriz geradora do reticulado é dada por

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(v_1) & \sqrt{\alpha_2}\sigma_2(v_1) & \sqrt{\alpha_3}\sigma_3(v_1) & \sqrt{\alpha_4}\sigma_4(v_1) & \sqrt{\alpha_5}\sigma_5(v_1) & \sqrt{\alpha_6}\sigma_6(v_1) \\ \sqrt{\alpha_1}\sigma_1(v_2) & \sqrt{\alpha_2}\sigma_2(v_2) & \sqrt{\alpha_3}\sigma_3(v_2) & \sqrt{\alpha_4}\sigma_4(v_2) & \sqrt{\alpha_5}\sigma_5(v_2) & \sqrt{\alpha_6}\sigma_6(v_2) \\ \sqrt{\alpha_1}\sigma_1(v_3) & \sqrt{\alpha_2}\sigma_2(v_3) & \sqrt{\alpha_3}\sigma_3(v_3) & \sqrt{\alpha_4}\sigma_4(v_3) & \sqrt{\alpha_5}\sigma_5(v_3) & \sqrt{\alpha_6}\sigma_6(v_3) \\ \sqrt{\alpha_1}\sigma_1(v_4) & \sqrt{\alpha_2}\sigma_2(v_4) & \sqrt{\alpha_3}\sigma_3(v_4) & \sqrt{\alpha_4}\sigma_4(v_4) & \sqrt{\alpha_5}\sigma_5(v_4) & \sqrt{\alpha_6}\sigma_6(v_4) \\ \sqrt{\alpha_1}\sigma_1(v_5) & \sqrt{\alpha_2}\sigma_2(v_5) & \sqrt{\alpha_3}\sigma_3(v_5) & \sqrt{\alpha_4}\sigma_4(v_5) & \sqrt{\alpha_5}\sigma_5(v_5) & \sqrt{\alpha_6}\sigma_6(v_5) \\ \sqrt{\alpha_1}\sigma_1(v_6) & \sqrt{\alpha_2}\sigma_2(v_6) & \sqrt{\alpha_3}\sigma_3(v_6) & \sqrt{\alpha_4}\sigma_4(v_6) & \sqrt{\alpha_5}\sigma_5(v_6) & \sqrt{\alpha_6}\sigma_6(v_6) \end{pmatrix}.$$

Então, temos

$\alpha_1 = \sigma_1(\alpha) = -2148.81$, $\alpha_2 = \sigma_2(\alpha) = -1138.31$, $\alpha_3 = \sigma_3(\alpha) = -667.653$,
$\alpha_4 = \sigma_4(\alpha) = -9.66111$, $\alpha_5 = \sigma_5(\alpha) = -27.8432$ e $\alpha_6 = \sigma_6(\alpha) = -3724.77$.

Além disso, temos

$\sigma_1(v_1) = 8.52411$, $\sigma_2(v_1) = -0.0807952$, $\sigma_3(v_1) = 1.75839$, $\sigma_4(v_1) = -1.42328$, $\sigma_5(v_1) = -0.422086$, $\sigma_6(v_1) = -56.3563$,
$\sigma_1(v_2) = -4.67671$, $\sigma_2(v_2) = 0.036464$, $\sigma_3(v_2) = -2.44482$, $\sigma_4(v_2) = -2.02792$, $\sigma_5(v_2) = -0.253094$, $\sigma_6(v_2) = 23.3661$,
$\sigma_1(v_3) = 2.97388$, $\sigma_2(v_3) = 0.0127279$, $\sigma_3(v_3) = 1.59408$, $\sigma_4(v_3) = 1.08097$, $\sigma_5(v_3) = 0.34848$, $\sigma_6(v_3) = 131.99$,
$\sigma_1(v_4) = 11.3368$, $\sigma_2(v_4) = 14.7675$, $\sigma_3(v_4) = 11.0491$, $\sigma_4(v_4) = -1.56684$, $\sigma_5(v_4) = -1.85674$, $\sigma_6(v_4) = -115.73$,
$\sigma_1(v_5) = -1.12741$, $\sigma_2(v_5) = 0.248837$, $\sigma_3(v_5) = 0.862169$, $\sigma_4(v_5) = -0.366086$, $\sigma_5(v_5) = -0.666232$, $\sigma_6(v_5) = -16.9513$,
$\sigma_1(v_6) = 6.54362$, $\sigma_2(v_6) = 0.0709935$, $\sigma_3(v_6) = -1.36451$, $\sigma_4(v_6) = 0.876412$, $\sigma_5(v_6) = 0.612485$ e $\sigma_6(v_6) = -108.739$.

Então, substituindo os valores encontrados, a matriz geradora computada para o reticulado E_6 é dada por

$$M = \begin{pmatrix} 1.616 & -0.809 & 1.586 & -0.973 & -0.629 & -0.933 \\ -0.886 & 0.365 & -2.205 & -1.387 & -0.377 & 0.387 \\ 0.563 & 0.127 & 1.437 & 0.739 & 0.519 & 2.186 \\ -1.579 & -1.664 & 0.071 & -0.148 & 0.700 & -1.488 \\ -0.213 & 2.494 & 0.777 & -0.250 & -0.993 & -0.280 \\ 1.240 & 0.711 & -1.230 & 0.599 & 0.913 & -1.801 \end{pmatrix}.$$

A distância produto mínima relativa é dada por

$$\sqrt[6]{d_{p,rel}(E_6)} = \left(\frac{1}{\sqrt{det(B)}}\sqrt{\frac{det(B)}{d_{\mathbb{K}}}}\frac{min(\mathscr{I})}{[\mathscr{O}_{\mathbb{K}} : \mathbb{Z}[\theta]]}\right)^{1/6}$$

com $det(B) = 12288$, $[\mathscr{O}_{\mathbb{K}} : \mathbb{Z}[\theta]] = 1$, $d_{\mathbb{K}} = 14631616$ e $h(\mathbb{K}) = 1 = min(\mathscr{I})$. Então

$$\sqrt[6]{d_{p,rel}(E_6)} = \left(\frac{1}{\sqrt{12288}}\sqrt{\frac{12288}{14631616}}\right)^{1/6} = 0.25286.$$

5.6 Performance da distância produto

Nesta seção apresentamos uma tabela comparando a distância produto mínima relativa normalizada dos reticulados construídos nas seções anteriores e os reticulados da família $\mathbb{Z}^n$ com as melhores distâncias produto mínima conhecidas.

Tabela 5.1: Performance

Dimensão	$\sqrt[n]{d_{p,rel}(\Lambda)}$	$\sqrt[n]{d_{p,rel}(\mathbb{Z}^n)}$
2	0.53728	0.66874
3	0.38316	0.52275
4	0.38555	0.43899
5	0.28890	0.38321
6	0.25286	0.34958

Apesar das distâncias produto mínima dos reticulados A_2, D_3, D_4, D_5 e E_6 construídos ficarem aquém das distâncias dos reticulados $\mathbb{Z}^n$, para $n = 2,3,4,5,6$, respectivamente, essas distâncias podem ser melhoradas, conforme as considerações a seguir.

CAPÍTULO

6

Considerações finais e perspectivas futuras

Neste trabalho apresentamos o método para a construção de reticulados baseado nos trabalhos de Krüskemper, Taussky e Oggier, através do qual construímos versões rotacionadas dos reticulados A_2, D_3, D_4, D_5 e E_6, com diversidade máxima, uma vez construídos sobre corpos totalmente reais, e com boa distância produto mínima.

Neste sentido, apresentamos uma detalhada base teórica algébrica e dos Reticulados, dos conceitos e resultados necessários para o entendimento do método, também apresentado detalhadamente, a partir dos resultados que servem de base para o algoritmo de construção dos reticulados.

Como descrito no Capítulo 4, com o objetivo de construir reticulados com a maior distância produto mínima possível, buscamos por um corpo de números $\mathbb{K}$ com a melhor combinação de três variáveis: o discriminante do corpo $d_{\mathbb{K}}$, uma ordem $\mathfrak{D} = \mathbb{Z}[\theta]$ para calcular o índice $[\mathscr{O}_{\mathbb{K}} : \mathfrak{D}]$ e a variável $min(\mathscr{I}) = \min_{0 \neq x \in \mathscr{I}} \frac{N(x)}{N(\mathscr{I})}$.

Como este último é um valor difícil de ser calculado, buscamos encontrar reticulados sobre ideais principais, de modo que tenhamos o class number $h(\mathbb{K}) = 1 = min(\mathscr{I}) = \min_{0 \neq x \in \mathscr{I}} \frac{N(x)}{N(\mathscr{I})}$, o que pode ser verificado através do software PARI/GP, ressaltando que o software não computa o valor de $h(\mathbb{K})$, somente indica se de fato seu valor é igual a 1.

A partir disso, a busca pela maior distância produto mínima fica restrita a melhor combinação entre o índice $[\mathscr{O}_{\mathbb{K}} : \mathfrak{D}]$ e o discriminante $d_{\mathbb{K}}$, variáveis que podemos calcular e temos controle através do software Wolfram Mathematica. Para determinar a melhor combinação possível, fizemos o seguinte cálculo: determinamos a distância produto mínima com um discriminante encontrado e com base integral de $\mathscr{O}_{\mathbb{K}}$ canônica, o que nos fornece $[\mathscr{O}_{\mathbb{K}} : \mathfrak{D}] = 1$. A partir disto, buscamos encontrar o mesmo valor para a distância produto mínima, fixando $[\mathscr{O}_{\mathbb{K}} : \mathfrak{D}] > 1$ e calculando qual seria o valor para o discriminante do corpo. Com este cálculo, concluímos que para encontrar o mesmo valor de distância produto mínima, com $[\mathscr{O}_{\mathbb{K}} : \mathfrak{D}] > 1$, precisaríamos de um discriminante $d_{\mathbb{K}}$ com valor muito baixo, menor que o mínimo existente para cada reticulado.

Ou seja, de forma resumida, verificamos que a melhor combinação possível entre o índice $[\mathscr{O}_{\mathbb{K}} : \mathfrak{D}]$ e o discriminante $d_{\mathbb{K}}$ para encontrar a maior distância produto mínima é determinando um corpo de números tal que tenhamos uma base integral canônica para $\mathscr{O}_{\mathbb{K}}$, e portanto $[\mathscr{O}_{\mathbb{K}} : \mathfrak{D}] = 1$, com seu menor discriminante. A partir disso, é possível restringir a busca no

software Mathematica para encontrar a matriz A que satisfaz $AB = BA^t$, onde B é a matriz de Gram do reticulado, filtrando a busca pela base integral canônica, com o menor discriminante do corpo respectivo.

O método apresentado neste trabalho tem como vantagem a construção de reticulados através de mergulho de corpos totalmente reais, o que resultado em reticulados de diversidade máxima, além de permitir o controle do discriminante do corpo e da ordem $\mathfrak{D} = \mathbb{Z}[\theta]$, e seu respectivo índice $[\mathscr{O}_{\mathbb{K}} : \mathfrak{D}]$, que temos através do algoritmo computacional pelo software Mathematica. Além disso, todo o algoritmo apresentado no capítulo 4, para a obtenção da matriz geradora que pretendemos calcular, pode ser implementado computacionalmente pelo referido software, simplificando cálculos manualmente custosos.

No entanto, à medida que avançamos para espaços dimensionais mais altos, o custo computacional para determinar a matriz A tal que $AB = BA^t$ aumenta consideravelmente, dificultando a obtenção dos melhores resultados possíveis, como encontrar matrizes cujo corpo de números possua ordem $\mathfrak{D}$ tal que $[\mathscr{O}_{\mathbb{K}} : \mathfrak{D}] = 1$. Com isso, algumas das medidas que adotamos para mitigar essa dificuldade de custo computacional foram fixar valores para algumas componentes da matriz A, ou colocando $A := BS$, onde B é a matriz de Gram e S é uma matriz simétrica, pelo qual facilmente se verifica que a relação $BA = AB^t$ se mantem. Em ambos os casos, como diminuímos a quantidade de variáveis livres a serem encontradas para determinar a matriz A, o custo computacional também diminui. Porém, ao utilizar essas ferramentas, diminuímos também o espaço das possíveis soluções para computar a matriz A com as condições postas.

Neste sentido, à medida que avançamos para espaços dimensionais maiores, deve ser feita a ponderação entre o custo computacional do cálculo da matriz A e as restrições que podem ser feitas para suavizar este custo, mas que causa restrições nas soluções, podendo impactar na obtenção dos melhores resultados.

Com base nesta questão, para trabalhos futuros temos a intenção de fazer um estudo aprofundado sobre algoritmos computacionais que permitam encontrar a matriz A, satisfazendo as condições necessárias em grandes dimensões, de forma mais otimizada, buscando diminuir o custo computacional e restringindo o mínimo possível o espaço das soluções.

A partir desta perspectiva futura, pretendemos também fazer a construção das versões rotacionadas de reticulados em dimensões maiores, buscando o melhor resultado possível em termos de distância produto mínima através do método apresentado.

Referências

[1] Conway, J.H.; Sloane, N.J.A. *Sphere Packings, Lattices and Groups*. 3rd edition *Springer-Verlag*, New York, 1999. Citado na(s) página(s): 14, 17

[2] Ferrari, A.J. *Reticulados algébricos via corpos abelianos*. *Dissertação de Mestrado*, Ibilce-Unesp, 2008. Citado na(s) página(s): 14

[3] Ferrari, A.J. *Reticulados algébricos: Abordagem matricial e simulações*. *Tese de Doutorado*, Imecc-Unicamp, 2012. Citado na(s) página(s): 14

[4] Endler, O. *Teoria dos Corpos*, *Monografias de Matemática*, N° 44, IMPA, Rio de Janeiro, 1987. Citado na(s) página(s): 14, 30, 31, 39, 40, 41, 43, 44, 46, 47, 48, 50, 54

[5] Herstein, I.N. *Tópicos de Álgebra*. *Editora Polígono S.A.*, 1970. Citado na(s) página(s): 14, 26, 27, 28, 30, 32

[6] Marcus, D.A. *Numbers Fields*. *Springer-Verlag*, New York, 1977. Citado na(s) página(s): 14

[7] Samuel, P. *Algebraic Theory of Numbers*. *Hermann*, Paris, 1967. Citado na(s) página(s): 14, 63

[8] Stewart, I. *Galois Theory*, *Chapman & Hall/CRC*, Third Edition, New York, 2004. Citado na(s) página(s): 14, 34, 35, 36, 37, 45, 47

[9] Stewart, I; Tall, D. *Algebraic Number Theory*. *Chapman & Hall*, New York, 1987. Citado na(s) página(s): 14, 61, 62, 63, 64, 66

[10] Kakuta, N. *Introdução à Teoria de Galois / Neuza Kakuta, Parham Salehyan.* - São Paulo: Cultura Acadêmica Editora, 2013. 87 p.; 21 cm. Citado na(s) página(s): 14, 53, 55, 56, 58, 59, 60

[11] Morandi, P. *Field and Galois Theory*, *GTM, Springer-Verlag*, 1996. Citado na(s) página(s): 14, 40, 42, 43, 51, 54, 57, 59

[12] Taussky, O. *On the similarity tansformation between an integral matrix with irreducible characteristic polynomial and its transpose*, *Math. Annalen, 166*, 1966. Citado na(s) página(s): 14, 70, 71

[13] Taussky, O. *On a theorem of Latimer and MacDuffee*, *Canad. J. Math., v.1, pp 300-302*, 1949. Citado na(s) página(s): 71, 73

[14] Taussky, O. *On matrix classes corresponding to an ideal and its inverse*, *Illinois Math, J, v.1, pp 108-113*, 1957. Citado na(s) página(s): 71

[15] Conner, E.P. *A survey of trace forms of algebraic number fields*, 1984. Citado na(s) página(s): 70

[16] Oggier, F. *Algebraic methods for Channel Coding*, *Pub. Math. de Besancon, Theorie des Nombres,* 1997. Citado na(s) página(s): 65, 66, 67, 68, 69, 71, 72, 73, 74

[17] Krüskemper, M. *Algebraic construction of bilinear forms over* $\mathbb{Z}$, *Ph.D. thesis, SB, Lausanne,* 2005. Citado na(s) página(s): 72

[18] Fluckiger, E.B. *Lattices and Number Fields*, *Contemp. Math., v. 241, pp. 69-84* 1999. Citado na(s) página(s): 14, 76